WORKSHOP W7

Wednesday, November 9
12:45 p.m.–1:45 p.m.

CYBER RISKS AND INSURANCE

Presented by

Michael Born
Vice President, Account Executive
Lockton Companies

Contractors face many of the cyber risks other nonretail companies face—including the hacking of corporate data, the use of ransomware, and breaches of customer or employee data—as well as a unique exposure arising out of smart-systems installed in new buildings or structures. The Internet of Things makes everything from property owners’ security systems and HVAC systems to the "key to the front door" vulnerable to cyber intruders. This session will provide insight on how to manage contractors’ cyber risks and how well cyber policies cover those risks, an overview of the cyber insurance market, and more.

To print on both sides of the page, set your printer for duplex printing.
For over 20 years, ORCPG has been a trusted leader in the US Construction Insurance Industry with a national platform; localized service through six regional offices across the country; and specialized Underwriting, Risk Control and Claims expertise to meet the unique needs of commercial contractors.

We partner with our clients to understand their unique needs and design the right solutions for each. Our parent company, Old Republic International Corporation, is one of the nation’s 50 largest publicly held insurance organizations.

*Insuring the Building of America.*

Old Republic Construction Insurance Agency, Inc. CLS#0799319
Old Republic Construction Insurance Agency of New York, Inc. LS#668042

www.orcpg.com
Mr. Born is vice president and account executive at Lockton Companies, where he provides expertise in the areas of data security, privacy liability, media, and specialty errors and omissions insurance. He has more than 20 years of experience in the professional liability insurance industry and is a member of Lockton’s Global Technology and Privacy Practice.

Mr. Born is a frequent speaker and panelist regarding data security and privacy issues, having presented on this topic for the Professional Liability Underwriting Society (PLUS), the Risk and Insurance Management Society (RIMS), the Public Risk Management Association (PRIMA), the American Society of Association Executives (ASAE), the Claims and Litigation Management (CLM) Alliance, and many others.

Mr. Born is licensed to practice law in Kansas, Missouri, Texas, and Illinois, as well as several federal jurisdictions. He has been at Lockton since 2012.
Notes
Cyber Risks and Insurance Solutions for the Construction Industry

Michael Born – Vice President – Account Executive
Lockton Companies – Cyber and Technology Practice

Education | Connection | Opportunity
Data Security and Privacy Liability
Where does my exposure come from?

Data Security
- Data Breach (theft of data, unauthorized access or use)
- Improper Collection, Use or sharing of Confidential Data
- Liability and Direct Costs

Network Security
- Transmission of Malicious Code
- Denial of Service Attacks
- Inability to Access Systems
- Liability and Direct Costs

Your Exposure: Am I a data owner?
- How many individuals’ personal information do you have in your care, custody, or control
- What kind of personal information do you have (name, address, credit card information, email address, SSN, Health Records, Bank Accounts, etc.)
- What type of confidential corporate information do you keep. (Plans, Bids, Accounts, etc.)

- Do you host your network and data OR do you outsource your network and/or data (data including personal information)
- Whether you host or outsource—you are legally liable in both cases (data is under your care, custody, or control)

- If you have data (as noted above) you ARE a data owner
- You may have the duty to notify in the event of a data breach
- You are legally liable for how you: protect, collect, share, and provide access to . . . confidential information
**Regulatory and Statutory Concerns**

STATE DATA BREACH NOTIFICATION LAWS – 47 states, including Kansas and Missouri have enacted legislation requiring notification of security breaches involving personal information.

- Family Educational Rights and Privacy Act (FERPA)
- Children’s Online Privacy Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm Leach Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA)
- Fair and Accurate Credit Transaction Act (FACTA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Children's Online Privacy Protection Act (COPPA)
- Gramm Leach Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA)
- Fair and Accurate Credit Transaction Act (FACTA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)

**Data Security and Privacy Liability Exposure**

Types of Exposure

- **Liability**
  - Suits from your customers or other individuals
  - Consumer Class Action Suits
- **Regulatory**
  - Costs of Investigation by the FTC, State AGs, HHS, FINRA, SEC, etc.
  - Privacy Regulatory Fines and Consumer Redress Funds
  - Notification Costs
  - Forensics & Data Recovery
  - Legal and Public Relations
  - Credit Monitoring and Call Center
- **Privacy Event Expenses**
  - Consumer Class Action Suits
  - Costs of Investigation by the FTC, State AGs, HHS, FINRA, SEC, etc.
  - Privacy Regulatory Fines and Consumer Redress Funds
  - Notification Costs
  - Forensics & Data Recovery
  - Legal and Public Relations
  - Credit Monitoring and Call Center
Data Security Breach Examples

• In May 2013, an Australian Broadcasting Corp. news program reported that Chinese hackers had accessed the computers of "a prime contractor" and stolen floor plans, communications-cable layouts, server locations and security-system designs for the Australian Secret Intelligence Organization's new headquarters.

• Security experts feared the leak compromised the building's physical and network security.

• Government documents say the project stretched to a fifth year and costs climbed by $132.6 million.
Network Security Breach Potential

- The unsanctioned release of sensitive plans is not unheard of. In July 2013, Forbes magazine published unclassified "for official use only" plans for data halls within the U.S. National Security Agency’s Utah data center while it was still under construction. The undisclosed source for those diagrams, according to the article’s author, was not the NSA.

- As difficult as they are to quantify, delays caused by first- and third-party losses could easily put a construction firm out of business, says John Voeller, senior vice president of construction at Black & Veatch. "At a 400-megawatt powerplant, every hour that we missed the start-up date cost $60,000—and that counts up really quick on a 24-hour clock," he notes.

Costs of a Data Breach

- 2016* – Direct costs of a data breach increased due to higher detection, response and lost business numbers.
- Average cost of a data breach: $7.01 million

<table>
<thead>
<tr>
<th>Cost</th>
<th>2014*</th>
<th>2015*</th>
<th>2016*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection &amp; Escalation</td>
<td>$14</td>
<td>$20</td>
<td>$21</td>
</tr>
<tr>
<td>Notification</td>
<td>$18</td>
<td>$19</td>
<td>$18</td>
</tr>
<tr>
<td>Response</td>
<td>$55</td>
<td>$54</td>
<td>$57</td>
</tr>
<tr>
<td>Lost Business</td>
<td>$114</td>
<td>$124</td>
<td>$125</td>
</tr>
<tr>
<td>Total</td>
<td>$201</td>
<td>$217</td>
<td>$221</td>
</tr>
</tbody>
</table>

* Data indicates the release date of the report which uses data gathered from the previous calendar year.

Cyber Claims Study – NetDiligence 2014

- Average Claim Payout: $733,109 ($2.9m for large companies and $1.3m for healthcare)
- Average Claim Payout Per Record - $956

Study based on 117 claims reported by carriers and includes only payments made, not total costs of breach. NetDiligence estimates that its study represents only 5-10% of all cyber claims handled by US carriers that year.
Blurring the Lines between the Cyber World and the “Real World.”

**ThyssenKrupp**

- In December 2014, Germany’s Federal Office for Information Security reported that a steel mill had suffered “massive” damage when malware prevented the proper shutdown of a blast furnace.
- The hackers gained access by “spear phishing” – sending e-mails that appear to be from trusted source but infect computers when opened – to employees of ThyssenKrupp’s business partners, and the malware then spread to ThyssenKrupp itself and eventually to the controllers on its production line.

- Which of your equipment/systems can be controlled remotely?
- What about your client’s systems to which you have access?
- If not now, what about in 5 years?
Ponemon 2015 Cost of Data Breach Study

Factors That Reduce Breach Costs:
- Strong Security Posture
- Incident Response Plan
- Business Continuity Management (BCM)
- Chief Information Security Officer (CISO)
Cyber Coverages

- Network Security Liability
  - Claim expenses and damages emanating from network and non-network security breaches

- Privacy Liability
  - Claim expenses and damages emanating from a violation of a privacy tort, law, or regulation
  - Claim expenses and damages emanating from a violation of a law or regulation arising out of a security breach

- Privacy Regulatory Proceeding and Fines
  - Claim expenses in connection with a privacy regulatory inquiry, investigation, or proceeding
  - Damages/fines (varies by market), consumer redress fund
  - Privacy regulations fines
  - Payment Card Industry fines (varies by market)

- Privacy Event Expense Reimbursement
  - Expense reimbursement for third-party forensics costs
  - Public relations costs
  - Legal
  - Mandatory notifications (comply with security breach notification laws)
  - Voluntary notification costs
  - Credit monitoring
  - Call center

First Party Cyber Coverages

- Data/Electronic Information Loss
  - Covers the cost of recollecting or retrieving data that was destroyed, damaged or corrupted due to a computer attack.

- Business Interruption or Network Failure Expenses
  - Covers cost of lost net revenue and extra expense arising from a computer attack and other human-related perils. Coverage is especially valuable for computer networks with high availability needs.

- Cyber-extortion
  - Covers both the cost of investigation and the extortion demand amount related a threat to commit a computer attack, implant a virus, etc.

- Reputational Harm
  - Loss of business income due to loss of client/customer/contracts etc. as the result of a negative publicity event, including data/network security breach or privacy violation.
Questions
Notes
Data and systems security and privacy liability exposures (aka cyber liability) have gotten a lot of press lately, but this is not a "one size fits all" risk. These exposures and the need for insurance are pretty clear if you are a hospital, bank, or retailer, but what are the exposures for a construction firm and would they benefit by mitigating these risks through cyber insurance. Below, we discuss Construction cyber exposures and the benefits of a specialized insurance policy to cover those exposures.

Primary Cyber Exposures

Exposure of confidential corporate information—Construction firms may hold engineering and design/build information on a number of “secure” facilities and other projects that are considered critical infrastructure and, therefore, potential terrorist targets. Other sensitive corporate information could include trade secrets or other proprietary information such as manufacturing processes. The exposure of this information could lead to the following direct costs and third-party damages:

- Forensic investigation of the breach.
- Legal advice on how to respond.
- Public Relations costs.
- Claims by clients and others for the cost to redesign or reconstruct secure facilities or systems.
- Damages associated with unfair competition due to release of trade secrets.
- Defense costs associated with the third-party claims.

Breach of Network Security—If a construction firm’s employee fell victim to a scam email and clicked on a link that downloaded malicious software onto their system, the firm could suffer the following direct damages and third party liability claims:

- Lost income related to the inability to conduct business and provide services due to a systems outage.
- Damages suffered by third parties that interact with a construction firm’s system caused by the transfer of that same malicious code from the construction firm’s systems to the claimant company’s systems.
- Loss of confidence by clients and potential loss of repeat business/reputational damage. (Not covered by traditional cyber insurance but available as a specialized stand-alone cover)
Construction Firms

Contractual Requirements

Construction firms will likely see more and more contracts requiring some kind of cyber (data security and privacy) insurance, given the increase in regulatory requirements in this area. Here are just a few examples of this heightened regulatory activity:

- In February of 2014, NIST released its cyber security framework as part of President Obama’s executive order designed to strengthen the cyber security of U.S. critical infrastructure. The executive order indicates that cyber insurance will play an important role in this initiative. As a result, many entities that are considered critical infrastructure are requiring cyber insurance in their service provider contracts.

- In 2013, the U.S. Department of Health and Human Services (“HHS”) released the final rule modifying the HIPAA Privacy, Security, and Enforcement Rules, and the HITECH Act’s breach notification rule relating to protected health information (“PHI”). This final rule broadens the definition of Business Associates (BA) (those businesses that provide services to healthcare companies) and makes those BAs directly responsible for HIPAA compliance. As a result, more and more companies are being asked to sign BA agreements and many of those agreements now contain cyber insurance requirements.

- On October 13, 2011, the Securities and Exchange Commission (SEC) issued disclosure guidance for cyber risks. The purpose of the guidance is to alert companies to types of cyber risks and events that should be disclosed to investors in a company’s public filings. One of the listed disclosures is the identification of relevant insurance coverage purchased by the company to address its exposures.

Professional Liability Coverage

How does a cyber insurance policy interact with and supplement a construction firm’s professional liability (PL) insurance?

- A cyber loss, if covered by the PL policy, would be subject to the self-insured retention which is often very high for construction firms and would be a large out-of-pocket expense for the firm.
- A cyber loss, if covered, would also erode the PL limits available for construction professional liability claims, and subsequently impact the professional liability loss-ratio and potentially, the premium.
- Cyber insurance is relatively inexpensive compared to the cost of PL insurance and usually contemplates much lower deductibles.

To trigger coverage under the construction firm’s PL policy, there must be an alleged wrongful act in the conduct of professional services. Construction firms could be liable for data or network security breaches even in the absence of a wrongful act and the incident will not always be in connection with the provision of professional services for others (a breach of employee information, for instance).

Cyber policies will often cover a breach regardless of allegations of wrongful conduct, so long as the firm was responsible for safeguarding the information breached. Furthermore, there is no requirement that the breach be connected to professional services.

Direct costs incurred by a construction firm in responding to a breach are not covered by the PL policy and include some of the following potentially costly expenses:

- IT forensic investigation of the breach.
- Legal advice on responding to the breach.
- Public relations costs.

Purchasing a cyber policy, gives the construction firm access to the resources provided by the cyber insurance company which include:

- Pre-vetted breach response vendors at discounted rates such as
Breach coach privacy attorneys.
> IT forensic firms.
> Public relations specialists.

Available Limits, Retention and Premiums

The cyber insurance marketplace is growing and there are over 20 carriers now offering various cyber products. Primary limits can be as high as $25m with towers of over $100m in coverage. Retentions can be as low as $5,000 but the larger the risk the higher the retention. Premiums vary widely depending on the size and complexity of the risk, the coverages offered and the limits and retention. Premiums can be as low as $5000 per $1m in limits or even lower.