Cyber Risk for the Construction Industry

Date: 20 September 2018
Agenda

1. Cyber Exposures in the Construction Industry
2. Overview of Cyber Insurance and the Insurance Markets
3. Cyber Incident Prevention and Incident Response
4. Key Takeaways
5. Q&A
6. Additional Information
Cyber Exposures in the Construction Industry
Brian J. Hunt, CPA, CRIS, CBCP
Why Should I Worry About Cyber Exposures

- Cyber crime will cost companies roughly $6T USD per year on average through 2021

- According to Forester, 75% of construction, engineering and infrastructure companies were impacted by a cyber-incident in the past 12 months
Is Technology in Construction Just a Fad??

“Eighty percent of construction firms report they are having a hard time filling hourly craft positions that represent the bulk of the construction workforce, according to the results of an industry-wide survey released today by Autodesk and the Associated General Contractors of America (AGC). Association officials said shortages pose a significant risk to future economic growth and they released a new workforce development plan to solve the growing problem.

…Technology can help bridge this gap, and more firms are bringing training in-house to implement digital strategies such as building information modeling, or BIM, to ease staffing challenges and train the next generation of industry professionals.”

Source: 2018 Associated General Contractors of America (AGC) Association report
Overview of Cyber Coverage for Construction Industry

- As the construction industry becomes more connected through internet-connected solutions and remotely accessible systems it creates more opportunities for hackers to launch a cyberattack:
  - Building Information Modeling (BIM)
  - Telematics
  - Project management software

- Any company who utilizes email or internet for business is at risk for a cyber event.

- Attackers are growing increasingly sophisticated, and are targeting companies like those in Construction who believe they are safe.
How is Cyber Theft Done?

- **Social engineering** - In the context of information security, refers to *psychological manipulation* of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. The term "social engineering" as an act of psychological manipulation of a human, is also associated with the social sciences, but its usage has caught on among computer and information security professionals.
  
  - e.g. Phishing – The fraudulent attempt to obtain sensitive information such as usernames, password and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication

- **Ransomware** - A type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a *ransom* is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.
  
  - In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as Ukash and cryptocurrency are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

*Source: Wikipedia*
Overview of Cyber Coverage for Construction Industry

- Construction firms have access to a wealth of information that might be desirable to hackers.
  - intellectual property
  - proprietary assets
  - architectural drawings / specifications
  - building schematics or blueprints
  - more.

- Construction firms have valuable details on their clients (e.g., corporate banking and financial account information) each which are prime targets for attack.

- Construction firms are frequently targeted with spear phishing campaigns looking to gain access to employee information such as full names, Social Security numbers and bank account data used for payroll.

- Hackers often go after general contractors and subcontractors as a means to gain access to clients’ networks.
Construction Trailers are not Ft. Knox

- With multiple stakeholders using mobile devices (e.g. phones, laptops), there are increased access points to networks

- Valuable technology (e.g., laptops) is often found and accessible on jobsites in unsecured trailers
Industry Instances of Cybercrime

- Turner Construction was the victim of a spear phishing scam in March 2015
  - employee sent tax information on current and former employees to a fraudulent email account.
    * spear phishing is an email scam targeted at a specific individual, business or organization
    * the information provided to the fraudulent email account included full names, Social Security numbers, states of employment and residence as well as tax withholding data for 2015.
    * all employees who worked for the company in 2015 were affected by the data breach.

- Baltimore-based Whiting-Turner Contracting may have also been the victim of a data breach.
  - The company was notified by an outside vendor that prepared W-2 and 1095 tax forms for the company’s employees about suspicious activity on that vendor’s systems.
Think You Are Immune?

**Company Size:** $200M in Corporate Program per year & $100-150M in Projects per year

- Large Civil/General Construction company in a Gulf Coast state
- Hackers took total control of all systems (Email both internal & external, payroll, phones, accounting, etc.) and demanded $250k in Bitcoin
- After months of negotiating, ended up paying $150k in Bitcoin to get their systems back
- Client was emailing on personal gmail accounts
- Multiple NOC’s went out as client didn’t have access to Accounting and could not pay premiums
- Total Downtime = 2.5 – 3 Months
- Client rejected Cyber before IRMI, declined the Cyber meeting with the markets at IRMI, and rejected coverage at Renewal
  - *They were hacked roughly 2-3 weeks later*
The Regulatory Environment

- The jurisdictional requirements vary across countries with multinational businesses likely to have to comply with multiple cybercrime or data breach measures.

- In the **United States** for example, class action lawsuits are typically launched in the aftermath of a data breach.

- The convergence of physical and technical security brings greater challenges to the construction industry organizations. If the cause of a cyber breach is traced back to a construction partner as evidenced by the Target breach, the consequences can be dire.

- Good cybersecurity can be an enabler to businesses in today’s interconnected and ever increasingly connected world and therefore, adapting a business focused and proactive approach to cybersecurity risk management will reap wider benefits rather than simply offer protection to previously unaddressed risks.

- **Construction firms** should instill and maintain discipline in adhering to their risk-governance framework and policies. They are likely to benefit from continuous monitoring of the evolving threat landscape, and from adopting a nimble approach toward managing cyber risk.
Is It Covered?

- John Smith, controller for Big Old Construction, gets an email from the company’s CFO, Jane Doe.
- Jane sends instructions to John to send $10M USD to an account in Geneva to complete a deal that the Board has authorized.
- At first glance, John sees nothing out of the ordinary with the word pattern in the e-mail and the email address looks correct.
- John sends the funds in accordance with Jane’s wishes.
- Upon Jane’s return to the office, John realizes the e-mail was a hoax.

*Is the loss of $10M USD covered by Big Old Construction’s cyber policy?*
Overview of Cyber Insurance and the Insurance Markets

Joseph Salazar
2018 situation: Rising cyber threats and increased complexity

Now more than ever, organizations are relying on interconnected technology solutions and an IT organization to ensure their functionality. With this reliance on technology and need for automation, enhanced cybersecurity and risk transfer are essential. As quickly as technology advances, the threat landscape evolves faster.

Understanding your risks, and charting a plan to mitigate exposures, will protect your company, your revenue, and foster business continuity.
Cyber Risk Impacts All Loss Quadrants

Any major cyber event will result in:
- Public relations, response, and continuity costs
- Immediate and extended revenue loss
- Restoration expenses
- Defense costs

Third parties will seek to recover:
- Civil penalties and awards
- Consequential revenue loss
- Restoration expenses

Physical damage is possible:
- Property damage
- Bodily injury

Physical damage may cascade to others:
- 3rd party property damage
- 3rd party bodily injury
Global Cyber Insurance Marketplace - 2018

Aon Client Premium Spend

- Domestic: 74%
- London: 20%
- Bermuda: 6%

**Domestic**
- AIG
- Allianz
- Arch
- Argo
- Aspen
- At-Bay
- AXIS
- AWAC
- BCS
- Beazley
- Berkley
- Berkshire Hathaway
- Cap Specialty
- Chubb
- CNA
- Coalition
- CV Starr
- Great American
- NAS
- Nationwide
- Navigators
- Hartford
- HCC
- Hiscox
- Huntersure
- Liberty/Ironshore
- MunichRe
- QBE
- RLI
- RSUI
- Safety National
- SCOR
- Sompo
- Swiss Re
- Travelers
- Validus
- XL-Catlin
- Zurich

**London**
- AIG
- Allianz
- Amlin
- Amtrust
- Ascent
- Aspen
- Argo
- Aviva
- AXA
- Axis
- Barbican
- Beazley
- Brit
- CFC
- Chubb
- Emergin Risk
- Hannover Re
- HDI Gerling
- Hiscox
- Liberty
- Markel
- Munich Re
- Navigators
- Neon/Tarian
- Nirvana
- QBE
- Sciemus
- SCOR
- Swiss Re
- Talbot
- Tokio Marine Kiln
- WRB
- XL-Catlin
- Zurich

**Bermuda (Excess only)**
- AIG
- Chubb
- Markel
- Argo
- Aspen
- AWAC
- AXIS
- Sompo
- Iron-Starr
- XL-Catlin

Aon Risk Solutions | Global Sales & Marketing Support
Proprietary & Confidential
### Q3 2018 Market Snapshot

**Capacity**
- Over 75 unique Insurers providing E&O / Cyber Liability capacity
- Capacity is available the United States, London and Bermuda
- Growing number of Insurers developing appetites for large, complex risks
- There is over $700M in theoretical capacity available in the E&O/Cyber market place

**Coverage**
- Coverage breadth continues to expand
- Insurers continue to differentiate their offerings with new or enhanced coverage components
- Emphasis on pre-arranged vendors
- Broadening systems failure and contingent business interruption coverage solutions

**Claims & Losses**
- Increased ransomware activity and business interruption concerns
- Complexity of breaches has driven an increase in incident response expenses incurred by Insureds
- Claims and loss data has expanded coverage offerings and improved actuarial data for loss modeling purposes
- Increasingly punitive legal and regulatory environment

**Retentions**
- Retentions of all levels are available in the market, but can vary greatly based on industry class, size and unique exposures
- Adjusting retentions can lead to increased coverage and/or pricing flexibility

**Pricing**
- Average premium rates reflect a decline – however dependent upon underwriting and scope of coverage
- Excess rate environment continues to be competitive
- Some Insureds have secured significant coverage improvements as a result of paying higher premiums

**Note:** This is a general summary and could vary based on client industry and size

---

*Proprietary & Confidential*
2018 Purchasing Trends by Industry

Limit increases at renewal

- Companies in a number of industries, including financial institutions, hospitality, healthcare, retail, manufacturing, technology, media and transportation, are seeking higher limits options
- For other industries, many organizations are still evaluating the purchase of cyber insurance or use of their captive to provide cyber cover due to regulatory, contract, D&O, benchmarking / loss information and financial statement pressures, among other reasons

More new buyers

- Manufacturing, critical infrastructure, pharmaceutical / life sciences, industrials & materials / automotive, public sector, energy / power and utilities, higher education, real estate / construction, agribusiness and transportation / logistics industries saw the biggest uptick in new cyber insurance purchases in 2018
- Major concern in these industries is business interruption loss and reliance on technology

Shifting focus on cyber risk exposures

- In prior years, organizations’ primary cyber concern was related to privacy breaches
- In 2018, more clients across all industries have focused on business interruption coverage, including system failure cover, cyber extortion and digital asset restoration
- Cyber insurance cases where courts upheld denial of coverage demonstrate the critical importance of matching customized policy wording to specific insured cyber exposures
The reality

$2.4M+
average cost malware attack spend\(^1\)

$11.5B+
annual increase in ransomware damage costs by 2019\(^2\)

6B+
records exposed in the first half of 2017\(^3\)

60%
of all cyberattacks last year struck SMBs\(^4\)

\(^1\)Source: 2017 Ponemon, 2017 Cost of Cybercrime Study
\(^2\)Source: 2017 Cost of Cybercrime Study to 2017 CSO Magazine Cybersecurity Business Report
\(^3\)Source: Data Breach Trends - First Six Months of 2017, Risk Based Security, July 2017
\(^4\)Source: Keeper Security and Ponemon Institute, June 2016. 2017 Cost Of Cyber Crime Study, Ponemon Institute and Accenture, September 2017
Market Standard Cyber Coverages Overview

- Network Business Interruption
- System Failure
- Dependent Business Interruption / System Failure
- Cyber Extortion
- Digital Asset Restoration

- Privacy and Network Security Liability
- Privacy Regulatory Fines and Penalties
- Media Liability
- PCI Fines and Penalties
- Breach Event Expenses
Scope of Cyber Insurance Coverage

• **Network Business Interruption** - Reimbursement coverage for the insured for lost net income caused by a network security failure, as well as associated extra expense. Retention and waiting periods are negotiable.

• **System Failure** - Expands coverage trigger for business interruption beyond computer network security failure to include any system failure.

• **Dependent Business Interruption/Dependent System Failure** - Reimbursement coverage for the insured for lost income caused by a network security failure of a business on which the insured is dependent, as well as associated extra expense. Retentions and waiting periods are negotiable.

• **Cyber Extortion** - Reimbursement coverage for the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat.

• **Digital Asset Restoration** - Reimbursement coverage for the insured for costs incurred to restore, recollect, or recreate intangible, non-physical assets (software or data) that are corrupted, destroyed or deleted due to a network security failure.
Scope of Cyber Insurance Coverage

- **Privacy and Network Security Liability** –
  - Privacy Liability: Liability coverage for defense costs and damages suffered by others for any failure to protect personally identifiable or confidential third-party corporate information, whether or not due to a failure of network security. Coverage may include: unintentional violations of the insured’s privacy policy, actions of rogue employees, and alleged wrongful collection of confidential
  - Security Liability: Liability coverage for defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, unauthorized use, denial of service attack or transmission of a computer virus

- **Privacy Regulatory Fines and Penalties** - Liability coverage for defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and/or a failure of network security. Coverage includes fines and penalties where insurable by law. Compensatory damages, i.e. amounts the insured is required by a regulator to deposit into a consumer redress fund, may be covered

- **Media Liability** - Liability coverage for defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy. The scope of covered media is variable and can range from the insured’s website only to all content in any medium

- **PCI Fines and Penalties** - Coverage for a monetary assessment (including a contractual fine or penalty) from a Payment Card Association (e.g., MasterCard, Visa, American Express) or bank processing payment card transactions (i.e., an “Acquiring Bank”) in connection with an Insured’s non-compliance with PCI Data Security Standards

- **Breach Event Expenses** - Reimbursement coverage for the insured’s costs to respond to a data privacy or security incident. Policy triggers vary but are typically based on discovery of an event, or a statutory obligation to notify consumers of an event. Covered expenses include computer forensics expenses, legal expenses, costs for a public relations firm and related advertising to restore your reputation, consumer notification, call centers, and consumer credit monitoring services
Cyber Incident Prevention and Incident Response
Jeffrey Shaffer
The Battleground
IDS, IPS, Threat Intel, SIEM, SOC, Awareness, IR Plans, Visibility, IoT, Mobile, AI, Malware RE
The adversaries

What’s most at risk?

- Nation States
  - Industrial Control Systems (SCADA)
  - Payment card and related information / financial transactions
- Hacktivists
  - Emerging technologies
  - Advanced materials and manufacturing techniques
- Insiders
  - R&D and / or product design data
  - Business deals, strategy and M&A information
- Organized Crime
  - Healthcare, pharma. and related technologies
  - Health records PHI and other personal data
- Insiders
  - Also: Nuisance activity and more like DDOS and CPU usage to mine BitCoin
Board and C-Suite Concerns

As high profile cyber attacks become more common, executive management teams and boards are deeply concerned:

- Is the business resilient to a cyber attack?
- Are there gaps in our cyber security capabilities?
- About which threats should we be most concerned?
- How much risk are we willing to take?
- Could a cyber incident impact our business?
- Are we spending in the right areas?

The Board needs to be confident that they have a “defensible” cyber security risk management program in place.

- Increasing demands from customers/business partners due to third party risk management initiatives
- Increasing demands from investors for insight into the management of risk in companies
- Increasing complexity in regulations, and requirements, relating to cyber security practices, and focus of regulatory examinations
- Continued outsourcing of information technology (e.g., cloud service providers) and security operations leading to greater complexity in risk management
Yahoo’s Top Lawyer Resigns and C.E.O. Marissa Mayer Loses Bonus in Wake of Hack

The Panama Papers are: 11.5 million leaked documents detailing financial and attorney-client information for more than 214 offshore entities

Who Is Ultimately Accountable When a Big Breach Happens?

Where Is Your Sensitive Information stored? Where Is It Going? How does it get there?
## Threat Actors and their Motives

<table>
<thead>
<tr>
<th>Threat Actor</th>
<th>Motive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation States</td>
<td>Steal Intellectual Property</td>
</tr>
<tr>
<td>Financially Motivated Hackers</td>
<td>Monetize Personal Data</td>
</tr>
<tr>
<td>Hacktivists / Terrorists</td>
<td>Trigger Damages Flowing from a Data Breach</td>
</tr>
<tr>
<td>Insiders</td>
<td>Destroy or Corrupt Data</td>
</tr>
<tr>
<td></td>
<td>Disrupt Services</td>
</tr>
<tr>
<td></td>
<td>Bragging Rights</td>
</tr>
<tr>
<td></td>
<td>Advance Political Agenda</td>
</tr>
<tr>
<td></td>
<td>Insider Trading, Short Selling</td>
</tr>
<tr>
<td>Security Researchers</td>
<td>Expose Sensitive Data</td>
</tr>
<tr>
<td></td>
<td>Extortion</td>
</tr>
</tbody>
</table>
A little of what I have seen

Don’t be next

- Large retail store gets phished with C2. $6Million
  - Response, Remediation, Rebuild

- IT Company sees threat actor for 4, no wait, 15 months, takes no action.
  - Monitoring is not useful without response
  - Resource allocation and interoperability

- Threat actor was in environment of a large tech company for 5 years
  - Threat Intelligence, IDS and thorough forensics

- Software security controls physical components
  - Internet of Things hacking vs. ICS

- 100 mobile apps, 21 permissions and more
  - Mobile visibility and control

**Cyber security is not a wall, it should be a malleable 360° bubble**
Common Stages of a Breach Lifecycle

1. INFRINGEMENT
2. PRIVILEGE ESCALATION
3. LATERAL MOVEMENT
4. DATA AGGREGATION
5. DATA EXFILTRATION

A breach detected in 30 days saves $1 million.
Average breach cost $3.8 million. Up 6.4% from 2017
Biggest motive? $$$$$$$
**Mobile and IoT in the Enterprise – EMM, MDM, MCM, MAM**

- Touch points and carriers
- IoT – Synching with everything
- Jump technology
- Medical devices – Injectable, Implantable, Wearable, Injectable
- Operates on both sides of your firewall
- Able to circumvent security controls with Bluetooth, NFC, WiFi, etc.
- Drones, AI, Robotics, Infotainment, Telematics
- Many applications use HTTP only
- Users and 5 generations

- 30% of apps access to contact information
- 30% of apps access GPS information
- 31% of apps access calendar information
- 39% of apps access smartphone’s microphone
- 75% of apps access the camera
- 34% of mobile com is not encrypted
- Business apps 3X ore likely to leak log in creds
- Soc. Media apps 3x more likely to expose pw’s
- 60K apps added to store/month
The Internet (more or less)

2018 Crowdstrike Report
Cyber Resilience Solutions Framework Services

**Assess**
- Security Architecture Assessment
- Security Controls Assessment
- Security Maturity Assessment
- Compliance Readiness Assessment
- Security Risk Assessment
- Security Strategy Assessment
- IR Readiness Assessment
- M&A Due Diligence Assessment
- Third-Party Risk Assessment
- Privacy Compliance Assessment
- Cyber Framework Assessment

**Improve**
- Security Strategy Development
- Security Controls Optimization
- IR Planning & Playbook Development
- Information Security Policies & Standards Development
- Security Design & Architecture
- SOC Optimization
- Cyber Threat Simulations/Tabletops
- Third Party Cyber Risk Management
- CISO Advisory
- Board Advisory
- Compliance Program Development
- Insider Risk Program Development
- Secure Software Development Lifecycle
- Security Training & Awareness

**Quantify**
- Cyber Insight
- Cyber Impact Analysis
- Risk Financing Decision Platform (RFDP)
- CyberMetrica
- Cyber Portfolio Aggregation Analysis

**Respond**
- Incident & Breach Response
- Reversing Malware
- Digital Evidence Preservation
- Expert Witness Testimony
- Claims Advocacy
- Complex Cyber Loss Preparation

**Test**
- Red Team Security Testing
- Social Engineering Testing
- Application Security Testing
- Network & Cloud Penetration Testing and Configuration Review
- Source Code Security Review
- Threat Hunting

**Transfer**
- Cyber Insurance
- Aon Cyber Enterprise Solution
- Insurance Program Review
- Proprietary Peer Benchmarking
- Global Broking Center
- Aon Client Treaty
- Aon Benfield Reinsurance Capacity

Aon Risk Solutions | Global Sales & Marketing Support
Proprietary & Confidential
World Class Talent Drawn From Top Organizations

1. British Army - The Intelligence Corps
2. U.S. Department of the Air Force
3. U.S. Postal Inspection Service
5. U.S. Marshalls Service
6. Federal Bureau of Investigation
7. U.S. Internal Revenue Agency
8. Financial Services Authority
10. U.S. Security & Exchange Commission
11. U.S. Federal Trade Commission
12. U.S. Department of Justice
13. Office of Special Investigations
14. U.S. Secret Service
Key Takeaways
Hope is NOT a Plan
Additional Information
Risk Management 101

Thursday, October 4 2018
Royal Oaks Country Club
7915 Greenville Avenue  |  Dallas, Texas 75231
CPE for Texas CPA's - 9.5 hours

Topics Covered
- Property
- Automobile Liability
- Certificates of Insurance
- Workers Compensation
- Texas Non-Subscription
- General Liability/Umbrella
- Management Liabilities
- Cyber-security
- Environmental
- Surety
Contact Information

brian.hunt@aon.com

joseph.salazar@aon.com

jeffrey.shaffer@aon.com