Why Cybersecurity Matters to the Ready Mix Concrete Industry

NRMCA Annual Convention
Las Vegas, NV
March 5, 2016

Audience Poll

- Does your business have an Internet connection?
- Do you use email?
- Do you store confidential information electronically?
- Are you part of a small, medium, or large business?
- Do you have a cybersecurity policy?

Today's Presentation

<table>
<thead>
<tr>
<th>Presenter</th>
<th>Company</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oliver Brooks</td>
<td>Why Cybersecurity Matters</td>
<td></td>
</tr>
<tr>
<td>Brandon Williams</td>
<td>Recent Case Studies</td>
<td></td>
</tr>
<tr>
<td>Ken Cook</td>
<td>Implications of a Breach</td>
<td></td>
</tr>
<tr>
<td>Carrie Heisler</td>
<td>Best Practices and Preventative Measures</td>
<td></td>
</tr>
</tbody>
</table>

Why Cybersecurity Matters

- "A future hot target for attacks – how construction companies can improve" (Construction Dive News 8/11/16)
- "60% of small firms that suffer a cyber attack are out of business within 6 months" (Denver Post 10/23/16)
- "If you spend more on coffee than on IT security, you will be hacked" (Richard Clarke, Cybersecurity Expert)

A Constant Headline

Are We Next?

- Yahoo!
- Target
- Turner
- LinkedIn
- Hyatt
- Sony
A Constant Threat…

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Sends viruses usually through email attachments</td>
</tr>
<tr>
<td>Phishing</td>
<td>Requests your data through disguised links</td>
</tr>
<tr>
<td>Password Attacks</td>
<td>Cracks your password</td>
</tr>
<tr>
<td>Denial-of-Service</td>
<td>Disrupts and cripples your network</td>
</tr>
<tr>
<td>Man in the Middle</td>
<td>Impersonates people and websites you know</td>
</tr>
<tr>
<td>Drive by Download</td>
<td>Downloads malware from a trusted site</td>
</tr>
<tr>
<td>Malvertising</td>
<td>Unleashes malicious codes when you click on ad</td>
</tr>
<tr>
<td>Rogue Software</td>
<td>Poses as legitimate software updates</td>
</tr>
</tbody>
</table>

…With Many Entry Points

Case Study:

Entry Point: Phishing email to HR employee
- Spoofed the “From” field to trick the target
- Employee replied with sensitive information

Information Obtained:
- Employee names
- Earnings
- Social Security #’s
- Residence
- Tax data

Implications:
- Company-wide breach
- Affected all employees employed in 2015
- Significant cost

Phishing Scams
- $3.7 million annual average cost
- rgabini@nrmca.com vs. rgabini@nmca.com
- @amazons.com vs. @amazon.com
- 156 million phishing emails are sent each day

Targeted Information

Employee:
- Name and address
- Earnings
- Beneficiaries
- Taxes

Customer:
- Credit cards
- Demographics
- Logins

Trade Secrets:
- Customer lists
- Pricing and plans
- Intellectual property

Financial:
- Account numbers
- Financial records

Implications of Data Breach
- Likely public relations nightmare
- Loss of trust
- Employees, customers and vendors
- Loss of business
**Implications of A Breach**

**Financial Impact**
- Average Cost:
  - $4 million globally
  - $7 million U.S.
  - ~$221 per each sensitive record compromised

**What makes up these costs?**
- Employee terminations
- Outside consultants
- Loss of business ($3.97/record)

Source: Ponemon Institute

**Implications of A Breach**

**Transportation Sector**
- ~$129 per each record (transportation industry)
- Average of 29,611 records compromised during 2016

An "average size" attack could replace your next acquisition!

**Potential Business Impact**

Less than 1,500 hacked records can cost as much as 1 ready mix truck

**Protecting Your Assets**

**Technical**
- Firewalls
- Security software
- Server back ups
- Data encryption

**Training & Prevention**
- Employee training
- External resources
- Incident response

**Policy & Culture**
- Written policy
- Password protection
- Being alert

**IT Led**
**Management Led**

**Where Can Senior Managers Focus?**

**Recommendation**
- Reinforce a culture of tight cybersecurity
- Support mandatory training
- Ban thumb drives
- Limit access to sensitive data
- Support a strong password policy

**Rationale**
- Most boards of directors think cyber security is a threat
- Management support is key
- Creates awareness
- Many carry viruses and malware
- Reduces risk exposure
- Most common passwords are easy to hack

Source: Paul McGillicuddy

**Most Common Passwords**

(Based on 2015 data)
- 123456
- password
- 12345
- 12345678
- qwerty
- 1234356789
- 1234

There are only two different types of companies in the world: those that have been breached and know it, and those that have been breached and don’t know it.

Ted Schlein, Venture Capitalist

Source: Paul McGillicuddy

**Ensuring Strong Passwords**

- Create password 10 characters or longer
- Include uppercase & lowercase letters, numbers, and symbols
**Key Takeaways**

- Cyber security threats are real and common
- Our industry and smaller firms are facing more targeted attacks
- It's important to know your exposure and customize your security policy accordingly
- Third-party security firms provide expertise

**Thank You**