Build It, and They Will Come: 
Data Security for the Construction Industry

Ilan Ramsey – Member 
Stites & Harbison PLLC – Louisville, Kentucky 
iramsey@stites.com

Stephen Oakes, Special Agent 
Federal Bureau of Investigation-Louisville, Kentucky 
seoakes@fbi.gov
CONSTRUCTION SITE OF THE FUTURE

CONNECTED

BIM 360

SITE SENSORS

COMMUNITY

EQUIPMENT

COLLABORATIVE

CLIENTS & DESIGNERS

BUILDING PRODUCT

WORKERS

DELIVERY

INTEGRATED SUPPLY CHAIN

COORDINATED
CONSTRUCTION SITE OF THE FUTURE

- Connected
- Site Sensors
- Community
- Equipment
- Workers
- Building Product
- Delivery
- Collaborative

BIM 360™
## Daily Mobile Device Usage

<table>
<thead>
<tr>
<th>Device</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>78.4%</td>
</tr>
<tr>
<td>Tablet</td>
<td>53%</td>
</tr>
<tr>
<td>Smartphone</td>
<td>76.8%</td>
</tr>
<tr>
<td>Wearable</td>
<td>11.1%</td>
</tr>
</tbody>
</table>

From the 2017 ConTech Report published by [JBKnowledge](https://www.jbknowledge.com)
Dedicated IT Department

2017
- We have a dedicated IT department: 49.6%
- We outsource a portion of our IT: 30.1%
- We have staff with IT responsibilities but not a dedicated department: 21.9%
- We outsource all IT: 19.5%
- Other: 1.9%

2014
- Yes: 58.9%
- No: 41.1%

2016
- Yes: 57.4%
- No: 42.6%

From the 2017 ConTech Report published by JBKNOWLEDGE®
Why Knowledge Matters

Survey Participants

• Estimator 27.8%
• Project Manager 24.6%
• Executive (CEO, CIO, CFO) 24.4%
How Much of Annual Sales Volume are Companies Spending on IT?

- Less than 1%: 46.4% (2017), 55.9% (2016)
- 1%: 14.1% (2017), 21.8% (2016)
- 2%: 10% (2017), 7% (2016)
- 3%: 3.6% (2017), 2.8% (2016)
- 4%: 1.1% (2017), 1% (2016)
- 5%: 2% (2017), 2.2% (2016)
- 6%: 1% (2017), 0.2% (2016)
- +7%: 1.8% (2017), 1.9% (2016)

I don't know: 12.8% (2017), 14.8% (2016)

From the 2017 ConTech Report published by JBKNOWLEDGE.
How can your client have effective data security when on average almost 90 percent are spending less than 5 percent of sales on IT?
Inserts for Agent Oakes
ABA Model Rule 1.6

*Client-Lawyer Relationship*

Rule 1.6 Confidentiality Of Information

- (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

- (c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
Chief Information Security Officer

The CISO identifies and implements with the CIO and CPO security measures to protect the Firm’s data assets by developing a security program that is designed to inhibit, detect, and respond to threats. The CISO advises on data risk issues, measures to mitigate risk, and recommendations for policies, procedures, and training. The CISO, with the assistance of the CIO and CPO, responds to, investigates, and remediates data security incidents. The CISO also assists in the review and negotiation of vendor contracts, requests for proposals, audits or other internal Firm administrative functions concerning data security and supports data security initiatives across all departments.

Chief Privacy Officer

The CPO serves as the Firm’s HIPAA Privacy Official with defined responsibilities under the Firm’s Information Security Policies, which include reviewing and negotiating business associate agreements, receiving and responding to allegations of HIPAA violations, and analyzing and documenting breach notification obligations. In addition, the CPO provides counsel to staff and attorneys regarding the firm’s HIPAA business associate obligation to Firm clients and collaborates with the CIO and CISO on security education and training, security notices, audits, and incident response. In addition, the CPO serves as a resource to align HIPAA requirements with Firm security policies and practices.

Chief Information Officer

The CIO aligns technology with the business needs of the Firm. The CIO is responsible for the IT Department, all IT staff, budgets, and day to day oversight of all technology needs to insure secure and uninterrupted data service to the Firm. The CIO is also responsible for setting the Firm’s short and long-term goals concerning software and equipment needs.
Methods of Securing Cloud Data

- Employee Training: 66.7% (2017), 54.9% (2016), 45.4% (2015)
- Corporate IT Policy: 45.9% (2017), 30.1% (2016), 24.3% (2015)
- Cyber Liability Insurance: 27.7% (2017), 22.5% (2016), 9.4% (2015)
- Cross-Platform Authentication: 14% (2017), 8.4% (2016), 8.7% (2015)
- Cloud Liability Insurance: 10.1% (2017), 5.1% (2016), 2.6% (2015)
- None: 12.3% (2017), 18.2% (2016), 23.1% (2015)
- I don't know: 9.5% (2017), 16.4% (2016), 20.1% (2015)
- Other: 1.3% (2017), 1.3% (2016), 1.3% (2015)

From the 2017 ConTech Report published by JBKNOWLEDGE
Law Firm Data Breaches

Mossack Fonseca: Panamanian Papers
Cravath Swaine & Moore LLP
Weil Gotschal & Manges LLP
DLA Piper

Jason Shore, Coinbul LLC v. Johnson & Bell, Ltd.
  technology sophisticated client
  red flag warnings
  withdraw as counsel
  judgment against client
  lawsuit follows
How much does it cost for your Clients and your Lawfirm?

Audit/Consulting
Customer Acquisition
Legal Compliance
Lost Business
Ponemon Institute 2017 Data Breach Study: Global Analysis/Impact of Business Continuity Management

- Average of 47% hacks or malware with average cost per record of $170 (down $14)
- Human error and negligence $128 average cost per record (down $5)
- System glitches and errors $126 average cost per record (down $12)
- United States average cost per record is $225, India by comparison is $64
- With an incident response team the cost reduces by $19 per record and with a 3rd party causing the breach it increases $17 per record
- United States organizations paid the highest price for losing customers from a data breach at $4.13 million
How Do You Reduce the Dollar Value of a Breach?

- Proactively be involved in projects about data security—from contract to completion.
- Plan for data security budgets that provide real long-term value and are not patches to get by for now.
- Train on data security and all other variables—avoid the expense of “negligence”.
- Get proper insurance coverage.
- Segmenting and Encrypting Key Information, i.e., separate and protect personally identifiable information or other highly valuable company information.
- Have an Incident Response Team and Incident Response Plan.
- Implement and Enforce Vendor Management Controls.
- Draft Data Loss Policies and Enforce those policies.
- Back-up systems and review the quality of that information regularly.
Data Security Minimums

- Designate an employee to maintain security program
- Anticipate and limit risk by:
  - Employee Training
  - Compliance
  - Detection and Prevention of system failures
- Imposing disciplinary measures for violations
- Preventing Access by Terminated employees

- Contractually require service providers to maintain security
- Limit and control physical access
- Monitor and Review Effectiveness and Compliance
- Document All Responses to Incidents
- Mass. 201 CMR 17
<table>
<thead>
<tr>
<th>Ranking</th>
<th>Password</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>ranking unchanged since 2016 list</td>
</tr>
<tr>
<td>2</td>
<td>password</td>
<td>ranking unchanged</td>
</tr>
<tr>
<td>3</td>
<td>12345678</td>
<td>up 1</td>
</tr>
<tr>
<td>4</td>
<td>qwerty</td>
<td>up 2</td>
</tr>
<tr>
<td>5</td>
<td>12345</td>
<td>down 2</td>
</tr>
<tr>
<td>6</td>
<td>123456789</td>
<td>new</td>
</tr>
<tr>
<td>7</td>
<td>letmein</td>
<td>new</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
<td>Unchanged</td>
</tr>
<tr>
<td>9</td>
<td>football</td>
<td>down 4</td>
</tr>
<tr>
<td>10</td>
<td>iloveyou</td>
<td>new</td>
</tr>
<tr>
<td>11</td>
<td>admin</td>
<td>up 4</td>
</tr>
<tr>
<td>12</td>
<td>welcome</td>
<td>unchanged</td>
</tr>
<tr>
<td>13</td>
<td>monkey</td>
<td>new</td>
</tr>
<tr>
<td>14</td>
<td>login</td>
<td>down 3</td>
</tr>
<tr>
<td>15</td>
<td>abc123</td>
<td>down 1</td>
</tr>
<tr>
<td>16</td>
<td>starwars</td>
<td>new</td>
</tr>
<tr>
<td>17</td>
<td>123123</td>
<td>new</td>
</tr>
<tr>
<td>18</td>
<td>dragon</td>
<td>up 1</td>
</tr>
<tr>
<td>19</td>
<td>passw0rd</td>
<td>down 1</td>
</tr>
<tr>
<td>20</td>
<td>master</td>
<td>up 1</td>
</tr>
<tr>
<td>21</td>
<td>hello</td>
<td>new</td>
</tr>
<tr>
<td>22</td>
<td>freedom</td>
<td>new</td>
</tr>
<tr>
<td>23</td>
<td>whatever</td>
<td>new</td>
</tr>
<tr>
<td>24</td>
<td>qazwsx</td>
<td>new</td>
</tr>
<tr>
<td>25</td>
<td>trustno1</td>
<td>new</td>
</tr>
<tr>
<td>Password</td>
<td>Time taken to crack</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------</td>
<td></td>
</tr>
<tr>
<td>Strong</td>
<td>instantly</td>
<td></td>
</tr>
<tr>
<td>looksstrong</td>
<td>10 days</td>
<td></td>
</tr>
<tr>
<td>LooksStrong</td>
<td>59 years</td>
<td></td>
</tr>
<tr>
<td>L00ks5trOng</td>
<td>412 years</td>
<td></td>
</tr>
<tr>
<td>Th!sL00ks5trOng</td>
<td>157 billion years</td>
<td></td>
</tr>
<tr>
<td>Th!sL00ks5trOng:-)</td>
<td>3 quintillion years</td>
<td></td>
</tr>
</tbody>
</table>
Biggest DATA BREACHES of the 21st century

- Equifax: 143m
- Adult Friend Finder: 412.2m
- Anthem: 78.8m
- eBay: 145m
- JP Morgan Chase: 76m
- Home Depot: 56m
- Yahoo: 3b
- Target Stores: 110m
- Adobe: 38m
- US Office of Personnel Management (OPM): 22m
- Sony's PlayStation Network: 77m
- RSA Security: 40m
- Heartland Payment Systems: 134m
- TJX Companies, Inc.: 94m

Source: csoonline.com
Ransomware
Skimming
Business Email Compromise

- Vector is stolen credentials and/or malware, or email from a spoofed or similar domain

- Compromised systems monitored and/or Files scanned for invoices/accounts payable

- Snooping or surveillance may be conducted On executives and/or their staff

- Impersonation of executives may be executed by way of email, voice, call-forwarding, and/or fax
Business Email Compromise

- The FBI (IC3) received 298,728 cyber crime and fraud complaints in 2016 with reported losses in excess of $1.3 Billion - BEC was the No. 1 cause of loss.

- BEC Global *Exposure* - Over $5 Billion (since 2013)

- BEC Reports - All 50 States & 131+ countries

- BEC From January 2016 - June 2017:
  - Attempted $222,890,660
  - Successful $148,059,454 (66%)
Business Email Compromise

Mules are Acquired Online through Social Engineering and Fake Job Postings on:

- Social Media
- Legitimate Job Boards
- Fake Job Boards
- Radio Advertising
- Romance scams on Dating Sites
- Other Social Engineering
BEC Exercise

Hello,

See the attached, it's important.

Regards,

Your Boss
BEC Exercise
BEC Exercise
Please check this out before the presentation tonight. We need to leave in 10 minutes.

Zachary Smith  
Federal Bureau of Investigation  
Louisville Division  
(502) 263-6000
Microsoft Office 2013

To display the contents of the document click on Enable Content button.

Microsoft Office 2010

To display the contents of the document click on Enable Content button.
Financial Fraud Kill Chain

Minimum $50,000

International Transfer

<72 Hours Since Wire Transfer Initiated

FBI, USSS, FINCEN, NCFTA, FS-ISAC
Financial Fraud Kill Chain Con’t.

- Minimum $50,000
- Summary of the Incident:
- Victim Name:
- Victim Location (City, State):
- Originating Bank Name:
- Originating Bank Account Number:
- Beneficiary Name:
- Beneficiary Bank:
- Beneficiary Account Number:
- Beneficiary Bank Location (if available):
- Intermediary Bank Name (if available):
- SWIFT Number:
- Date:
- Amount of Transaction:
- Additional Information (if available) - including “FFC” - For Further Credit; “FAV” – In Favor
Questions?