CYBERSECURITY: BEST PRACTICES AND RISK MITIGATION STRATEGIES

PRESENTED BY:

MICHAEL CAMACHO, PARTNER, CPA, CIA
KEVIN RICCI, PRINCIPAL, MCSE, CISA, CRISC, QSA
AGENDA

• Emerging Trends in Cybersecurity
  • Latest Cyber Trends
  • Industry Specific Trends
  • What we’re seeing – stories from the trenches

• The Path to Cybersecurity Awareness
  • Understanding your risk
  • Developing a plan
  • Effective plan execution

• Addressing Key Cybersecurity Risks in the Construction Industry

• Q & A
Everyone’s a Target
THE STATS:

Average Cost per Record Stolen: $150/record
(up from $148 in 2018)

Average Number of Records lost per Breach:
25,575 records

Average Days to Detect Breach: 206
(up from 191 days in 2018)

Average Days to Contain Breach: 73
(up from 66 days in 2018)

Average cost of a breach is 39.5% higher when a Company is not prepared

Further Reduction in Cost when Automated Security Solutions are in Place: 8%
THE STATS:

- Average Cost per Breach: $3.92M (up from $3.86M in 2018)
- Percentage of Breach Cost from Loss of Business: 36%
- Average Cost per Breach per employee +25,000 Employees: $204/employee
- Average Cost per Breach per employee 500-1000 Employees: $3,523/employee
- Breach Cost Allocation by Year:
  - Year 1: 67%
  - Year 2: 22%
  - Years 3+: 11%
- Likelihood of recurring breach: 29.6% (up from 27.9% in 2018)
Statistics: Global

- 5 billion records were lost, stolen, or exposed in 2018
- There is a cyber attack every 39 seconds
- 43% of cyber attacks target small businesses
- 91% of breaches are the result of phishing attacks
Statistics: What We’re Seeing

• Incidents/Breaches TRAC has responded to in 2019:
  • 16

• Average business downtime during a breach:
  • One to two weeks (longest just over a month)

• Average cost of breach response:
  • $75,000 for TRAC breach response services
  • Exponentially higher for downtime, legal fees, tech expenditures, etc.

• Hackers are industry agnostic:
  • Entertainment company
  • Salt Company
  • Law Firm
A&E / Real Estate / Construction

• Lower end of spectrum for risk now, but industry profile is changing
  • Increased use of internet-connected solutions
  • More information stored in cloud
  • Increasing use of wireless devices

• Higher likelihood of incidents occurring from breach of “Human firewall”

• Hackers not just focused on direct financial gain

• Compliance element could be significant
  • Non-compliance can impact your ability to meet customer contract requirements
A&E / Real Estate / Construction

- Regulations that may apply:
  - PCI DSS
  - State and Local Privacy Laws and Regulations
    - California Consumer Privacy Act
  - CUI
  - HIPAA
  - GDPR

- WAYS A DATA BREACH CAN HURT YOUR COMPANY:
  - Breach Response and Technology Expenditures
  - Legal and Forensic Costs
  - Fines and Penalties
  - Inescapable Reputational or Brand Damage
A&E / Real Estate / Construction

- Industry Examples:
  - Turner Construction
  - Whiting-Turner Contracting
  - Two of the 16 breaches we responded to involved a company in the Construction industry
QUESTIONS FOR THE AUDIENCE

• Do you believe Cybersecurity is a significant risk to your business?

• For those who say “YES”, how many of you have developed a plan to address Cybersecurity risk as it relates to your business?

• For those who have a plan, have you dedicated funds to execute that plan?
The Path to Cybersecurity Awareness

- Understanding your company’s cybersecurity risk
- Developing a plan to address identified risks
- Executing the plan

Identify → Protect → Detect → Respond → Recover

Recover → Identify → Respond → Protect → Detect

Identify → Protect → Detect → Respond → Recover

Recover → Identify → Protect → Detect → Respond
Understanding Your Risk

- Perform a Risk Assessment
  - Internally or through a 3rd party (can provide you external validation of your concerns)
  - Multi-functional – Consider all functions/departments
  - Focus on:
    - What critical information/data you may have
    - Should the information/data be protected? Is it required?
    - Where is the information/data kept?
    - How is it protected?
    - Who is responsible for protecting it?
    - How is protection monitored?
- Understand which risks are applicable to your company which could impact the security of your information/data
Develop a Plan to Address Risks

- Prioritize identified risks – High / Moderate / Low
- Develop action plans to address each risk.
- Assign roles and responsibilities for each action plan
- Establish timeline for executing action plans – should align with risk ranking
Execute Plan

- Requires support (both facially and through funding) from the top
- Must monitor timeline to ensure timely completion of milestones
- Review/approval process should be in place to ensure plan execution addresses risk, both design and operating effectiveness
- Reassess / reevaluate on periodic basis
Addressing Key Cybersecurity Risks - Construction Industry

- Spear Phishing
- Lack of Employee Education
- Mobile / Wireless Device Management (IoT)
- Lack of Encryption
- Insufficient Logical Security (Password) Controls
- Lack of Cloud Controls
- Other:
  - Lack of Monitoring (Automated or Otherwise)
  - No Consideration of Compliance Requirements
  - No Cyber Insurance
Spear Phishing

• Phishing has evolved into spear phishing
• The email appears safe but has a sinister purpose
• Awareness and education are the best weapons against this threat
• Consequences of a Spear Phishing Attack:
  – Betrayal of sensitive information
  – Transferal of funds
  – Facsimile of a website
  – Ransomware
Ransomware

• A mechanism for digital extortion
• A victim typically has 72 hours to pay
• Hundreds of millions of attacks
• Can hit mobile devices
Spear Phishing

- The key question to ask when receiving an email that asks you to provide sensitive information, click a link or open an attachment:

  Did you expect this email from this sender at this time?
Email Usage

• Do not open email attachments from an unknown sender or that you are unfamiliar with

• Hover before you click
  — www.Safe.com

• Don’t rely on the sender’s address
  — KRICCI@YOURBUSINESS.com
  — KRICCI@YOURBUSINESS.com
In addition to spear phishing, attackers will also use other modes of social engineering:

- **SMiShing** is an attack via text message
- **Vishing** is an attack via a phone call
Passwords

• A critical first line of defense
• The longer and more complex the password, the better
• Never share or write down your password
Encryption

• Closest thing to a silver bullet
• Passwords are not the same as encryption
• Included for free with business versions of Microsoft Windows
Event Logs

• Logs provide the raw data needed for intrusion detection and prevention
• Benefits of a SIEM (security information and event management) solution over manual log monitoring
• Critical for forensics after an incident
Mobile Devices

• Be cautious when installing apps
• Enable a password
• Avoid free Wi-Fi
Remote Access

- Login credentials
- Protecting laptops/tablets when travelling
- Secure networks
- Multi-factor authentication
Social Media

• Implement a social media policy for your business
• Educate your employees
• Restrict any social media sites that are not used for business purposes
• Consider post-separation agreements
#HAMBURGLAR

BURGER KING® USA official Twitter account. Just got sold to McDonalds because the whopper flopped =[ FREDOM IS FAILURE mcdonalds.com In a hood near you • info.bk.com/press/sold-to-...
Cloud Backups

• Compliance requirements
• Obtain a SOC 2 Report
• Plan for rain!
Work with your legal and insurance contacts to make sure you have the necessary level of cyber insurance in the event of an attack or data breach.
Education

- Critically important – end users are often your weakest security link!
- Provide security training during the onboarding process
- Provide your staff with an annual security training
- Provide additional focused training to anyone with direct contact with PHI, PII, or other sensitive information
- Have employees sign a document that they acknowledge the security policies
<table>
<thead>
<tr>
<th>Category</th>
<th>Indicator</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Operations</td>
<td>Staffing</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>IT policies and procedures</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Steering committee</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Security event history</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Network Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Web filtering</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Email filtering</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Email encryption</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Firewall and antivirus</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Wireless security</td>
<td>Down</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Entrance security</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Access tracking</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Environmental controls</td>
<td>Down</td>
</tr>
<tr>
<td>Logical Security</td>
<td>User ID assignments</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>User ID review</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>Password strength</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Password change frequency</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Handling of terminated users</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Network equipment passwords</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Automated login requirement</td>
<td>Up</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>Policies</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Phone and tablet security</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Laptop security</td>
<td>Down</td>
</tr>
<tr>
<td>Recovery</td>
<td>Policies</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Backup power</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Redundant ISP</td>
<td>Down</td>
</tr>
<tr>
<td>System and Hardware Controls</td>
<td>RAID configurations</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Online Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cloud data policies</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Cloud data backups</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>Cloud data security</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Website policies</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Website backups</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Website security</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Social media policies</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Privacy and Security Compliance</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>PHI policies and security</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>PHI training</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>PHI breach response plan</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>PHI policies and security</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>PHI training</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>PHI breach response plan</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>PCI DSS policies and security</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>PCI DSS training</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>PCI DSS breach response plan</td>
<td>Up</td>
</tr>
</tbody>
</table>
# The Score Report

**SCORE Report** - Hot Spots

**ABC Company**

Security, Compliance, and Operations Risk Evaluation

## Data Privacy and Security Compliance

<table>
<thead>
<tr>
<th>Section</th>
<th>Issue</th>
<th>Risk</th>
<th>Solution</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIH Training</td>
<td>There is no formal training in place to provide guidance regarding</td>
<td>As a business that maintains PIH, the Company is required to comply</td>
<td>Provide periodic security and privacy training to all employees that covers best practices on</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>the protection of personally identifiable information (PIH).</td>
<td>with state security and privacy regulations e.g. Massachusetts's</td>
<td>protecting PIH.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>data security regulations 201 CMR 17.1 requirements. These</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>regulations typically require, among other things, ongoing employee</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>training on the proper use of the computer system and the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>importance of PIH. Lack of training could result in significant</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>fines while also hindering employees from making good security</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>decisions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIH Breach Response Plan</td>
<td>There is no formal response plan in place to provide remediation</td>
<td>Without a set of periodically tested breach response procedures in</td>
<td>Document all PIH breach response policies and procedures, with detailed descriptions and action</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>steps in the event of a personally identifiable information (PIH)</td>
<td>place, the response may not be organized and the remediation time</td>
<td>steps. Test to the fullest extent possible, the plan on an annual basis. Update the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>data breach.</td>
<td>may be significantly extended.</td>
<td>documentation as policies and procedures change.</td>
<td></td>
</tr>
<tr>
<td>PCIDSS Training</td>
<td>There are no formal policies or training in place to provide</td>
<td>This is a requirement of PCIDSS v3.1. In the event of a data breach,</td>
<td>Complete the requirements of the PCIDSS SAQ that addresses the needs of the regulations</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>guidance regarding the protection of cardholder data.</td>
<td>lack of such policies and training would result in the</td>
<td>surrounding the care of cardholder data. Update the documentation as policies and procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>organization being considered not in compliance with the PCIDSS and</td>
<td>change and submit on an annual basis. Provide periodic training to all employees on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>could result in significant fines and penalties. It also</td>
<td>importance of protecting cardholder data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hinders employees from making good security decisions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCIDSS Breach Response Plan</td>
<td>There is no formal response plan in place to provide remediation</td>
<td>Without a set of periodically tested breach response procedures in</td>
<td>Document all PCIDSS breach response policies and procedures, with detailed descriptions and</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>steps in the event of a cardholder data breach.</td>
<td>place, the response may not be organized and the remediation time</td>
<td>action steps. Test to the fullest extent possible, the plan on an annual basis. Update the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>may be significantly extended.</td>
<td>documentation as policies and procedures change.</td>
<td></td>
</tr>
<tr>
<td><strong>THE SCORE REPORT</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>If your employees utilize a remote connectivity solution such as a VPN, is two-factor authentication required?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Do you perform viability testing on your backups on a periodic basis?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>In addition to providing cybersecurity awareness training to the all employees, do you also provide training to all new hires before they start?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Do each of your IT consultants sign a non-disclosure agreement?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Are all of your workstations running operating systems that are more recent than Microsoft Windows 7?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**THE SCORE REPORT**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does a member of senior management receive key procedures and credentials from your IT consultant or internal IT team on a periodic basis?</td>
<td></td>
</tr>
<tr>
<td>If your business accepts credit card payments, are you compliant with the Payment Card Industry Data Security Standards (PCI DSS)?</td>
<td></td>
</tr>
<tr>
<td>Do you have system information and event manager (SIEM) in place to monitor logs?</td>
<td></td>
</tr>
<tr>
<td>Are all of your servers running operating systems that are more recent than Microsoft Windows Server 2008?</td>
<td></td>
</tr>
<tr>
<td>Do you perform penetration testing on your IT environment on a periodic basis?</td>
<td></td>
</tr>
</tbody>
</table>
## THE SCORE REPORT

<table>
<thead>
<tr>
<th>Number of “YES” Answers</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td><img src="image1" alt="Risk Level" /></td>
</tr>
<tr>
<td>7-9</td>
<td><img src="image2" alt="Risk Level" /></td>
</tr>
<tr>
<td>4-6</td>
<td><img src="image3" alt="Risk Level" /></td>
</tr>
<tr>
<td>1-3</td>
<td><img src="image4" alt="Risk Level" /></td>
</tr>
</tbody>
</table>
CyberSecure

Where you turn in the event of a data breach

Does your organization have the RESOURCES and TRAINING in place to quickly recover from the devastating effects of a data breach? Can your employees IDENTIFY and AVOID spear phishing, the cause of more than 90% of data breaches?

If not, you need CYBERSECURE, your cybersecurity resource and breach recovery solution.
It’s not a matter of if... it’s a matter of when you will be breached!”
LEADERSHIP TEAM

Michael Camacho  
CPA, CIA  
Partner  
(401) 421-4800 x233  
mcamacho@citrincooperman.com

Dr. Suzanne H. Miller, Ph.D.  
CHS-III, CISA, CISM, CRISC, QSA  
Principal  
(401) 421-4800 x273  
smiller@citrincooperman.com

Kevin Ricci  
CISA, MCSE, CRISC, QSA  
Principal  
(401) 421-4800 x278  
kricci@citrincooperman.com

Matt Wagenknecht  
CISSP, CREA, CEH  
Director  
(401) 421-4800 x352  
mattw@citrincooperman.com
QUESTIONS?

Michael Camacho
mcamacho@citrincooperman.com

Kevin Ricci
kricci@citrincooperman.com