CIS Controls, the Building Blocks of Organizational Cybersecurity

Independent Bankers of Colorado Convention 2019
RACHAEL SCHWARTZ

Rachael has been an IT consultant for financial firms for more than 9 years. Prior to joining CSI, she worked with some of the largest hedge funds and private equity funds in New York City as an IT and cybersecurity consultant. She now lends her expertise to community banks, helping them maximize their technology investments and increase security while reducing their operational burdens.

Email: Rachael.Schwartz@csiweb.com
Cell: 720-676-9175
LinkedIn: linkedin.com/in/reschwartz/
Top 5 Corporate Data Breaches

- Yahoo (2013-2014) – 3 Billion Accounts
- Marriott/Starwood (2018)- 500 Million Accounts
- Friend Finder Network (2016)- 412 Million Accounts
- Equifax (2017)- 146 Million Accounts
- eBay (2014)- 145 Million Accounts
ARE WE GETTING ANY BETTER AT PROTECTING OURSELVES AND OUR DATA?

<table>
<thead>
<tr>
<th>Cybercrime</th>
<th>Estimated Daily Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious scans</td>
<td>80 billion</td>
</tr>
<tr>
<td>New malware</td>
<td>300,000</td>
</tr>
<tr>
<td>Phishing</td>
<td>33,000</td>
</tr>
<tr>
<td>Ransomware</td>
<td>4,000</td>
</tr>
<tr>
<td>Records lost to hacking</td>
<td>780,000</td>
</tr>
</tbody>
</table>

Table 1. Estimated daily cybercrime activity
WHAT WE WILL COVER TODAY:

• What is a Cybersecurity Framework
• What are the CIS Top 20 Controls
• Why use the CIS Controls as Your Cybersecurity Framework
• Deeper dive into the top 6 Basic Controls
WHAT IS A CYBERSECURITY FRAMEWORK?

• Guide to help organizations focus cybersecurity efforts and spend

• Common Frameworks
  • NIST (National Institute of Standards and Technology)
  • ISO 27000
  • CIS (Center for Internet Security)
  • Cybersecurity Assessment Tool (sort of)

• How to Choose the Right Framework for your Organization
WHY IS A CYBERSECURITY FRAMEWORK IMPORTANT?

- Rooted in best practices
- Holistic security
- Compliance and regulatory satisfaction
- Methodology for strategic planning
WHY THE CIS CONTROLS?

Risk Reduction

Responsive to Changes

Proven Track Record

Budget Friendly

Variety of Expert Input

FFIEC Recommended

User-Friendly
TOP 20 CIS CONTROLS LIST

1. Inventory Control of Hardware Assets
2. Inventory Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Implement a Security Awareness Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Test and Red Team Exercises
TODAY’S FOCUS AREAS

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software
6. Maintenance, Monitoring, and Analysis of Audit Logs
1. **Inventory and Control of Hardware Assets**

- Are you keeping an accurate list of hardware assets for your organization?
  - What is required when onboarding a new asset
    - Configuration
    - Inventory records
    - Tagging/Logging who is in possession of the assets
  - How do you handle/record changes
  - How do you handle/record decommission and disposal of assets
  - How do you handle lost or stolen assets
2. INVENTORY AND CONTROL OF SOFTWARE ASSETS

• Do you know what software is installed on every device that connects to your network?
• Do you control what is being installed on devices?
• Less is More (even for executives)
3. CONTINUOUS VULNERABILITY MANAGEMENT

- How often should you be scanning?
  - Vulnerability Scans
  - Penetration Tests
- Always monitor
- Patching
- Documentation
4. CONTROLED USE OF ADMIN PRIVILEGES

- What are Admin Rights?
- How to Handle Admin Rights
  - General Users
  - Executives and C-Suite
  - IT Staff
- Security vs Convenience
5. Secure Configuration for Hardware and Software

- Devices to Consider
  - Laptops
  - Workstations
  - Servers
- Standards vs Default Settings
- Security Content Automation Protocol (SCAP)
LOG MANAGEMENT AND MONITORING POLICY: A MATH EXERCISE

- 2 Million events per month per device
- A small branch has an average of 25 devices
- 25*2M = 50M events per branch per month
- Of 50M events, 6.5 require investigation
- Equal to .000013%
- Who feels confident they can manually find 7 events in 50M logs?
6. MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS

- How long can an attack go unnoticed?
- Enable Logging
- Collect Logs
- Analyze Logs
- Respond
- Log Tampering Prevention
## Foundational CIS Controls

<table>
<thead>
<tr>
<th></th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Email and Web Browser Protections</td>
</tr>
<tr>
<td>9</td>
<td>Limitation and Control of Network Ports, Protocols and Services</td>
</tr>
<tr>
<td>11</td>
<td>Secure Configuration for Network Devices, such as Firewalls, Routers and Switches</td>
</tr>
<tr>
<td>13</td>
<td>Data Protection</td>
</tr>
<tr>
<td>15</td>
<td>Wireless Access Control</td>
</tr>
<tr>
<td>8</td>
<td>Malware Defenses</td>
</tr>
<tr>
<td>10</td>
<td>Data Recovery Capabilities</td>
</tr>
<tr>
<td>12</td>
<td>Boundary Defense</td>
</tr>
<tr>
<td>14</td>
<td>Controlled Access Based on the Need to Know</td>
</tr>
<tr>
<td>16</td>
<td>Account Monitoring and Control</td>
</tr>
</tbody>
</table>

## Organizational CIS Controls

<table>
<thead>
<tr>
<th></th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Implement a Security Awareness and Training Program</td>
</tr>
<tr>
<td>19</td>
<td>Incident Response and Management</td>
</tr>
<tr>
<td>18</td>
<td>Application Software Security</td>
</tr>
<tr>
<td>20</td>
<td>Penetration Tests and Red Team Exercises</td>
</tr>
</tbody>
</table>
CONCLUSION

- Use a Framework to help guide your organization
- Start from the top and work your way down the list
- What sounds simple is much more involved than it seems
- Don’t assume IT or Vendors are following the rules
- Security vs Convenience
- Review and make changes this is an ongoing battle
QUESTIONS?

Rachael Schwartz
rachael.schwartz@csiweb.com
720-676-9175
linkedin.com/in/reschwartz