Cybersecurity
How Much Is Enough?

Tony Sager
Center for Internet Security (CIS)
Minnesota Cyber Summit, October 2018
Classic Risk Equation

\[
\text{Risk} = f \{ \text{Vulnerability, Threat, Consequence, countermeasures} \}
\]
A Lifetime of Cybersecurity Lessons

- We are not Special Snowflakes, and the Bad Guy doesn’t perform Magic
- Knowing about vulnerabilities doesn’t get them fixed
- There’s a large but limited number of defensive choices
  - the 80/20 rule applies (The Pareto Principle)
- People/enterprises don’t make security decisions
  - they make economic and social decisions
- Cybersecurity == Information Management (*not Threat Sharing*)
  - when you hear “share”, think “translate” and “execute”
- Cybersecurity is more like **Groundhog Day** than **Independence Day**
The Defender’s Dilemma

1. What’s the “right thing” to do?
   • and how much do I need to do?

2. How do I actually do it?

3. And how can I demonstrate to others that I have done the “right thing”?
Evolution of the CIS Controls

NSA/DoD Project

The Consensus Audit Guidelines (CSIS)

“The SANS Top 20” (the SANS Institute)

The Critical Security Controls (CCS/CIS)
CIS Controls Version 7
<table>
<thead>
<tr>
<th>WHAT Real People SHOULD KNOW</th>
<th>WHAT DOES IT MEAN?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anyone in organized crime (or espionage) who is not in this (cyber) ought to be sued for malpractice</td>
<td>The Bad Guys are highly motivated</td>
</tr>
<tr>
<td>Just pointing out problems doesn’t get them fixed</td>
<td>Solutions are part of a complex system of feedback, incentives, and verification</td>
</tr>
<tr>
<td>It’s hard to have a unique problem or an original thought</td>
<td>Point to existing standards, ideas, frameworks</td>
</tr>
<tr>
<td>No security snapshot will work, trust is dynamic</td>
<td>Encourage machinery, not reports; measurement, not a state (of security); good IT and Ops management</td>
</tr>
<tr>
<td>Threat Sharing is over-rated</td>
<td>Focus on translation, action, efficiency</td>
</tr>
<tr>
<td>Not every problem can be solved in the cyber domain</td>
<td>Diplomacy, economics, policy, social norms</td>
</tr>
<tr>
<td>Everybody’s role is changing (industry, government, academia, standards)</td>
<td>Less control, more about behavior; less central and top-down, more cooperative</td>
</tr>
<tr>
<td>We need better parts</td>
<td>Software quality, architectures, <strong>services</strong></td>
</tr>
<tr>
<td>We’ve hit Peak Geek in cybersecurity</td>
<td>Cyber as foundation for economic and social decision-making. Demand what you’d demand elsewhere</td>
</tr>
</tbody>
</table>
“It’s Not About The List”

• The CIS Controls Version 7
• Mappings to other Frameworks
  • Special focus on NIST CSF [updated!]
• CIS Community Attack Model
• CIS Controls Measures and Metrics [updated]
• SME Implementation Guide
• Companion Guides to the Controls [in development]
  • IOT, Cloud, Privacy, Outsourcing for Small/Medium Enterprises
• CIS Risk Assessment Method (CIS-RAM) [new]
• Website:  [www.cisecurity.org](http://www.cisecurity.org)
• Email:  [Controlsinfo@cisecurity.org](mailto:Controlsinfo@cisecurity.org)
• Twitter:  @CISecurity
• Facebook: Center for Internet Security
• LinkedIn Groups:
  • Center for Internet Security
  • 20 Critical Security Controls