Legislative Cyber Security Briefing
Introduction

Tony Sager
Center for Internet Security (CIS)
Minnesota Cyber Security Summit, October 2018
CIS Programs

CIS is a forward-thinking, nonprofit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

**CIS Benchmarks™**
Consensus-based, internationally-recognized software configuration guidelines curated by experienced IT practitioners to help assess and improve network security.

**CIS Controls™**
A prioritized set of policy-level controls that set a secure foundation for organizations around the world. Common security practices distilled into a scalable, actionable list to provide real security for real threats.

**CIS Hardened Images**
A prioritized set of policy-level controls that set a secure foundation for organizations around the world. Common security practices distilled into a scalable, actionable list to provide real security for real threats.

**MS-ISAC®**
Multi-State Information Sharing & Analysis Center®
The focal point for cybersecurity resources for U.S. State, Local, Tribal, and Territorial (SLTT) government entities. 24x7 Security Operations Center provides real-time monitoring, threat warnings, and incident response.

**Elections Infrastructure ISAC**
The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) supports the cybersecurity needs of the elections subsector. The EI-ISAC is supported by the MS-ISAC. Membership is open to all U.S. State, Local, Tribal, and Territorial government organizations that support U.S. elections and associations thereof.

**CIS Services**
Services such as vulnerability assessment, incident response, phishing exercises, and monitoring.

**CIS CyberMarket**
Purchasing program that serves SLTT governments and not-for-profit entities to improve cybersecurity through cost-effective group procurement.
“The Fog of More”

Identity Theft
Denial-of-Service Attack
Card skimming
ransomware
phishing
hackers
Man-In-The-Middle Attack
Computer viruses
Computer worms

Botnets
CEO Fraud
2 Factor Authentication

Toll fraud
Mic/Camera Hijacking
Watering hole attacks
Support Scams
Anti-malware
Anti-virus
Virtual Private Networks

Internet of Things
Black hats
Toll fraud
IRS Fraud
EMV Cards
Ad Blockers

Open Public WiFi

Support Scams

IRS Fraud
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”?
The Cybersecurity Problem

• Every type of victim: country, sector, size, individual...
• Every motivation: financial and IP theft, extortion, social control, political statements, notoriety, influence operations, “false flags”, “prep of the battlespace”....
• Attackers are efficient: information sharing, automation, very large scaling, specialization, a marketplace... (4K ransomware attacks/day)
• threat of cyber a top 3 disruption (World Economic Forum)
• Cyber threats greater than physical threats (DHS Secretary Nielsen)
• Worldwide cybercrime costs $600B/year (McAfee, CSIS)
• Expect $100B in defensive spending in 2020 (IDC)
• Y2K with real impact, and without the deadline
Small Businesses and Cyber

• 29 million small businesses - less than 500 employees (SBA)
• Over half of all attacks target them (NCSA, Symantec, DBIR, etc.)
• Over half of them report an attack or data breach in prior year
• Half have no budget allocated for risk mitigation
• Most of the data breaches are from small businesses (the Hill)
• Typical cost between $84k and $148K, 60% out-of-business 6 months later (UPS Capital)
<table>
<thead>
<tr>
<th><strong>WHAT Real People SHOULD KNOW</strong></th>
<th><strong>WHAT DOES IT MEAN?</strong></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>Almost all attacks are repeats of a type or class</td>
<td>Build a foundation before taking a “moonshot”</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, non-profits, 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, services</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>
A DC-centric View

• Legislative
  • Sharing; “hygiene”; use of commercial standards
  • Privacy (encryption policy; commercial data gathering)

• Executive
  • Regulatory approaches
  • MS-ISAC

• Market Forces
  • Compliance, “Multi-Framework Era”
  • Supply Chain management
  • Alignment with existing risk-decision models in industry
Some References

• Verizon Data Breach Incident Report:
  https://www.verizonenterprise.com/verizon-insights-lab/dbir/

• Center for Strategic & International Studies Cyber Incident List
  https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

• National Academy of Sciences: At The Nexus of Cybersecurity and Public Policy
  https://www.nap.edu/catalog/18749/at-the-nexus-of-cybersecurity-and-public-policy-some-basic