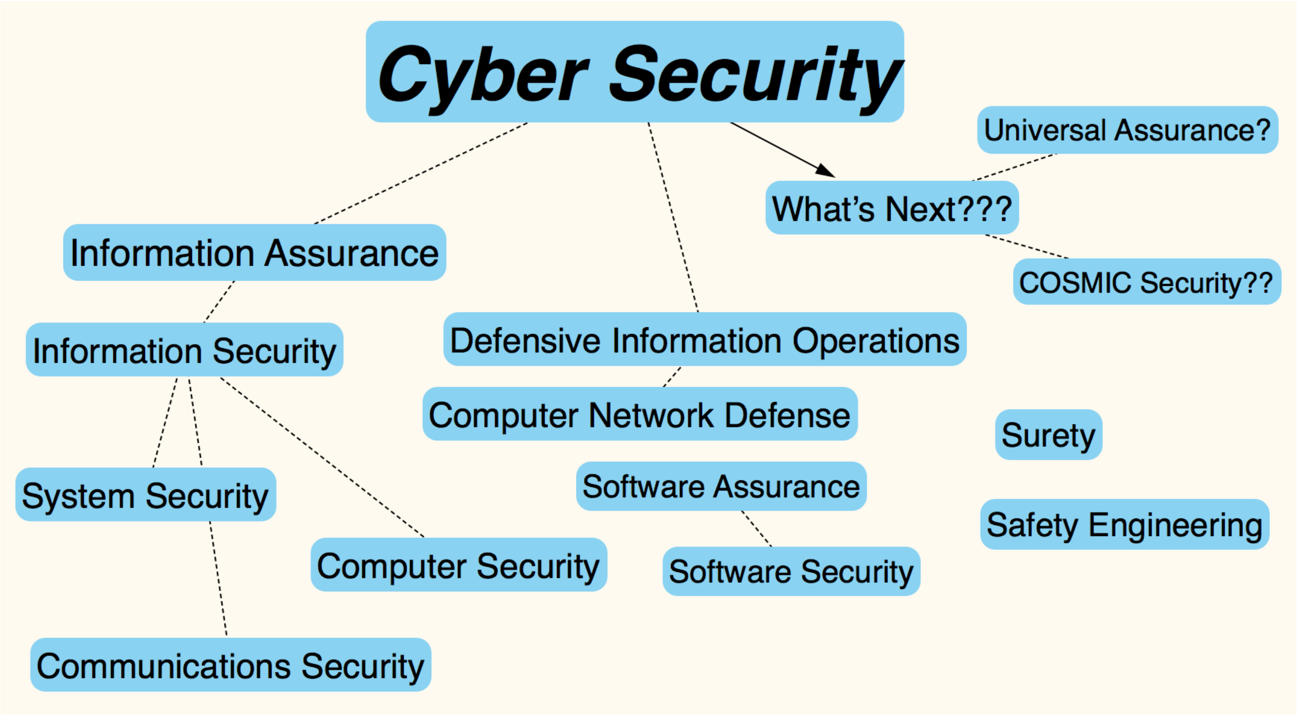
CYBER SECURITY SUMMIT 2016

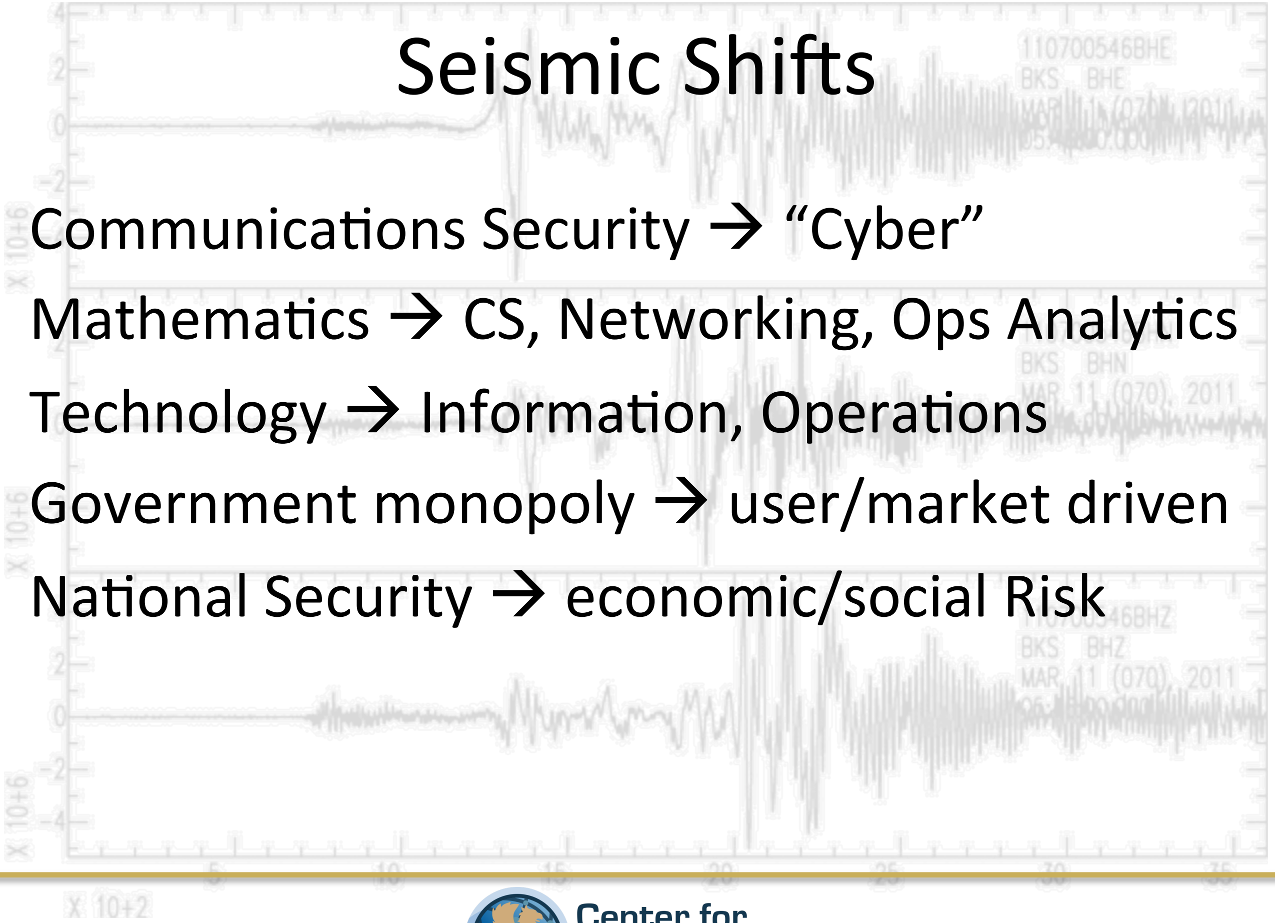
Making Best Practice Common Practice: the CIS Controls

Tony Sager, the Center for Internet Security

The Long and Winding Road….



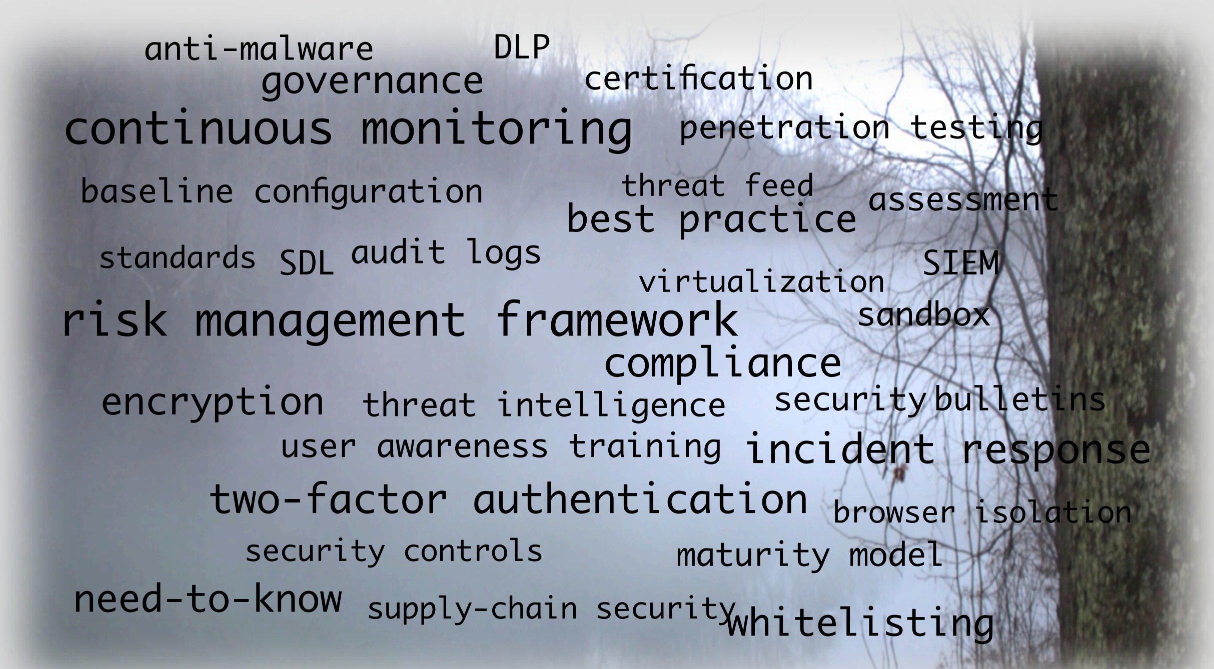
Seismic Shifts



- Communications Security → “Cyber”
- Mathematics → CS, Networking, Ops Analytics
- Technology → Information, Operations
- Government monopoly → user/market driven
- National Security → economic/social Risk

A few cybersecurity lessons

- Cybersecurity is like "Groundhog Day", not "Independence Day"
- Knowing about flaws doesn't get them fixed
- Cyber Defense == Information Management
  - ***not*** Information Sharing, ***not*** technology
  - the most important verb is ***translate***
- The Bad Guy doesn't perform magic
- There's a large but limited number of defensive choices
  - prioritization is ALWAYS required
  - and the 80/20 rule applies (The Pareto Principle)



anti-malware DLP

governance certification

continuous monitoring penetration testing

baseline configuration threat feed assessment

best practice

standards SDL audit logs SIEM

virtualization

risk management framework sandbox

compliance

encryption threat intelligence security bulletins

user awareness training incident response

two-factor authentication browser isolation

security controls maturity model

need-to-know supply-chain security whitelisting

"The Fog of More"

Center for
Internet Security®

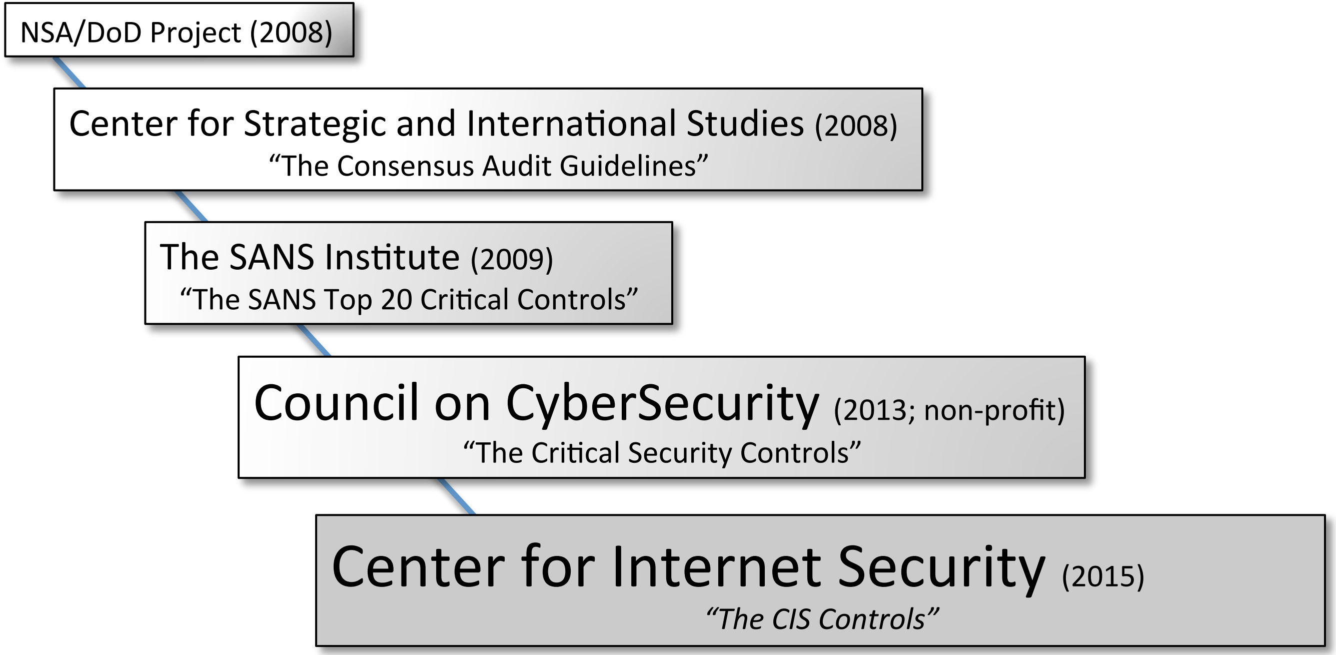
The Defender’s Dilemma

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?

from Best Practice → Common Practice

- How do we know what is "best"?
  - Based on Data? Solution to the worst problem? Trusted source?
- What is a "practice"?
  - How specific? How do I actually do it? What do I need to do this?
- What are the barriers?
  - Knowledge? Cost? Tools? Training? Enforcement? Misalignment? Repeatability?
- It takes more than a list of practices
  - Marketplace of tools, training; community-building; sharing of ideas; alignment of practices with oversight, auditing, compliance.

How did we get here?



NSA/DoD Project (2008)

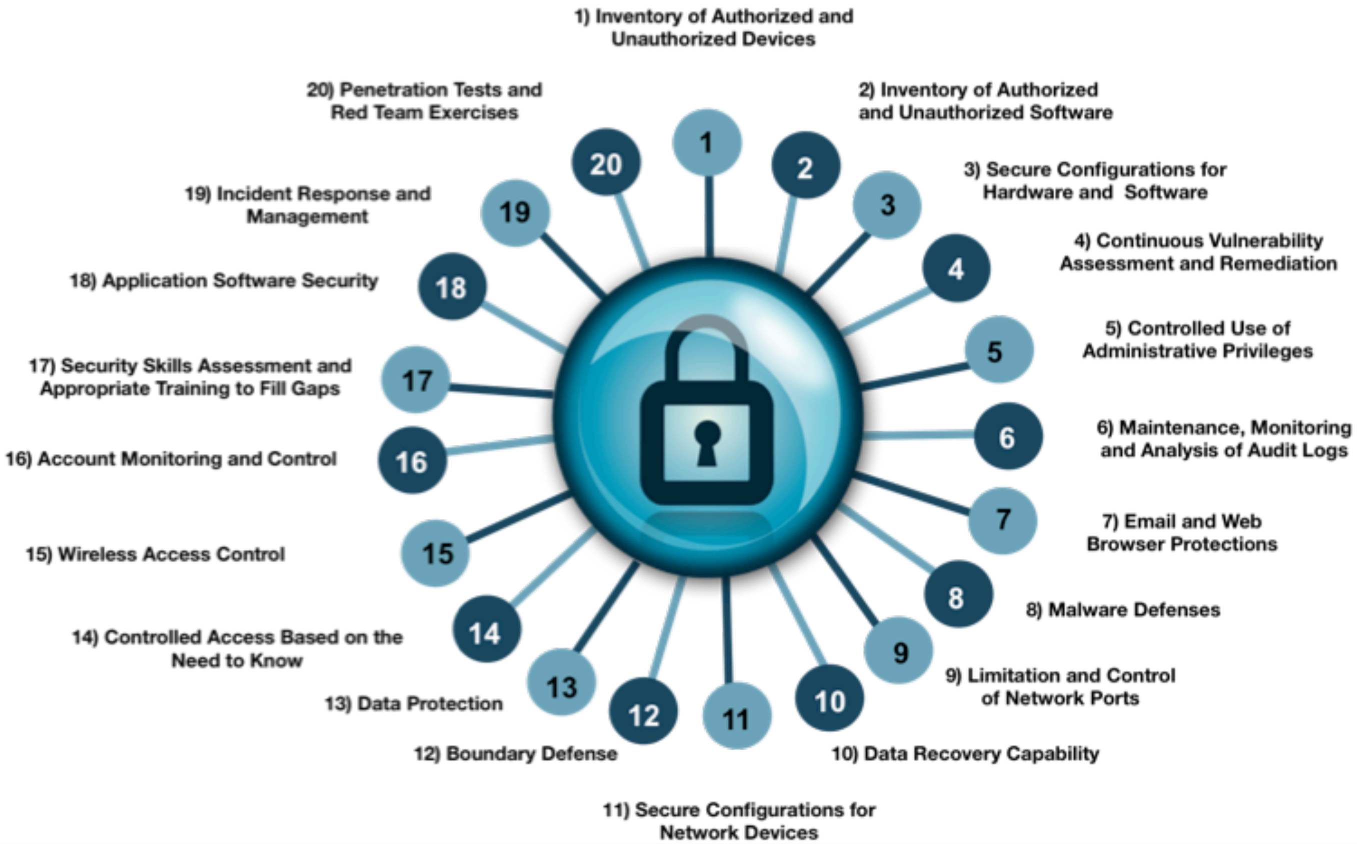
Center for Strategic and International Studies (2008)
"The Consensus Audit Guidelines"

The SANS Institute (2009)
"The SANS Top 20 Critical Controls"

Council on CyberSecurity (2013; non-profit)
"The Critical Security Controls"

Center for Internet Security (2015)
"The CIS Controls"

CIS Critical Security Controls (Version 6)



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations 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) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

Center for Internet Security®

Recent References to the *CIS Controls*

- California Attorney General's 2016 Data Breach Report
- The NIST Cybersecurity Framework
- Symantec 2016 Internet Security Threat Report
  - and Verizon DBIR, HP, Palo Alto, Solutionary…)
- National Governor's Association
- National Consortium for Advanced Policing
- Conference of State Bank Supervisors
- Zurich Insurance
- UK Critical Protection for National Infrastructure
- ENISA, ETSI

The Center for Internet Security

MS-ISAC
MULTI-STATE
Information Sharing & Analysis Center
Integrated Intelligence Center
Security Benchmarks
Trusted Purchasing Alliance
CIS CRITICAL SECURITY CONTROLS
NATIONWIDE CYBER SECURITY REVIEW
CH
National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat

Making Best Practice Common Practice

Center for Internet Security®

Contact

- Website: www.cisecurity.org
- Email: contact@cisecurity.org
- Twitter: @CISecurity
- Facebook: Center for Internet Security
- LinkedIn Groups:
  - The Center for Internet Security
  - 20 Critical Security Controls