
# Twenty Steps To Better Information Security

CORNERSTONES OF TRUST

# Personal Introduction


- Forty-six years in IT and fourteen years specializing in Information Security
- Ex-CISO for Expedia Inc.
- Ex-VP IT Operations for Hotwire
- Currently providing executive level information security professional services
- First person certified by the SANS Institute in the assessment and implementation of the Twenty Critical Security Controls

John M. Millican
Principal, The Office Of The CIO
(925) 235-0469
jmillican@oocio.com

# Twenty Critical Security Controls
## History

- In 2008 the Office of the Secretary of the Defense asked for the NSA's assistance in developing a prioritized list of security controls
- Originally designated as "For Official Use Only"
- First published by the Center for Strategic and International Studies in 2008
- Became a public/private effort in conjunction with the SANS Institute and the Center for Internet Security comprised of representatives from the military, government, industry, and educational organizations
- Stewardship turned over to the Council on Cyber Security in 2013

# Twenty Critical Security Controls
## Philosophy and Approach


- Only controls that could be shown to stop or mitigate an attack should be made a priority
- Derived from the most common attack patterns and vetted across a very broad community of government and industry
- Prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy
- Process focused – not checklists
- A strong emphasis on "What Works"
- Standardization and automation is a top priority to gain operational efficiencies while also improving security

# Real World Results

The U.S. Department of State implemented a measurement and monitoring system to gather data every 72 hours on elements of the highest priority CSCs and ranked each embassy and office on their progress in mitigating risks. They shared the ratings with the top management at the State Department. *Over 12 months, the measured risk levels across all 80,000 systems declined by 89%, and these reductions were extended and improved in the second year.* The CISO was asked to implement a broader version of his solution across the entire government and was given a large budget to make that happen.

# Components Of A Critical Security Control


- Sub-controls
  - Quick wins
  - Visibility and Attribution
  - Configuration and Hygiene
  - Advanced Measures
- Implementation Components
  - Sensors
  - Baselines
  - Tools
    - Automated
    - Scripted
- Evaluation Components
  - Criteria
  - Metrics
    - Effectiveness
    - Automated
  - Audit measures

# The Twenty Critical Security Controls
## Objectives


| 1 | 2 | 3 |
| --- | --- | --- |
| Inventory of Authorized and Unauthorized Devices | Inventory of Authorized and Unauthorized Software | Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers |
| "Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access." | "Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution." | "Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings." |

# The Twenty Critical Security Controls
## Objectives


| 4 | 5 | 6 |
| --- | --- | --- |
| Continuous Vulnerability Assessment and Remediation | Malware Defenses | Application Software Security |
| "Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers." | "Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action." | "Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses." |

# The Twenty Critical Security Controls
## Objectives

**7**
Wireless Access Control

"The processes and tools used to track / control / prevent / correct the security use of wireless local area networks (LANS), access points, and wireless client systems."

**8**
Data Recovery Capability

"The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it."

**9**
Security Skills Assessment and Training

"Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs."

# The Twenty Critical Security Controls
## Objectives

| 10 | 11 | 12 |
| --- | --- | --- |
| Secure Configurations for Network Devices such as Firewalls, Routers, and Switches | Limitation and Control of Network Ports, Protocols, and Services | Controlled Use of Administrative Privileges |
| "Detect / prevent / correct the flow of information transferring networks of different trust levels with a focus on security-damaging data." | "Manage (track / control / correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers." | "The processes and tools used to track / control / prevent / correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications." |

# Success Story

A new security manager at a mid-sized utility learned about the CSCs and saw their implementation as a way of getting his arms around the challenges and opportunities he would face in his new position. He first measured and mapped the utility's current posture in each of the 20 controls, produced an implementation score for each and charted the scores on a red/yellow/green satellite chart. He then worked out a 3-year plan to improve those scores substantially. His CIO asked him to brief the Chairman of the Board and the Executive Committee on the current status chart and the 3-year plan. The Chairman's reaction was remarkable; he said, "This is the first time a security person has made sense to me."



Source: Tarala, James, "Critical Security Controls: From Adoption to Implementation", SANS Institute, November, 2014

# The Twenty Critical Security Controls
## Objectives

| 13 | 14 | 15 |
| --- | --- | --- |
| Boundary Defense | Maintenance, Monitoring, and Analysis of Audit Logs | Controlled Access Based on the Need to Know |
| "Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data." | "Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack." | "The processes and tools used to track / control / prevent / correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. |

# The Twenty Critical Security Controls
## Objectives

**16**
Account Monitoring and Control

"Actively manage the life-cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them."

**17**
Data Protection

"The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information."

**18**
Incident Response and Management

"Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems."

# The Twenty Critical Security Controls
## Objectives


**19**
Secure Network Engineering

"Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers."

**20**
Penetration Tests and Red Team Exercises

"Actively manage (inventory, "Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker."

# Twenty Critical Security Controls
## Implementation


- Assess the current state
- Identify the gaps
- Develop a prioritized roadmap
  - Do the "First Four" first
  - Other appropriate "Quick Wins"
- Implement the first phase
- Integrate the controls into Operations
- Measure and report
- Lather, rinse, repeat

# Adoption Rates

- High levels of support for adoption
  - 26% of organizations adopting the CSCs say their top executives outside of IT are actively supporting adoption
  - 61% of those organizations say IT management above the CISO is providing support for adoption of the controls
  - 66% say the CISO, CSO or InfoSec manager is the key source of support

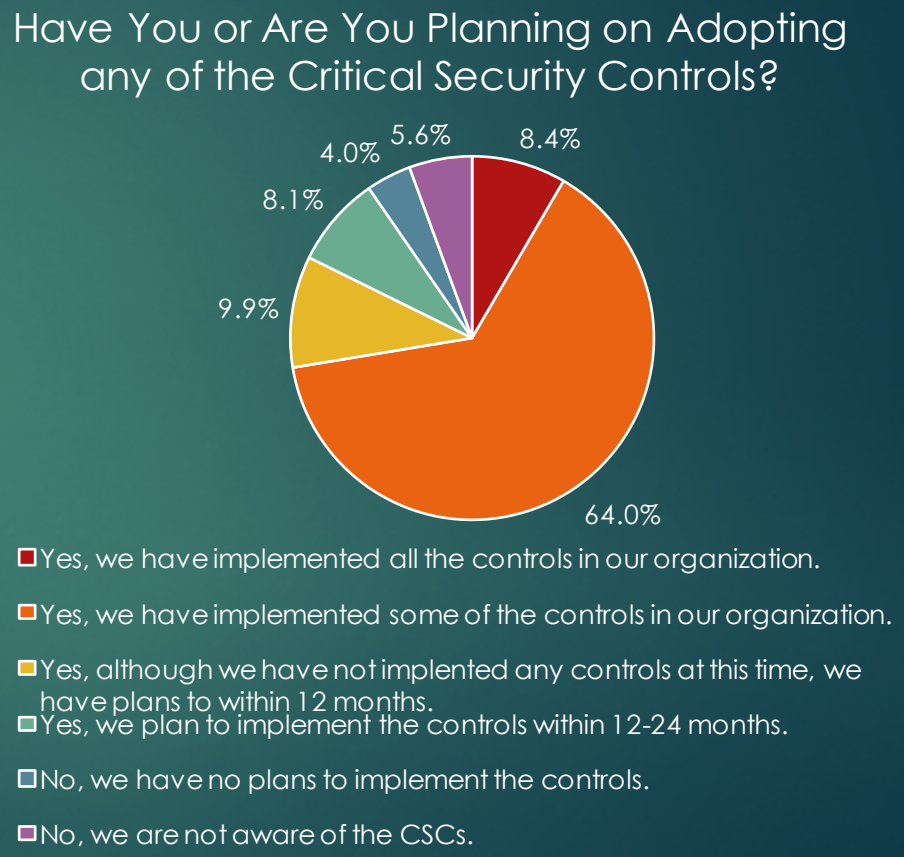


*Figure 6. State of CSC Adoption*



Source: Tarala, James, "Critical Security Controls: From Adoption to Implementation", SANS Institute, November, 2014

# Barriers To Adoption

- Barriers to adoption remain
  - 54% cite budget issues and 63% cite staffing shortages
  - 36% note operational silos while 32% point to incompatible legacy systems

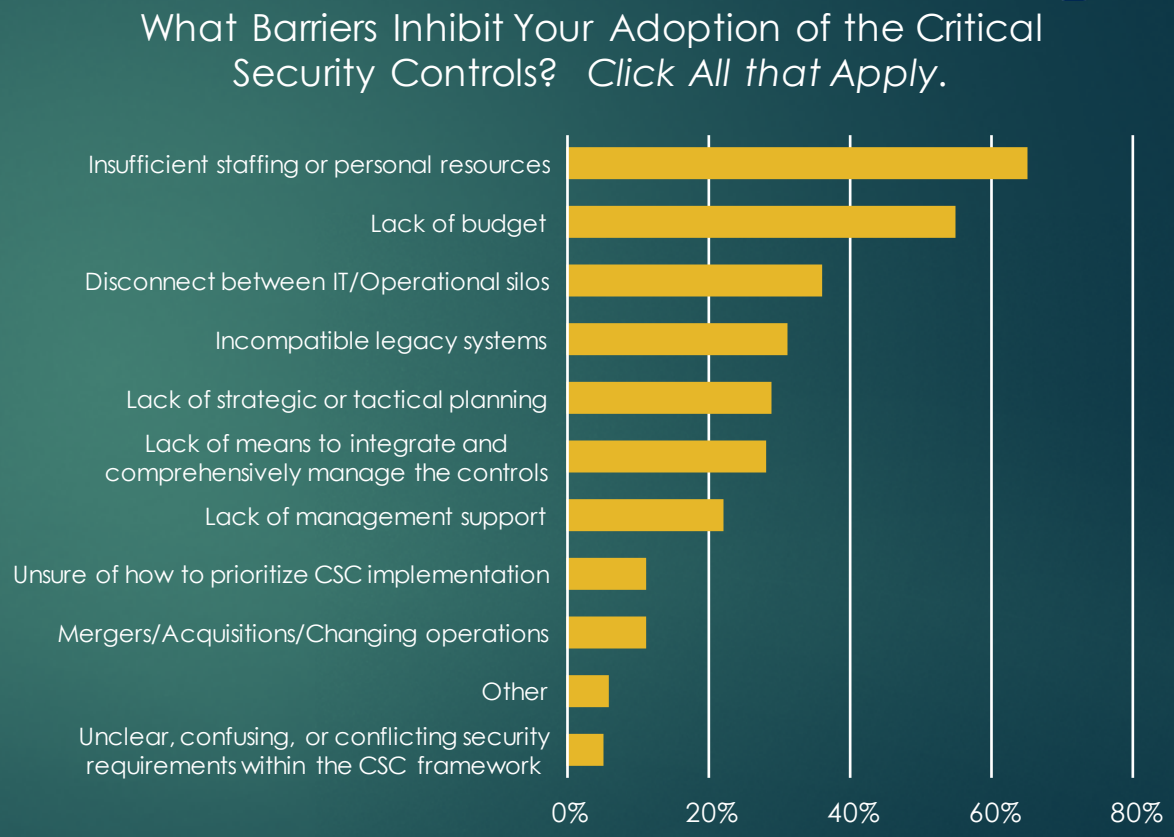




*Figure 8. Barriers to CSC Adoption*

Source: Tarala, James, "Critical Security Controls: From Adoption to Implementation", SANS Institute, November, 2014

# Most And Least Widely Adopted Controls


- Most fully adopted
  - Malware Defenses (96%)
  - Boundary Defense (94%)
- Least fully adopted
  - Application Software Security (73%)
  - Effective Security Skills Assessment And Training (73%)
  - Penetration Testing (64%)



Source: Tarala, James, "Critical Security Controls: From Adoption to Implementation", SANS Institute, November, 2014

# CSC Adoption Rates

| Rank | Critical Security Control | Partial | Full | None |
|---|---|---|---|---|
| 1 | 5: Malware Defenses | 47% | 50% | 4% |
| 2 | 13: Boundary Defense | 45% | 49% | 4% |
| 3 | 7: Wireless Access Control | 45% | 43% | 12% |
| 4 | 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches | 51% | 41% | 8% |
| 5 | 8: Data Recovery Capability | 52% | 39% | 7% |
| 6 | 11: Limitation and Control of Network Ports, Protocols, and Services | 53% | 36% | 9% |
| 7 | 12: Controlled Use of Administrative Privileges | 57% | 34% | 8% |
| 8 | 15: Controlled Access Based on the Need to Know | 57% | 29% | 13% |
| 9 | 4: Continuous Vulnerability Assessment and Remediation | 58% | 28% | 14% |
| 10 | 1: Inventory of Authorized and Unauthorized Devices | 60% | 27% | 12% |
| 11 | 3: Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, and Servers | 62% | 27% | 10% |
| 12 | 16: Account Monitoring and Control | 58% | 26% | 15% |
| 13 | 19: Secure Network Engineering | 59% | 25% | 15% |
| 14 | 17: Data Protection | 58% | 24% | 16% |
| 15 | 18: Incident Response and Management | 62% | 23% | 15% |
| 16 | 2: Inventory of Authorized and Unauthorized Software | 64% | 22% | 13% |
| 17 | 20: Penetration Tests and Red Team Exercises | 43% | 21% | 35% |
| 18 | 14: Maintenance, Monitoring, and Analysis of Audit Logs | 63% | 19% | 16% |
| 19 | 6: Application Software Security | 55% | 18% | 26% |
| 20 | 9: Security Skills Assessment and Appropriate Training to Fill Gaps | 54% | 18% | 26% |



Source: Tarala, James, "Critical Security Controls: From Adoption to Implementation", SANS Institute, November, 2014

# Opportunities For Improvement

- Need to quantify improvements enabled by the CSCs
  - 25% report they are able to quantify results and report those to management
  - 52% have noted improvements, but have not quantified them
- Sharing of information needed to accelerate implementing the CSCs
  - 68% requested usable case studies of successful implementations
  - 58% would like better operational best practices and support
  - 54% would like to see a directory of applicable tools
  - 53% would like sector-specific guidelines

# Conclusion – Are They Working?

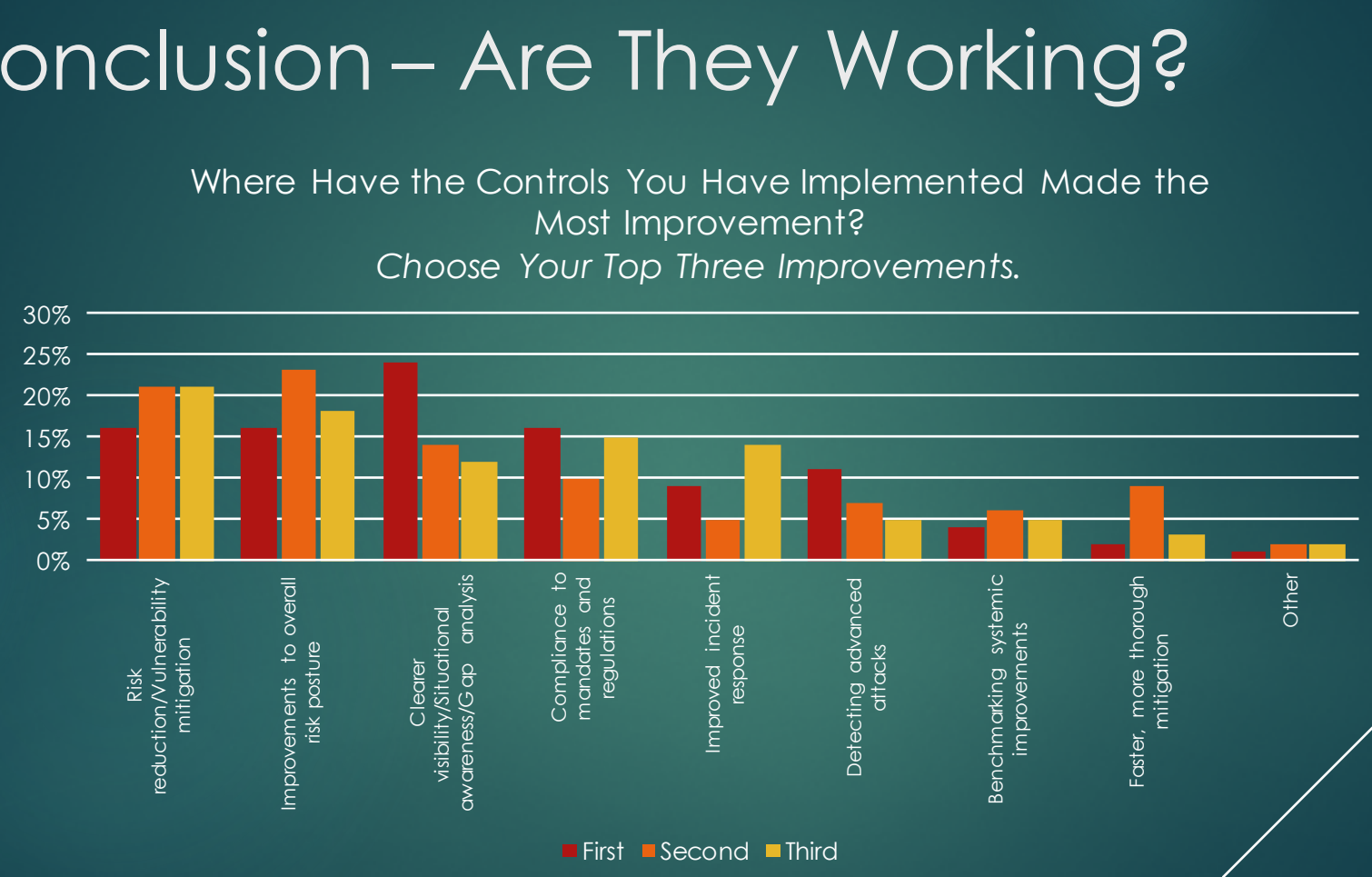




*Figure 16. Reported Improvements by CSC Implementers*

Source: Tarala, James, "Critical Security Controls: From Adoption to Implementation", SANS Institute, November, 2014

# Questions?

# Thank You

JOHN M. MILLICAN
PRINCIPAL, THE OFFICE OF THE CIO
(925) 235-0469
JMILLICAN@OOCIO.COM