Solving the CIO's Cybersecurity Dilemma: 20 Critical Controls for Effective Cyber Defense

John M. Gilligan

Information systems Security Association
National Capital Chapter

January 19, 2010

Topics

- Background
- Philosophy and Approach for the “20 Critical Controls”
- Control Examples and List of Controls
- Relationship of 20 Critical Controls to FISMA
- Recommendations
- Final thoughts

A CIO's Environment

- We are in a cyber "war" and are losing badly!
- The IT industry has produced an inherently unsecure environment—total is security not achievable
- CIO mandates exceed time and resources available
- Cyber security is an enormously complex challenge—there are very few true experts

It is time for CIOs and CISOs to focus on ways to make <u>real and measurable improvements</u> in security

The Challenge

- CIOs/CISOs can lead global change
- In the near-term, we must focus and measure progress
- Automation of security control implementation and continuous assessment is essential
- A well managed system is a harder target to attack and costs less to operate

CIOs/CISOs must take the lead in fighting the cyber war

FISMA Was Well Intended; What is Not Working??

- Original intent was good:
  - Ensure effective controls
  - Improve oversight of security programs
  - Provide for independent evaluation
- Implementation took us off course
  - Agencies unable to adequately assess cyber risks
  - (Lots of) NIST "guidance" became mandatory
  - No auditable basis for independent evaluation
  - Grading became overly focused on paperwork

Bottom Line: OMB mandates and paperwork debates has distracted CIOs/CISOs from achieving real security improvements

Analogy of Current Cybersecurity Approach

- An ambulance shows up at a hospital emergency room with a bleeding patient
- Hospital takes a detailed medical history, gives inoculations for seasonal flu, swine flu, tetanus, shingles, and vaccination updates
- Hospital tests for communicable diseases, high blood pressure, sends blood sample for cholesterol check, gives eye exam, checks hearing, etc.
- At some point, a nurse's aid` inquires about the red fluid on the floor

Implementation of FISMA has Resulted in a Checklist Approach: Not A Focus on Biggest Cyber Threats/Risks!

Meanwhile, the patient is bleeding to death!!

We Need Cybersecurity Triage—Not Comprehensive Medical Care

An "Aha" Moment!

- Scene: 2002 briefing by NSA regarding latest penetration assessment of DoD systems
- Objective: Embarrass DoD CIOs for failure to provide adequate security.
- Subplot: If CIOs patch/fix current avenues of penetration, NSA would likely find others
- Realization: Let's use NSA's offensive capabilities to guide security investments

Let "Offense Inform Defense"!

"20 Critical Controls": The Philosophy

- Assess cyber attacks to inform cyber defense – focus on high risk technical areas first
- Ensure that security investments are focused to counter highest threats — pick a subset
- Maximize use of automation to enforce security controls — negate human errors
- Define metrics for critical controls
- Use consensus process to collect best ideas

Focus investments by letting cyber offense inform defense

Approach for developing 20 Critical Controls

- Engage the best security experts:
  - NSA “Offensive Guys”
  - NSA “Defensive Guys”
  - DoD Cyber Crime Center (DC3)
  - US-CERT (plus 3 agencies that were hit hard)
  - Top Commercial Pen Testers
  - Top Commercial Forensics Teams
  - JTF-GNO
  - AFOSI
  - Army Research Laboratory
  - DoE National Laboratories
  - FBI and IC-JTF
- Identify top attacks—the critical risk areas
- Prioritize controls to match successful attacks—mitigate critical risks
- Identify automation/verification methods and measures
- Engage CIOs, CISOs, Auditors, and oversight organizations
- Coordinate with Congress regarding FISMA updates

Top 20 Attack Patterns—the biggest risks*

1. **Scan for unprotected systems on networks**
2. **Scan for vulnerable versions of software**
3. **Scan for software with weak configurations**
4. **Scan for network devices with exploitable vulnerabilities**
5. **Attack boundary devices**
6. **Attack without being detected and maintain long-term access due to weak audit logs**
7. **Attack web-based or other application software**
8. **Gain administrator privileges to control target machines**
9. **Gain access to sensitive data that is not adequately protected**
10. **Exploit newly discovered and un-patched vulnerabilities**
11. **Exploit inactive user accounts**
12. **Implement malware attacks**
13. **Exploit poorly configured network services**
14. **Exploit weak security of wireless devices**
15. **Steal sensitive data**
16. **Map networks looking for vulnerabilities**
17. **Attack networks and systems by exploiting vulnerabilities undiscovered by target system personnel**
18. **Attack systems or organizations that have no or poor attack response**
19. **Change system configurations and/or data so that organization cannot restore it properly**
20. **Exploit poorly trained or poorly skilled employees**

* Developed as a part of developing 20 Critical Controls and not in priority order

Example--Critical Control #1
Inventory of Authorized and Unauthorized Devices

- **Attacker Exploit**: Scan for new, unprotected systems
- **Control**:
  - Quick Win: Automated asset inventory discovery tool
  - Visibility/Attribution: On line asset inventory of devices with net address, machine name, purpose, owner
  - Configuration/Hygiene: Develop inventory of information assets (incl. critical information and map to hardware devices)
- **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:**
  - CM-8 (a, c, d, 2, 3, 4), PM-5, PM-6
- **Automated Support**: Employ products available for asset inventories, inventory changes, network scanning against known configurations
- **Evaluation**: Connect fully patched and hardened test machines to measure response from tools and staff. Control identifies and isolate new systems (Min--24 hours; best practice--less than 5 minutes)

Example--Critical Control #3
Secure Configurations for Hardware and Software on Laptops, Workstations and Servers

- **Attacker Exploit**: Automated search for improperly configured systems
- **Control**:
  - QW: Define controlled standard images that are hardened versions
  - QW: Negotiate contracts for secure images "out of the box"
  - Config/Hygiene: Tools enforce configurations; executive metrics with trends for systems meeting configuration guidelines
- **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:**
  - CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6
- **Automated Support**: Employ SCAP compliant tools to monitor/validate HW/SW/Network configurations
- **Evaluation**: Introduce improperly configured system to test response times/actions (Minimum--24 hours; best practice--less than 5 min)

20 Critical Controls for Effective Cyber Defense (1 of 2)

***Critical Controls Subject to Automated Collection, Measurement, and Validation*:**

1. **Inventory of Authorized and Unauthorized Devices**
2. **Inventory of Authorized and Unauthorized Software**
3. **Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers**
4. **Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**
5. **Boundary Defense**
6. **Maintenance, Monitoring, and Analysis of Security Audit Logs**
7. **Application Software Security**
8. **Controlled Use of Administrative Privileges**
9. **Controlled Access Based on Need to Know**
10. **Continuous Vulnerability Assessment and Remediation**
11. **Account Monitoring and Control**
12. **Malware Defenses**
13. **Limitation and Control of Network Ports, Protocols, and Services**
14. **Wireless Device Control**
15. **Data Loss Prevention**

20 Critical Controls for Effective Cyber Defense (2 of 2)

Additional Critical Controls (partially supported by automated measurement and validation):

16. **Secure Network Engineering**
17. **Penetration Tests and Red Team Exercises**
18. **Incident Response Capability**
19. **Data Recovery Capability**
20. **Security Skills Assessment and Appropriate Training to Fill Gaps**

Federal CIO Observation: The 20 Critical Controls are nothing new; they are recognized elements of a well managed enterprise

Evaluating Tools for Implementing the 20 Critical Controls

- State Department and other organizations have effectively automated controls
- SANS-led survey compiling list of tools aligned with controls (http://www.sans.org/critical-security-controls/user-tools.php)
- Vision is to have government-wide contract vehicles

Complying with FISMA and NIST Guidelines

- FISMA
  - Implement security protection commensurate with risk
  - Develop and maintain minimum controls
  - Selection of specific security solutions left to agencies
  - Ensure independent testing and evaluation of controls
- NIST Guidelines
  - Use risk assessment to categorize systems
  - Select controls based on risk
  - Assess security controls

Relevance of 20 Critical Controls to FISMA and NIST Guidelines

FISMA and NIST

1. Assess cyber security risk in an organization
2. Implement security based on risk
3. Select controls from NIST SP 800-53 to mitigate risk areas
4. Objectively evaluate control effectiveness

20 Critical Controls

1. Based on government-wide (shared) risk assessment
2. Controls address top cyber risks
3. 20 Critical Controls are subset of 800-53 Priority 1 controls
4. Use automated tools and periodic evaluations to provide continuous monitoring

20 Critical Controls are designed to help agencies comply with FISMA and NIST guidance!

20 Critical Controls—Implementation Recommendations

Step 1: Accept CAG **consensus threats as risk baseline** for your organization

Step 2: **Implement 20 Critical Controls**

Step 3: Use **organization specific risk assessment to select and implement additional controls** from 800-53

- Focus on unique, mission critical capabilities and data

Step 4: Use **automated tools and periodic evaluations to continuously measure compliance** (demonstrate risk reduction)

Step 5: Partner with senior management and auditors to **motivate compliance improvement**

- Use examples and lessons learned from State Dept. and others

Final Thoughts

- CIOs must lead global change
- In the near-term CIOs/CISOs must focus and measure
- Automation of security control implementation and continuous assessment is essential
- A well managed system is a harder target to attack and costs less to operate – the ultimate "no brainer" for a CIO

It is all about leadership.

We need to stop the bleeding—Now!

Contact Information

John M. Gilligan

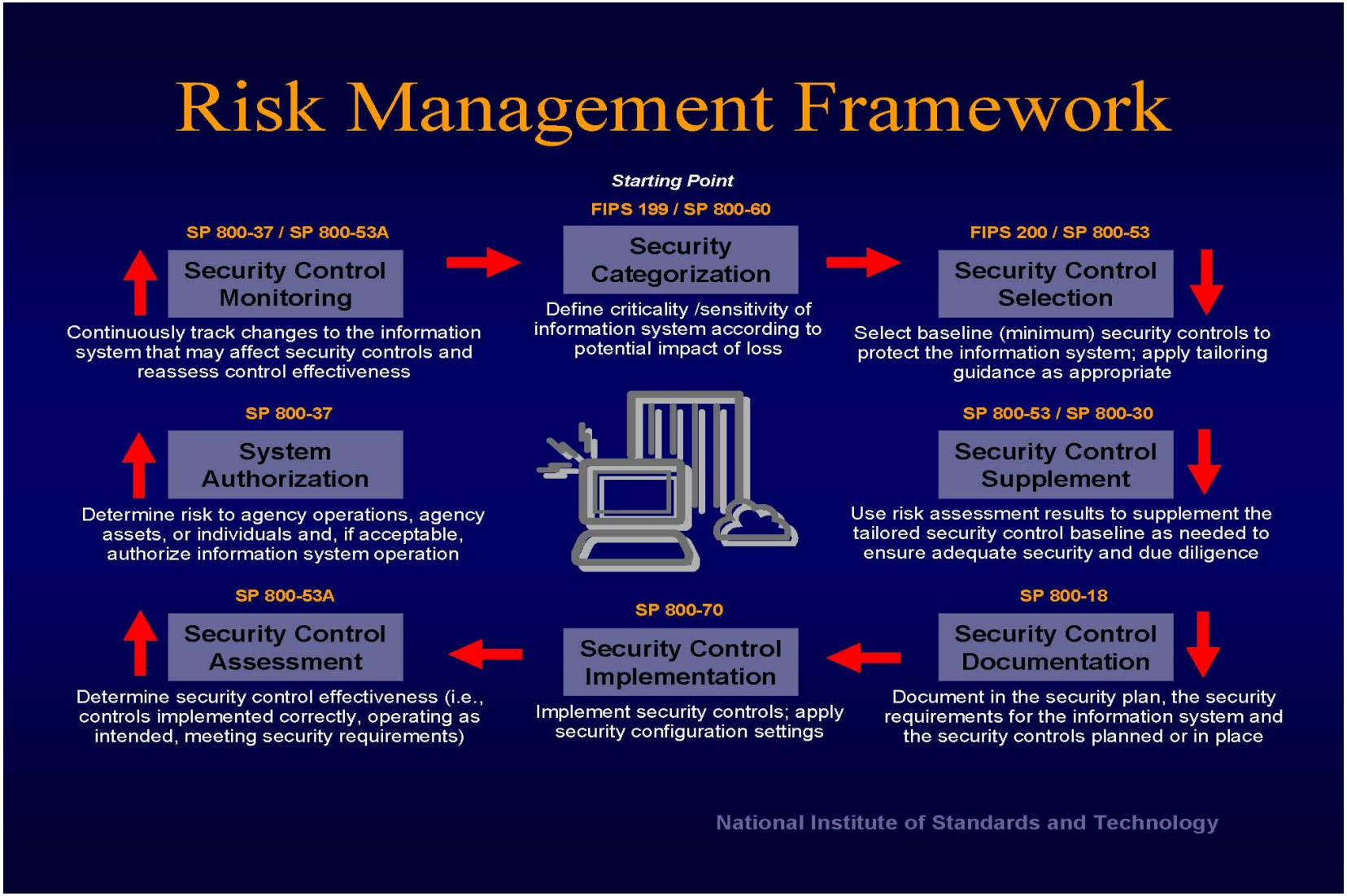
jgilligan@gilligangroupinc.com
703-503-3232
www.gilligangroupinc.com

FISMA Original Intent

- Framework to ensure effective information security controls
- Recognize impact of highly networked environment
- Provide for development and maintenance of minimum controls
- Improved oversight of agency information security programs
- Acknowledge potential of COTS capabilities
- Selection of specific technical hardware and software information security solutions left to agencies
- Provide independent evaluation of security program

However: FISMA has evolved to “grading” agencies based largely on secondary artifacts

Risk Management Framework



NIST Guidance: 1200 pages of FIPS Pubs, Special Pubs, Security Bulletins, etc.