

Ensuring Effective Security: The CIO's Dilemma

John M. Gilligan
Gilligan Group, Inc.

21 November 2008

Another Day in the life...

- Congressional language and GAO reports citing inadequacies of department's cyber security program
- Employee(s) arrested for downloading classified/sensitive information
- Nuclear response team loses disks with weapons design information
- Invited to Congressional hearing to explain why department has an "D" on FISMA report card
- Four-star generals dispute CIO assessment of security weaknesses

CIO's Spend Lots of Energy to Manage External and Internal Issues

CIO's Real Nightmare

- Cyber attacks impact ability to execute military missions (or to provide critical services to citizens or...)
- Cyber security restrictions reduce ability of military to operate effectively in coalition environment

Department mission impacted due to weaknesses in cyber security

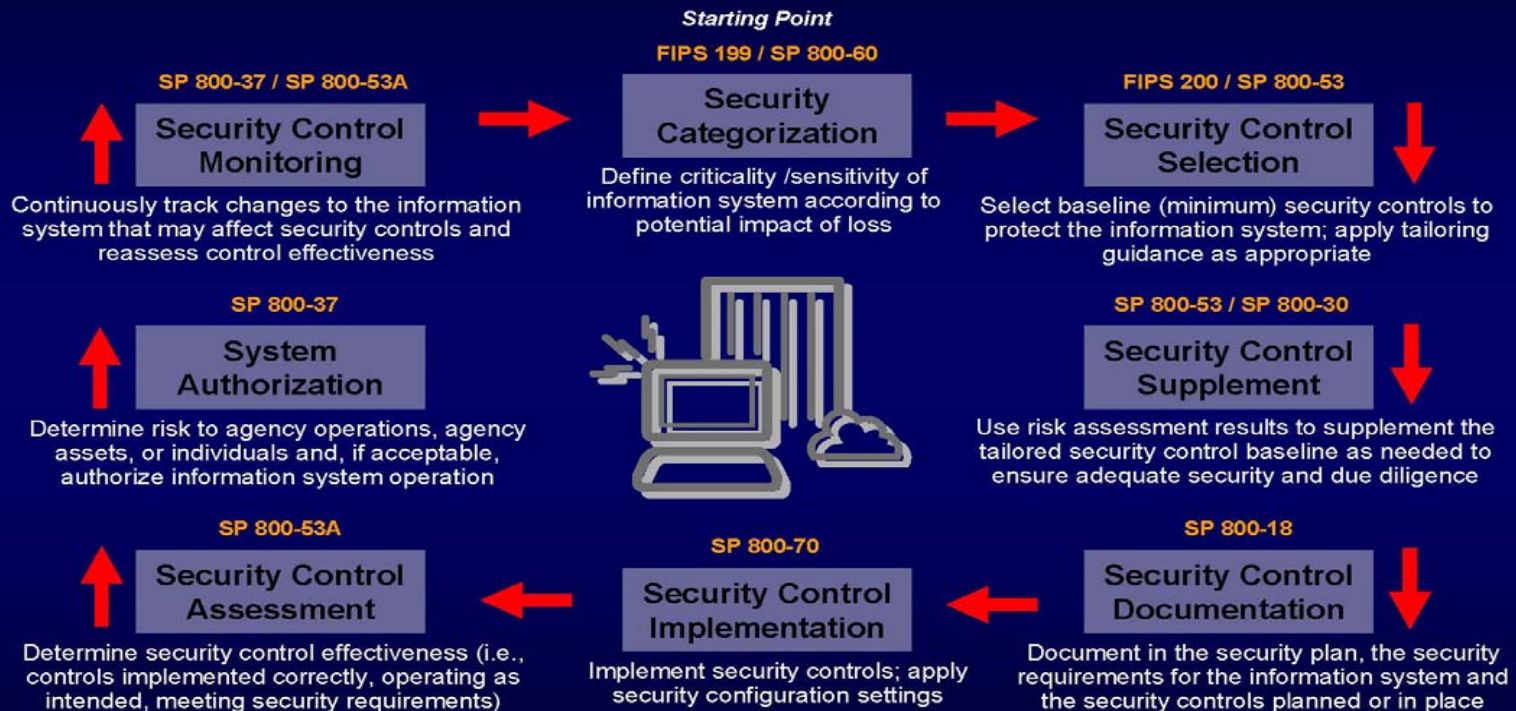
FISMA* Objectives

- 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

* Title III of the E-Government Act of 2002

(c) 2008, All Rights Reserved. Gilligan
Group Inc.

Risk Management Framework



National Institute of Standards and Technology

How to Assess Effective Security

"Pentagon Shuts Down Systems After *Cyber-Attack*"

GAO Reports?

Malicious scans of DoD
increase 300%!





Percentage of
Systems Certified?

Number of Systems with
Contingency Plans?

AGENCY AUDITOR
REPORTS?

The threat is increasing! Are we measuring the right things?

Effectiveness of FISMA*

- More attention to information security 
- Improved guidance for security 
- Additional cyber security investments 
 - Auditors to assess security
 - Contractors to certify systems
- Improved effectiveness against threats 

* As assessed by a former government CIO

The objectives are right, but implementation can be significantly improved

The CIO's Cyber Security Dilemma

- There are only so many resources available to be allocated against all CIO priorities
- There is no such thing as perfect cyber security
- Finding flaws in cyber security implementation is a “target rich” environment

How much security is enough, and where should investments be applied?

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

The origins of what eventually became the FDCC

AF Secure Desktop Configuration → FDCC

- NSA Offensive Team briefings to Air Force on attack patterns and vulnerabilities exploited
- ~80% of vulnerabilities tied to incorrectly configured COTS software
- Joint effort by NSA, NIST, DISA, Microsoft to create Secure Desktop Configuration (SDC)
- AF validated concept; OMB adopted government-wide

Lesson learned: Focused investments can significantly improve security

Another Example: Robust User Identity

- Breaking passwords was another common attack by offensive attackers
 - Many users did not comply with password standards
 - Even passwords that met DoD standards could be broken
- DoD mandated use of Common Access Card (CAC) to access DoD systems

Successful cyber attacks against DOD drop dramatically

Continued Evolution of “Aha” Realization: The Consensus Audit Guidelines (CAG)

- Ensure that investments are focused to counter highest threats — pick a subset
- Leverage offense to inform defense — focus on high payoff areas
- Maximize use of automation to enforce security controls — negate human errors
- Use consensus process to ensure best ideas

Focus investments by letting cyber offense inform defense!

Summary

- FISMA had the right objectives...
- Government agencies spending a lot for security with little confidence that it is effective
- Consensus Audit Guidelines—an approach that addresses the CIO's dilemma
 - Focus on mission-impacting security controls
 - Common basis for assessing/measuring security

Backup

NIST Security Guidance

- NIST Risk framework consists of over 1200 pages of guidance
- An additional security-related mandatory 15 Federal Information Processing Standard (FIPS) Publications
- Over 100 additional security related special publications
- Over 35 Interagency Reports
- Over 65 Security Bulletins (since 2002)

A very impressive list of guidance—but is it contributing to improved security?

Weaknesses of Auditor Reports and FISMA Scorecards

- Dependent on skills and expectations of assessors (numerous examples of poor security getting high grades)
- Most security assessments rely on external (i.e., lots of paper) artifacts