

Information Systems Under Attack

Managing Enterprise Risk in Today's World of Sophisticated Threats and Adversaries

March 8, 2007

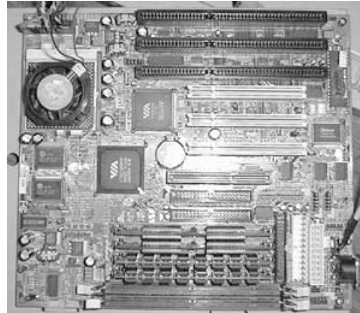
Dr. Ron Ross
Computer Security Division
Information Technology Laboratory

Current State of Affairs

- Continuing serious attacks on federal, state, and local information systems, large and small; targeting key government operations and assets.
- Significant exfiltration of critical and sensitive information and implantation of malicious software.
- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries: nation states, terrorist groups, hackers, criminals, and any individuals or groups with intentions of compromising public and private sector information systems.
- Increasing number of trusted employees taking dangerous and imprudent actions with respect to organizational information systems.

Threats to Security

Connectivity



Complexity

U.S. Critical Infrastructures

- “...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.”

-- *USA Patriot Act (P.L. 107-56)*

U.S. Critical Infrastructures

- Energy (electrical, nuclear, gas and oil, dams)
- Transportation (air, road, rail, port, waterways)
- Public Health Systems / Emergency Services
- Information and Telecommunications
- Defense Industry
- Banking and Finance
- Postal and Shipping
- Agriculture / Food / Water
- Chemical

Legislative and Policy Drivers

- Public Law 107-347 (Title III)
Federal Information Security Management Act of 2002
- Homeland Security Presidential Directive #7
Critical Infrastructure Identification, Prioritization, and Protection
- OMB Circular A-130 (Appendix III)
Security of Federal Automated Information Resources
- OMB Memorandum M-06-16
Protection of Sensitive Information

Information Security

Why is it important at the FTA?

- Rich target of opportunity for adversaries
 - Very substantial, interconnected networks of diverse resources including computers and important financial information.
- Need to protect the critical/sensitive taxpayer information from unauthorized:
 - Disclosure (confidentiality breach)
 - Modification (integrity breach)

FISMA Strategic Vision

- We are building a solid foundation of information security across one of the largest information technology infrastructures in the world based on comprehensive security standards and technical guidance.
- We are institutionalizing a comprehensive Risk Management Framework that promotes flexible, cost-effective information security programs for federal agencies.
- We are establishing a fundamental level of “security due diligence” for federal agencies and their contractors based on minimum security requirements and security controls.

Key Players

- Authorizing Officials
- Mission / Information System Owners
- Chief Information Officers
- Chief Information Security Officers
- Inspectors General

FISMA Characteristics

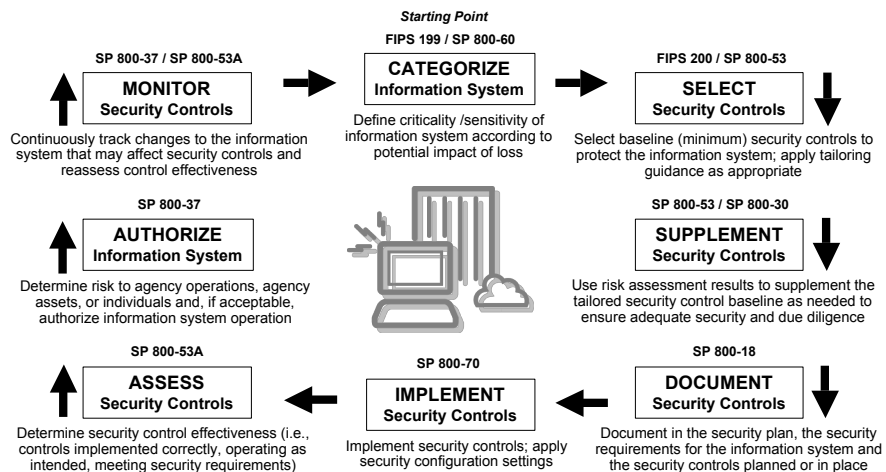
- The NIST *Risk Management Framework* and the associated security *standards* and *guidance* documents provide a process that is:
 - Disciplined
 - Flexible
 - Extensible
 - Repeatable
 - Organized
 - Structured

“Building information security into the infrastructure of the organization... so that critical enterprise missions and business cases will be protected.”

Managing Enterprise Risk

- Key activities in managing enterprise-level risk—risk to the enterprise and to other organizations resulting from the operation of an information system:
 - ✓ **Categorize** the information system (criticality/sensitivity)
 - ✓ **Select** and tailor baseline (minimum) security controls
 - ✓ **Supplement** the security controls based on risk assessment
 - ✓ **Document** security controls in system security plan
 - ✓ **Implement** the security controls in the information system
 - ✓ **Assess** the security controls for effectiveness
 - ✓ **Authorize** information system operation based on mission risk
 - ✓ **Monitor** security controls on a continuous basis

Risk Management Framework

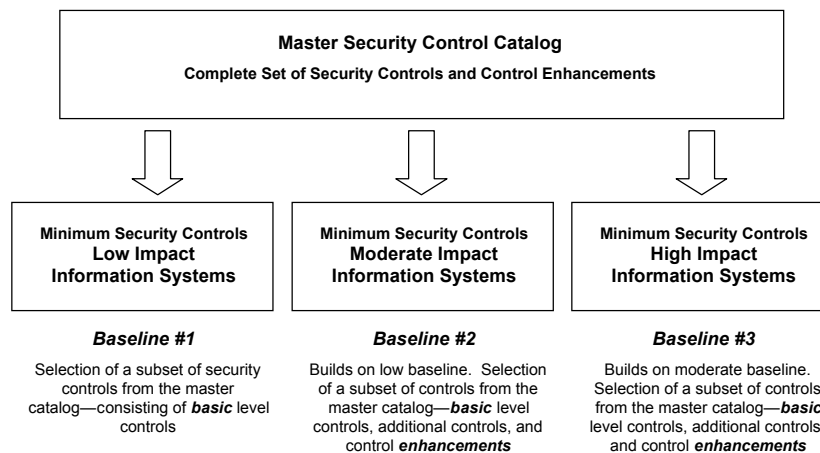


Security Categorization

Example: An Enterprise Information System

FIPS Pub 199	Low	Moderate	High
Confidentiality	The loss of confidentiality could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Security Control Baselines



Information Security Program



Links in the Security Chain: Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning
- ✓ Security policies and procedures
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments
- ✓ Certification and accreditation
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Boundary and network protection devices (Firewalls, guards, routers, gateways)
- ✓ Intrusion protection/detection systems
- ✓ Security configuration settings
- ✓ Anti-viral, anti-spyware, anti-spam software
- ✓ Smart cards

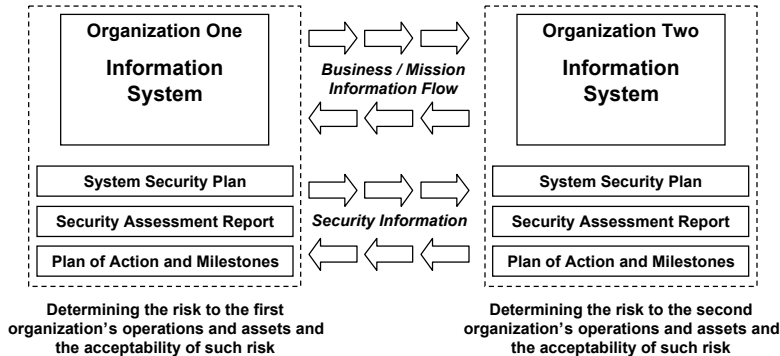
Adversaries attack the weakest link...where is yours?

Information Security Strategy

- Successful FISMA implementation demands that organizations adopt an enterprise-wide security strategy.
- Metrics of a successful implementation:
 - Cost-effective
 - Consistent
 - Comprehensive
 - Effective

The Desired End State

Security Visibility Among Business/Mission Partners



The objective is to achieve *visibility* into prospective business/mission partners information security programs BEFORE critical/sensitive communications begin...establishing levels of security due diligence and trust.

Some Final Thoughts

- Your adversaries don't care about FISMA compliance—they just want to compromise your information systems.
- FISMA is not just a paperwork exercise; it is the application of comprehensive security controls to information systems that are supporting critical enterprise missions.

Some Final Thoughts

- The most dangerous person to an enterprise is an uninformed senior management official.
- FISMA security standards and guidelines should not impede the mission; rather the standards and guidelines should enable and support the mission— with respect to reliability, fidelity, and quality.

Some Final Thoughts

- FISMA is about the application of common sense security—it is not dogma to be followed blindly.
- The only mandatory requirement under the FISMA security standards and guidance is the application of the NIST Risk Management Framework—everything else is negotiable.

Some Final Thoughts

- Policies and procedures are not just FISMA paperwork—they are a corporate statement of commitment to protecting critical enterprise information and information systems and the necessary details describing how to do it.



Some Final Thoughts

- If the successful accomplishment of enterprise missions depends on information systems, including the information processed, stored, and transmitted by those systems, the systems must be dependable—to be dependable in the face of serious threats, the systems must be appropriately protected.



Some Final Thoughts

- Never underestimate the capabilities of your adversaries.
- Never overestimate the ability of your organization and your personnel to protect critical enterprise missions.
- Information technology—if you can't protect it, don't deploy it.

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Matt Scholl
(301) 975-2941
matthew.scholl@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov