

Managing Cybersecurity Risk

An Integrated Approach to Building a Risk-Based Cybersecurity Program

Dr. Ron Ross Computer Security Division Information Technology Laboratory



The current landscape.



- We are vulnerable because our information technology is fragile and susceptible to a wide range of threats including:
 - natural disasters.
 - structural failures.
 - cyber attacks.
 - errors.





Advanced Persistent Threat

An adversary that —

- Possesses significant levels of expertise / resources.
- Creates opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, deception).
- Establishes footholds within IT infrastructure of targeted organizations:
 - To exfiltrate information;
 - To undermine / impede critical aspects of a mission, program, or organization; and
 - To position itself to carry out these objectives in the future.

Classes of Vulnerabilities

A 2013 Defense Science Board Report described—

- Tier 1: Known vulnerabilities.
- Tier 2: Unknown vulnerabilities (zero-day exploits).
- Tier 3: Adversary-created vulnerabilities (APT).







Complexity. An adversary's most effective weapon in the 21st century.



Good cyber hygiene is necessary... But not sufficient.



You can't count, configure, or patch your way out of this problem space.

Difficult decisions ahead.





Today, in cybersecurity, we are doing a lot of things right... <u>But we are not doing enough</u>.



The hard cybersecurity problems are buried below the water line...



In the hardware, software, and firmware.



Reducing susceptibility to cyber threats requires a multidimensional systems engineering approach. **Security Architecture** and Design Harden the Limit damage System target to the target Achieving Trustworthiness and Resiliency Make the target survivable

Z



Getting the attention of the C-Suite.



TACIT Security

- Threat
- Assets
- Complexity
- Integration
- Trustworthiness

MERRIAM-WEBSTER DICTIONARY
tac·it adjective
expressed or understood without being directly stated

Threat

- Develop a better understanding of the *modern* threat space, including the capability of adversaries to launch sophisticated, targeted cyber-attacks that exploit specific organizational vulnerabilities.
 - Obtain threat data from as many sources as possible.
 - Include external and insider threat analysis.



Assets

- Conduct a comprehensive criticality analysis of organizational assets including information and information systems.
 - Focus on mission/business impact.
 - Use triage concept to segregate assets by criticality.





Complexity

- Reduce the *complexity* of the information technology infrastructure including IT component products and information systems.
 - Employ enterprise architecture to consolidate, optimize, and standardize the IT infrastructure.
 - Adopt cloud computing architectures to reduce the number of IT assets through on-demand provisioning of services.



Integration

- Integrate information security requirements and the security expertise of individuals into organizational development and management processes.
 - Embed security personnel into enterprise architecture, systems engineering, SDLC, and acquisition processes.
 - Coordinate security requirements with mission/business owners; become key stakeholders.



Trustworthiness

- Invest in more *trustworthy* and *resilient* information systems supporting organizational missions and business functions.
 - Isolate critical assets into separate enclaves.
 - Implement solutions using modular design, layered defenses, component isolation.



Summary – TACIT Security

- Understand the cyber threat space.
- Conduct a thorough criticality analysis of organizational assets.
- Reduce complexity of IT infrastructure.
- Integrate security requirements into organizational processes.
- Invest in trustworthiness and resilience of IT components and systems.



Getting immediate help.



Joint Task Force Cyber Security Toolset

- NIST Special Publication 800-39 Managing Information Security Risk: Organization, Mission, and Information System View
- NIST Special Publication 800-30 Guide for Conducting Risk Assessments
- NIST Special Publication 800-37 Applying the Risk Management Framework to Federal Information Systems
- NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems and Organizations







Cybersecurity Command and Control

Communicating and sharing risk-related information from the strategic to tactical level, that is from the executives to the operators.

TIER 1 Organization (Governance)

TIER 2 Mission / Business Process (Information and Information Flows) Communicating and sharing risk-related information from the tactical to strategic level, that is from the operators to the executives.

TIER 3 Information and Weapons Systems (Environment of Operation)



Risk Management Framework





Dual Protection Strategies

Sometimes your information systems will be compromised even when you do everything right...

Boundary Protection

Primary Consideration: *Penetration resistance.* Adversary Location: *Outside defensive perimeter.* Objective: *Repel the attack.*

Agile Defense

Primary Consideration: Information system resilience.
Adversary Location: Inside defensive perimeter.
Objective: Operate while under attack, limit damage, survive.



The road ahead.





Institutionalize.

The ultimate objective for security.



Operationalize.





On the Horizon...

NIST Special Publication 800-160

Systems Security Engineering An Integrated Approach to Building Trustworthy Resilient Systems





Multidisciplinary integration of security best practices.



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

27



Command and control of the security space.







NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

28



ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes



Technical Processes

- Business or mission analysis
 - Stakeholder needs and requirements definition
 - System requirements definition
 - Architecture definition
 - Design definition
 - System analysis
 - Implementation
 - Integration
 - Verification
 - Transition
 - Validation
 - Operation
 - Maintenance
- Disposal





ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes



Nontechnical Processes

- Project planning
 - Project assessment and control
 - Decision management
 - Risk management
 - Configuration management
 - Information management
 - Measurement
 - Quality assurance
 - Acquisition and Supply
 - Life cycle model management
 - Infrastructure management
 - Portfolio management
 - Human resource management
 - Quality management
- Knowledge management



Some final thoughts.



A Winning Strategy

"Build the Right Solution" Meets operational intent

Systems Engineering Software Assurance System Life Cycle Testing/Evaluation Trustworthiness Resiliency Design Architecture Acquisition Secure Coding Static Code Analysis Systems Integration Systems Security Engineering

"Build the Solution Right"

Meets design intent



A two-pronged attack on the threat space

> Critical Missions and Business Functions

To survive in the digital age of total IT dependence...

"Continuously Monitor" Preserves operational intent over time

> Security Configurations Ongoing Authorization Separation of Duties Software Patching Traffic Analyses Security State Asset Inventory Network Sensors Incident Response Threat Assessment Situational Awareness Administrative Privileges Vulnerability Assessment

"Continuously Maintain" Preserves design intent over time

Foundation of Components, Systems, Services





Security should be a by-product of good design and development practices—integrated throughout the organization.





Be *proactive*, not *reactive* when it comes to protecting your organizational assets.







Government

Academia

Security is a team sport.







NIST

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

LinkedIn http://www.linkedin.com/in/ronrossnist

Senior Information Security Researchers and Technical Support

Pat Toth (301) 975-5140 patricia.toth@nist.gov Kelley Dempsey (301) 975-2827 kelley.dempsey@nist.gov

Web: csrc.nist.gov

Comments: sec-cert@nist.gov

