Health IT Standards Committee Meeting

Security Risk Management
For Health IT Systems and Networks

Dr. Ron Ross
Computer Security Division
Information Technology Laboratory

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Setting the stage.
The growing use of advanced information technologies...

Key Challenge
Exercising security and privacy due diligence and managing risk.

The sanctity of the patient’s privacy (data confidentiality) and safety (data integrity and service availability)
We are vulnerable because our information technology is **fragile and susceptible** to a wide range of threats including:

- cyber attacks.  
  (including insider threat)
- natural disasters.
- structural failures.
- errors and misuse.
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.
A 2013 Defense Science Board Report described—

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

A significant number of these vulnerabilities are “off the radar” of most organizations...
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...

*But we are not doing enough.*
The hard cybersecurity problems are buried below the water line...

*In the hardware, software, and firmware.*
The argument for building stronger, more resilient information systems…

Software assurance.
Systems security engineering.
Supply chain risk management.
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

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

Federal 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*
The Healthcare Organization

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)

TIER 3
Information Systems and Medical Devices (Environment of Operation)

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

**Starting Point**

**CATEGORIZE Information System**

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

**SELECT Security Controls**

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

**IMPLEMENT Security Controls**

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

**ASSESS Security Controls**

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

**AUTHORIZE Information System**

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

**MONITOR Security Controls**

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

---

**Security Life Cycle**

164.308(a)(1)(i) Security Management Process
164.308(a)(1)(ii)(A) Risk Analysis
164.308(a)(1)(ii)(B) Risk Management
164.316(b)(1) Documentation
164.316(b)(2)(ii) Updates

164.308(a)(8) Evaluation
164.308(a)(1)(ii)(D) Information System Activity Review
164.308(a)(1)(ii)(B) Risk Management
164.308(a)(1)(ii)(D) Information System Activity Review
164.308(a)(1)(ii)(B) Risk Management
164.308(a)(8) Evaluation
164.316(b)(1) Documentation
164.316(b)(2)(ii) Updates
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 during disruption, mitigate damage, recover quickly.*
On the Horizon…

NIST Special Publication 800-160

Systems Security Engineering

*An Integrated Approach to Building Trustworthy Resilient Systems*
Building on International Standards

- Stakeholder requirements definition.
- Requirements analysis.
- Architectural design.
- Implementation.
- Integration.
- Verification.
- Transition.
- Validation.
- Operation.
- Maintenance.
- Disposal.

Integrating the RMF and security concepts, principles, and best practices into IEEE/ISO/IEC 15288 Systems and software engineering — System life cycle processes
Some final thoughts.
Security is critical to the success of any healthcare organization, and to the privacy, safety, and health of patients.

Security should be a by-product of good design and development practices.
Be *proactive*, not *reactive* when it comes to protecting your organizational assets.
Cybersecurity is a team sport.

Government

Academia

Industry
Necessary *and* Sufficient Security Solutions…

Cyber Security Hygiene

COUNTING, CONFIGURING, AND PATCHING IT ASSETS

Has your organization achieved the appropriate balance?

Strengthening the IT Infrastructure

SYSTEM/SECURITY ENGINEERING, ARCHITECTURE, AND RESILIENCY
Contact Information

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

**Project Leader**
Dr. Ron Ross
(301) 975-5390
ron.ross@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

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

Comments: sec-cert@nist.gov