HIMSS17
WHERE THE BRIGHTEST MINDS IN HEALTH AND IT DRIVE IMPROVED OUTCOMES
HIMSS ANNUAL CONFERENCE & EXHIBITION | FEB 19–23, 2017
ORLANDO | ORANGE COUNTY CONVENTION CENTER

The Road Ahead for Healthcare Sector: What to Expect in Cybersecurity

Session CS6, February 19, 2017

Donna F. Dodson, Chief Cybersecurity Advisor,

National Institute of Standards and Technology

Speaker Introduction

Donna F. Dodson

Chief Cybersecurity Advisor &

Director, National Cybersecurity Center of Excellence

National Institute of Standards and Technology

Conflict of Interest

Donna F. Dodson

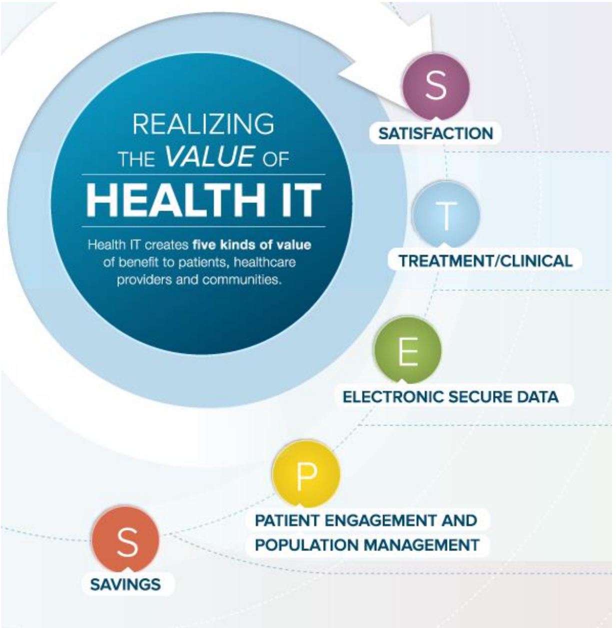
Works for the US Department of Commerce’s National Institute of Standards and Technology (NIST) and has no real or apparent conflicts of interest to report.

Agenda

- Introduction
- Motivation for Cybersecurity in Healthcare
- NIST Efforts in Cybersecurity
- NIST Key Programs in Cybersecurity and a Look to the Future
- Discussion and Questions

Learning Objectives

- Explain how new technology can introduce new vulnerabilities and points of access into your network
- Describe new privacy and cybersecurity concerns as a result of adopting new technology
- Illustrate multiple dependencies of the healthcare sector on other sectors and how preparedness and response efforts should change to avoid critical infrastructure failures


REALIZING THE VALUE OF
HEALTH IT
Health IT creates five kinds of value of benefit to patients, healthcare providers and communities.
S
SATISFACTION
T
TREATMENT/CLINICAL
E
ELECTRONIC SECURE DATA
P
PATIENT ENGAGEMENT AND POPULATION MANAGEMENT
S
SAVINGS

Healthcare, Technology and Cybersecurity

- In December 2010, the Department of Health and Human Services launched Healthy People 2020, which has four overarching goals:
  - Attain high-quality, longer lives free of preventable disease, disability, injury, and premature death;
  - Achieve health equity, eliminate disparities, and improve the health of all groups;
  - Create social and physical environments that promote good health for all; and
  - Promote quality of life, healthy development, and healthy behaviors across all life stages.
- Technology is an important tool to achieve these goals
  - Innovation
  - Rapid Change
  - Evolving “business models”
- Cybersecurity Risk Management is a critical tool to address the changing environment

NIST Cybersecurity Program

- Standards, Guidance, Tools and Metrics
- Cybersecurity Education and Workforce Development
- Standards-based Cybersecurity Blueprints

NIST’s Cybersecurity Program

Research Areas:

- Authentication -Access Control
- Biometrics
- Continuous Monitoring
- Cryptography
- Identity Management
- Information Sharing
- Key Management
- Network Security
- Privacy
- Risk Management
- Security Automation
- Software Quality
- Security Testing
- Usable Security
- Vulnerability Management

Secure Applications and Engineering:

- Cloud
- Cyber Physical Systems
- Healthcare
- IoT
- Mobility
- Public Safety Networks
- Smart Grid
- Voting

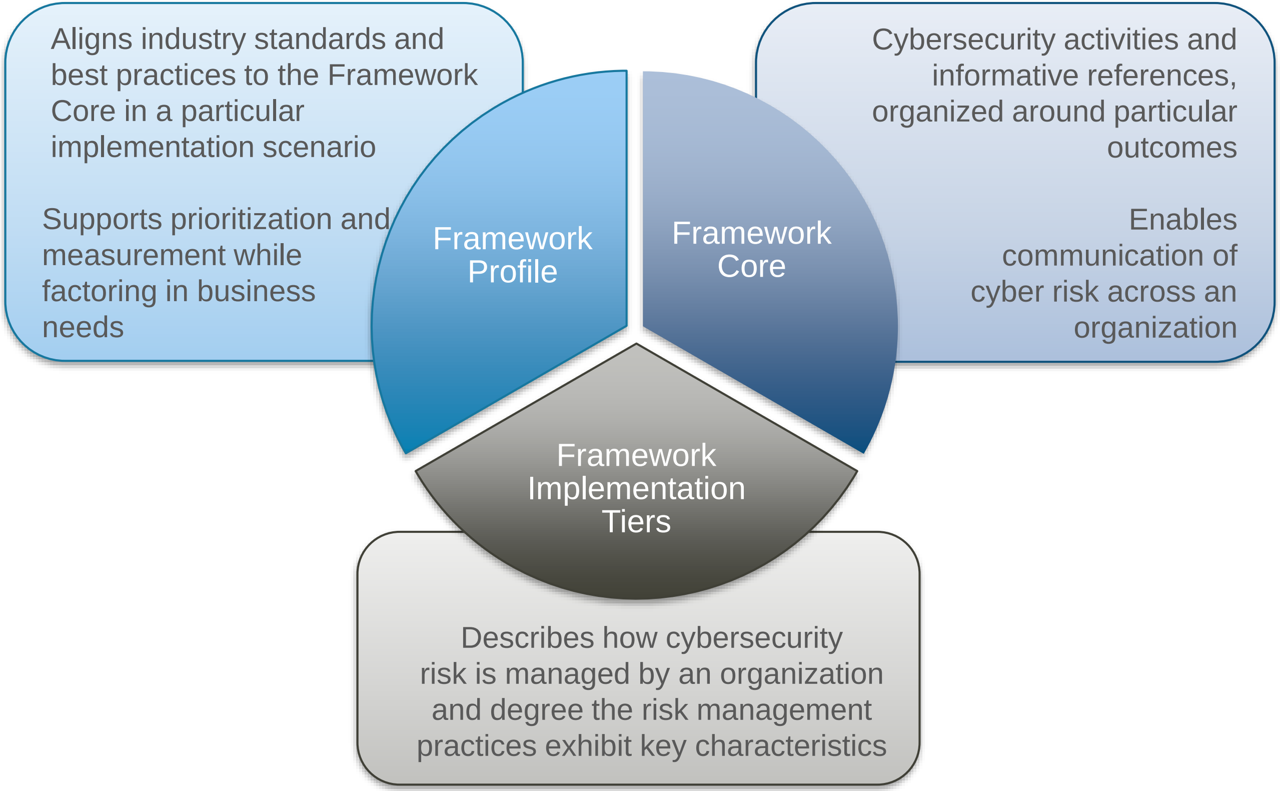
Key Program Areas

- Framework for Improving Critical Infrastructure Cybersecurity
- Cryptography
- Mobility and Security
- Security and Internet of Things
- National Cybersecurity Center of Excellence

Framework for Improving Critical Infrastructure Cybersecurity

- Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk
- Identify areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations
- Be consistent with voluntary international standards

Cybersecurity Framework Components



Framework Profile

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs

Framework Core

Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Framework Implementation Tiers

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Core

Cybersecurity Framework Component

	Function	Category	ID
What processes and assets need protection?	**Identify**	Asset Management	**ID.AM**
		Business Environment	**ID.BE**
		Governance	**ID.GV**
		Risk Assessment	**ID.RA**
		Risk Management Strategy	**ID.RM**
What safeguards are available?	**Protect**	Access Control	**PR.AC**
		Awareness and Training	**PR.AT**
		Data Security	**PR.DS**
		Information Protection Processes & Procedures	**PR.IP**
		Maintenance	**PR.MA**
		Protective Technology	**PR.PT**
What techniques can identify incidents?	**Detect**	Anomalies and Events	**DE.AE**
		Security Continuous Monitoring	**DE.CM**
		Detection Processes	**DE.DP**
What techniques can contain impacts of incidents?	**Respond**	Response Planning	**RS.RP**
		Communications	**RS.CO**
		Analysis	**RS.AN**
		Mitigation	**RS.MI**
		Improvements	**RS.IM**
What techniques can restore capabilities?	**Recover**	Recovery Planning	**RC.RP**
		Improvements	**RC.IM**
		Communications	**RC.CO**

Implementation Tiers

	1 Partial	2 Risk Informed	3 Repeatable	4 Adaptive
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization benefits my sharing or receiving information from outside parties			

Profile

Cybersecurity Framework Component

Ways to think about a Profile:

- A customization of the Core for a given sector, subsector, or organization
- A fusion of business/mission logic and cybersecurity outcomes
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state
- A decision support tool for cybersecurity risk management

Identify
Protect
Detect
Respond
Recover

Cryptography and Healthcare

- Cryptography for Lightweight Devices
  - Resource constrained environments and connectivity
  - Performance Metrics
  - Hardware-Specific Metrics
  - Software- Specific Metrics
- Blockchain and Distributed Ledger Technology
- Quantum Resistant Cryptography

Mobility and Security

- Mobile Threat Catalogue
- NCCoE Mobile Device Security Building Block
  - a government build, enterprise build, and privacy-enhancing build
- LTE Security
- Update to NIST Mobility Guidance
- Public Safety Work
  - Over the Air SIM / UICC Provisioning
  - Handset and Wearable Security

Security and Internet of Things

- Laying groundwork for IoT and security
- Support standards organizations looking at both foundational aspects and sector specific challenges

National Cybersecurity Center of Excellence

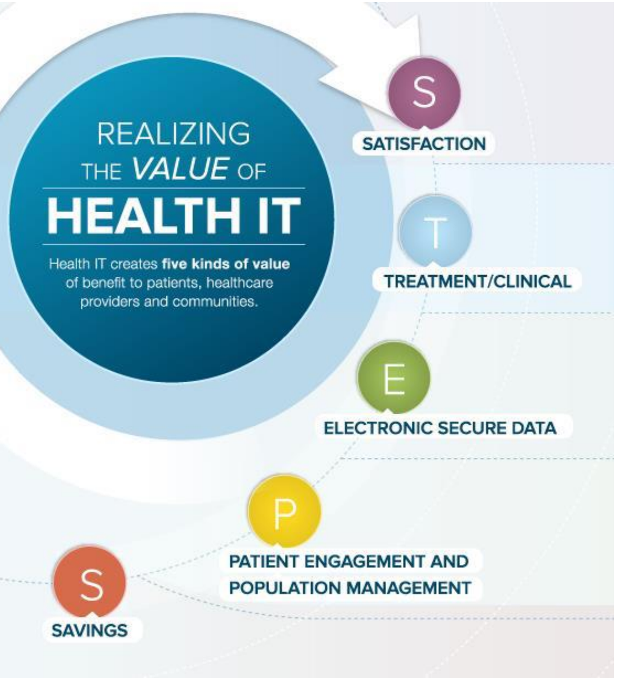
- Accelerates businesses' adoption of standards-based, advanced security technologies.
- Work with industry to identify their most pressing cybersecurity issues.
- Generate detailed technical descriptions of the problems and map the desired solution to NIST and industry standards and best practices.
- Collaborate with industry to build end-to-end example solutions we build in our labs.
- Each project results in a freely available NIST Cybersecurity Practice Guide (Special Publication series 1800), which includes information and instructions organizations can use to implement an example solution for themselves. Organizations that want to adopt similar solutions can use products from our collaborating vendors, or products with similar characteristics that fit their budgets and IT infrastructure.

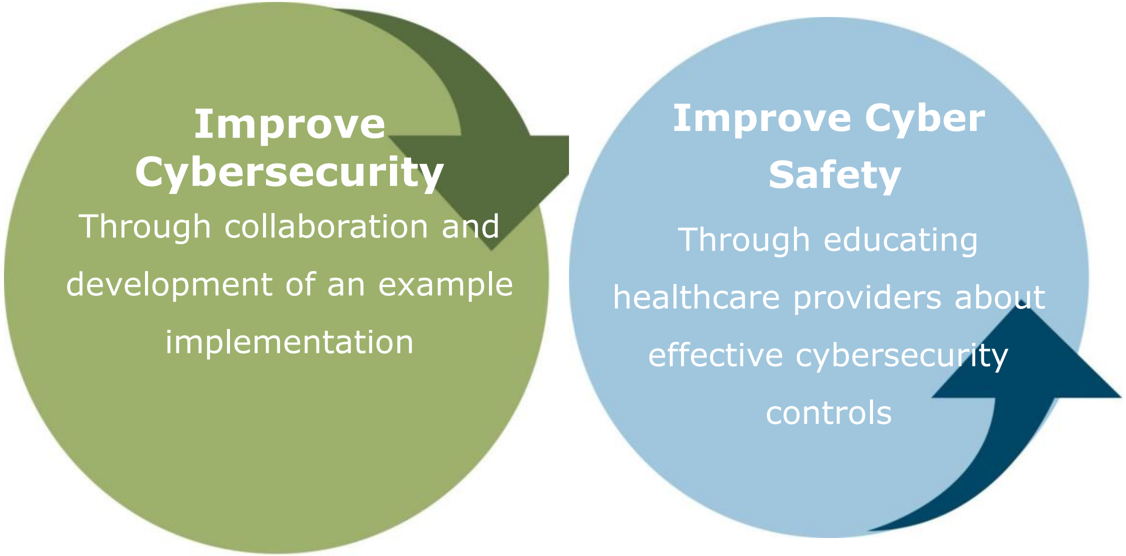
National Cybersecurity Center of Excellence

The Center is conducting projects to help advance the cybersecurity postures of health care organizations.

- Secure Electronic Health Records on Mobile Devices : A platform for health care providers to securely document, maintain, and exchange electronic patient information among mobile devices.
- Wireless Medical Infusion Pumps: Helping health care providers secure wireless medical infusion pumps on an enterprise network.

Realizing the Value of Health IT


REALIZING THE VALUE OF
HEALTH IT
Health IT creates five kinds of value of benefit to patients, healthcare providers and communities.
S
SATISFACTION
T
TREATMENT/CLINICAL
E
ELECTRONIC SECURE DATA
P
PATIENT ENGAGEMENT AND POPULATION MANAGEMENT
S
SAVINGS



Improve Cybersecurity

Through collaboration and development of an example implementation

Improve Cyber Safety

Through educating healthcare providers about effective cybersecurity controls

Questions ?

Donna F. Dodson
donna.dodson@nist.gov

NIST Computer Security Resource Center
http://csrc.nist.gov/

Cybersecurity Framework
www.nist.gov/cyberframework

National Cybersecurity Center of Excellence
https://nccoe.nist.gov

National Initiative for Cybersecurity Education
http://csrc.nist.gov/nice/