National Cybersecurity Challenges and NIST

Donna F. Dodson
Chief Cybersecurity Advisor
ITL Associate Director for Cybersecurity

Though no-one knows for sure, corporate America is believed to lose anything from $100 billion to $1 trillion a year from online theft of proprietary information—trade secrets, research findings, internal costs, marketing plans, personal information, credit-card numbers, bank-account details and much more -

Babbage (blog), The Economist, May 11, 2012

The internet of things (to be hacked)

Cybersecurity is now a part of all our lives. "Patches" and other security updates arrive for phones, tablets and PCs. Consultants remind us all not to open unknown files or plug unfamiliar memory sticks into computers...Now a new phase in this contest is emerging: "the internet of things". This involved embedding miniature computers in objects and connecting them to the internet using wireless technology. Cisco, a technology company, predicts that 50 billion connected devices will be in circulation by the end of decade, up from 11 billion last year.

The Economist, July 12, 2014

NIST Focus Areas

- Standards, Guidance, Tools and Metrics
  (Computer Security Division)
- Cybersecurity Outreach and Education
  (National Initiative for Cybersecurity Education)
- Vibrant Identity Management Ecosystem
  (National Strategy for Trusted Identities in Cyberspace)
- Standards based Cybersecurity Blueprints
  (National Cybersecurity Center of Excellence)
- Secure and Resilient Critical Infrastructure
  (Executive Order- Improving Critical Infrastructure Cybersecurity)

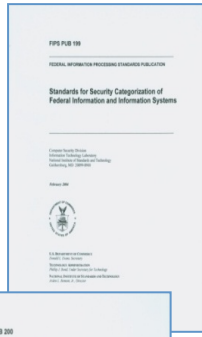
NIST's Cybersecurity Core Program

- Research, Development, and Specification
  - Security Mechanisms (e.g. protocols, cryptographic, access control, auditing/logging)
  - Security Mechanism Applications
    - Confidentiality
    - Integrity
    - Availability
    - Authentication
    - Non-Repudiation
- Secure System and Component configuration
- Assessment and assurance of security properties of products and systems

Key Project Areas

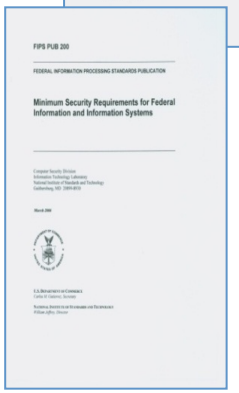
Risk Management

Focus on a complete Risk Management Framework that supports the lifecycle management of organization's traditional information and information infrastructure as well as cyber physical systems


FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems


FIPS PUB 200

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Minimum Security Requirements for Federal Information and Information Systems

Configuration Baselines

Standardized security configurations for operating systems and automated tools to test the configurations

Security Automation and Vulnerability Management

Continue to develop tools and specifications that address situational awareness, conformity and vulnerability management compliance…

Virtualization and Cloud

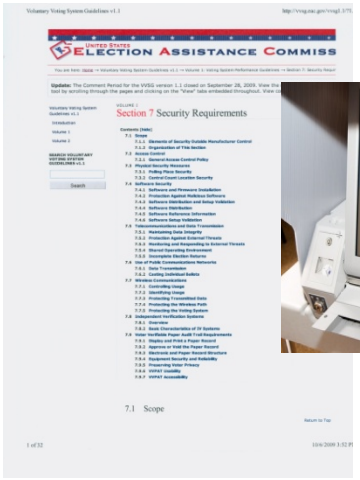
- Support for cloud special publication and standards activities to support security, portability and interoperability

Key Management

- Foster the requirements of large-scale key management frameworks and designing key management systems
- Support transitioning of cryptographic algorithms and key sizes

Next Generation Cryptography

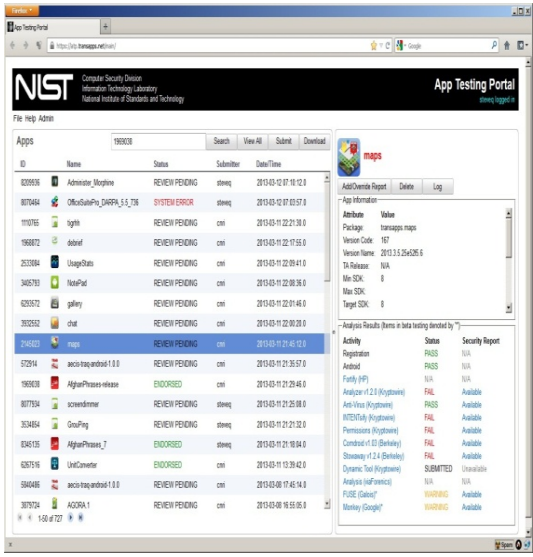
- Open competition for new Hash algorithm
- Developing new, light weight, quantum resistant encryption for use in current and new technologies
- New modes of operation



Secure Mobility

Focuses on research and development in the area of mobile security including mobile application testing and mobile

- Guidelines for Testing and Vetting Mobile Applications
- Mobile App Software Assurance Requirements
- Mobile Roots of Trust



Supply Chain

Work with industry, academic, and government stakeholders to develop foundational definitions, baseline requirements, general implementation methodologies, and a set of supply chain risk management best practices encompassing the system development lifecycle

Trusted Roots of Hardware

Collaborate with industry to develop guidelines that identify security properties for hardware trust roots

Network Security

Foster requirements for secure networking technology such as DNSSEC, IPv6 and BGP technologies

Cyber Physical System Security

Collaboration with industry in developing, integrating, and utilizing cybersecurity standards and mechanisms capable of providing appropriate protection for cyber physical systems, Internet of Things and Sensor Networks

Usability of Security

Performing groundwork research to define factors that enable usability in the area of multifactor authentication and developing a framework for determining metrics that are critical to the success of usability

Identity Management Systems

Standards development work in biometrics, smart cards, identity management, and privacy framework.

R&D: Personal Identity Verification, Match-On-Card, ontology for identity credentials, development of a workbench

ID Credential Interoperability

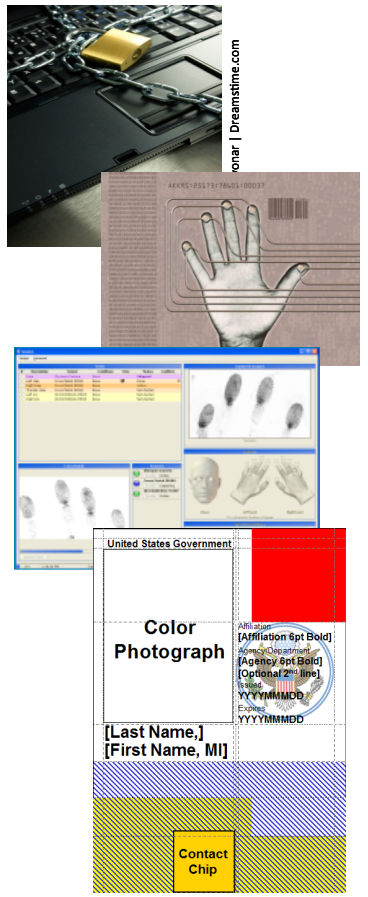
Infrastructure Support

Cybersecurity for application infrastructure including Health Information Technology, Smart Grid and Voting

Standards Development Organizations

IETF ANSI

IEEE ISO



National Initiative For Cybersecurity Education (NICE)

NICE is "enhancing the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population."

NIST, as the interagency lead for NICE, promotes the coordination of existing and future activities in cybersecurity education, training, and awareness to enhance and multiply their effectiveness

Raise national awareness about risks in cyberspace.
Broaden the pool of individuals prepared to enter the cybersecurity workforce.
Cultivate a globally competitive cybersecurity workforce.

National Strategy for Trusted Identities in Cyberspace (NSTIC)

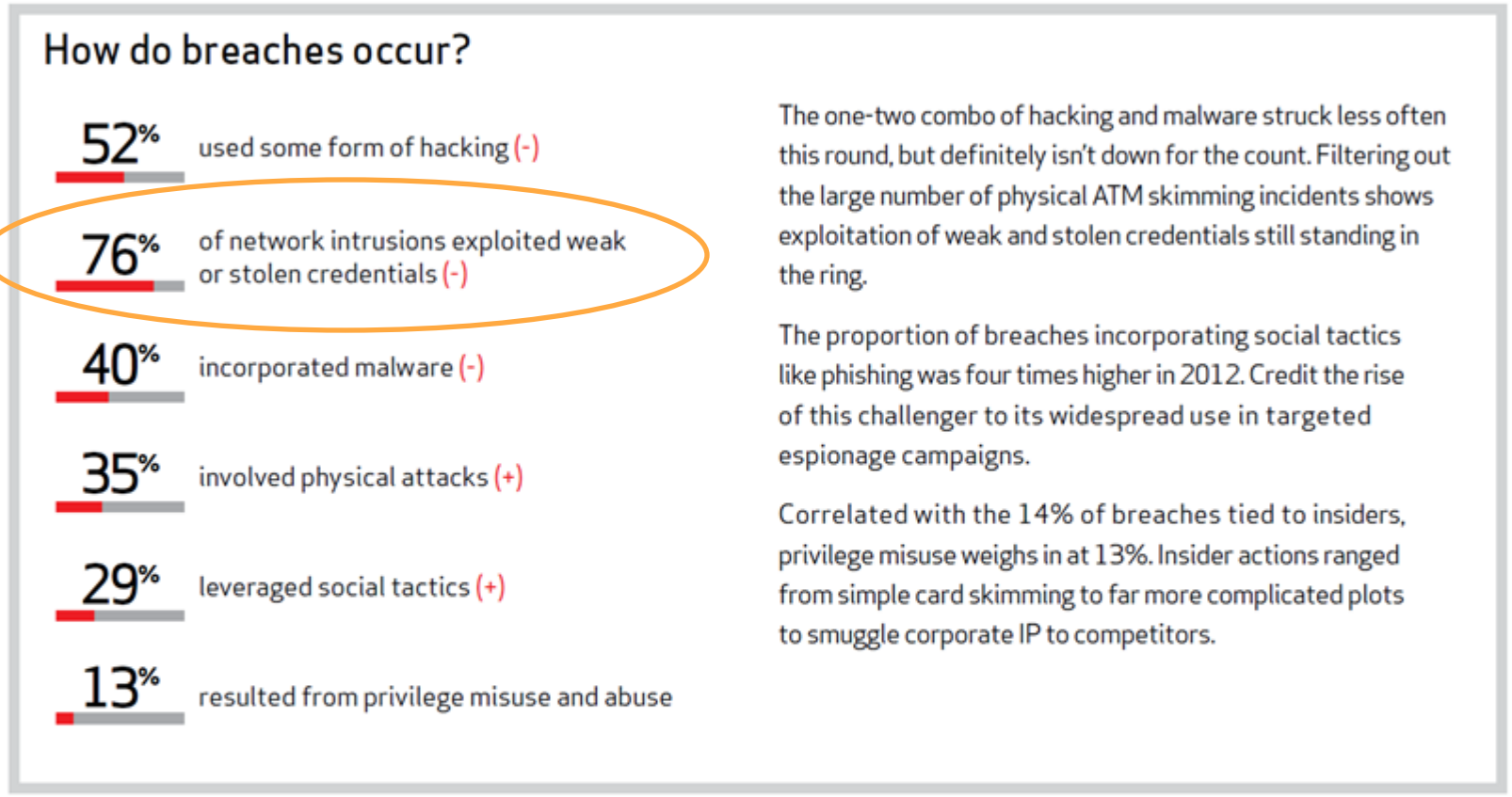
President's Cyberspace Policy Review (May 2009):
a "cybersecurity focused identity management vision and strategy…that addresses privacy and civil-liberties interests, leveraging privacy-enhancing technologies for the nation."

Guiding Principles

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use

NSTIC calls for an **Identity Ecosystem**, "an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities."

Why NSTIC?



Source: 2013 Data Breach Investigations Report, Verizon and US Secret Service

There is a marketplace today – but there are barriers the market has not yet addressed on its own

Key Implementation Steps

- Engage the Private Sector
  - Identity Management Ecosystem Steering Committee
- Fund Innovative Pilots to Advance the Ecosystem
- Government as early implementer
- Identify standards and best practices and fill gaps

National Cybersecurity Center of Excellence (NCCoE)

Accelerated adoption of practical, affordable, and usable cybersecurity solutions

Integrated cybersecurity solutions, built on commercial technologies, designed to address a sector's specific business needs

Increased opportunities for innovation through the identification of technology gaps

Trusted environment for interaction among businesses and solution providers

Further the understanding of current cybersecurity technology capabilities and the cost of their implementation

Broader awareness of cyber security technologies and standards

NCCoE

Use Cases

Energy

Identity and Access Management

Situational Awareness

Health

Mobile Device Management

Financial Management

Access Rights Management

IT Assess Management

Building Blocks

Trusted Geolocation in the Cloud

Software Asset Management

Attribute Access Control

Mobile Device Security

Executive Order 13636—Improving Critical Infrastructure Cybersecurity

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

NIST is directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure.

This Cybersecurity Framework is being developed in an open manner with input from stakeholders in industry, academia, and government, including a public review and comment process, workshops, and other means of engagement.

The Cybersecurity Framework

For the Cybersecurity Framework to meet the requirements of the Executive Order, it must:

- 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* that should be addressed through future collaboration with particular sectors and standards-developing organizations able technical innovation and account for organizational differences include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

Framework Components

Framework Core

Cybersecurity activities and references that are common across critical infrastructure sectors organized around particular outcomes.

Enables communication of cybersecurity risk across the organization.

Framework Profile

Alignment of industry standards and best practices to the Framework Core in a particular implementation scenario.

Supports prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation.

Framework Implementation Tiers

Describe how cybersecurity risk is managed by an organization.

Describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics (e.g., risk and threat aware, repeatable, and adaptive).

Partial (Tier 1), Risk-Informed (Tier 2), Risk-Informed and Repeatable (Tier 3), Adaptive (Tier 4).

Framework Core

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Definitions of Tiers (Excerpts)

Tier 1: Partial

- **Risk Management Process:** Organizational cybersecurity risk management practices are not formalized and risk is managed in an ad hoc and sometimes reactive manner.
- **Integrated Program** – There is a limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established.

Tier 2: Risk-Informed

- **Risk Management Process** – Risk management practices are approved by management but may not be established as organizational-wide policy.
- **External Participation** – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally

Tier 3: Risk-Informed and Repeatable

- **Integrated Program:** There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and validated.
- **External Participation:** The organization understands its dependencies and partners and receives information from these partners enabling management decisions.

Tier 4: Adaptive

- **Risk Management Process:** The organization adapts its cybersecurity practices based on lessons learned and predictive.
- **External Participation:** The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed before an event occurs.

Solving all of these challenges

- Changing Culture
- Talents from a wide variety of disciplines
- Better Metrics
- Computer Scientists, Engineers, Mathematicians
  - Build in cybersecurity
  - Complexity
  - Testing

Resiliency, Safety, Privacy, Security

For Additional Information

- http://csrc.nist.gov
- http://csrc.nist.gov/nice/
- http://www.nist.gov/nstic/
- http://nccoe.nist.gov
- http://www.nist.gov/cyberframework/