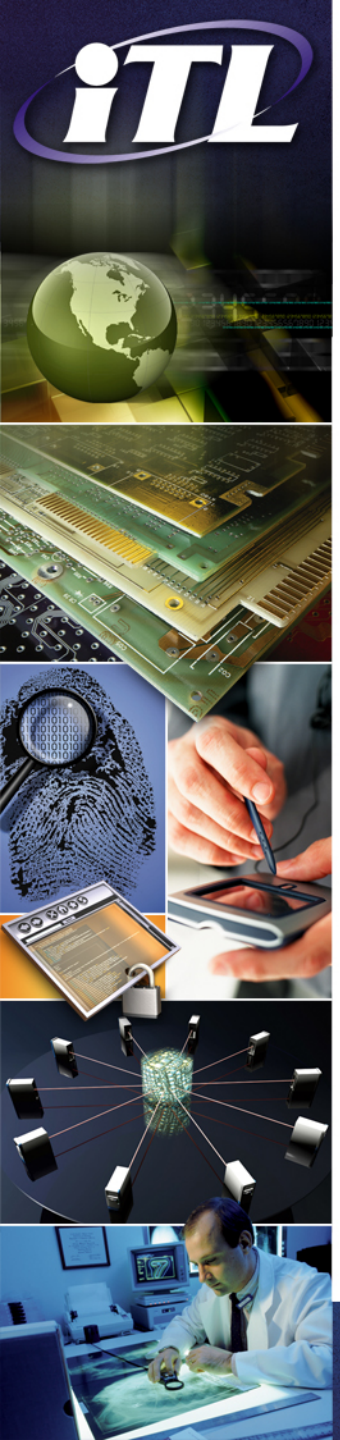


Cybersecurity

and the Cloud

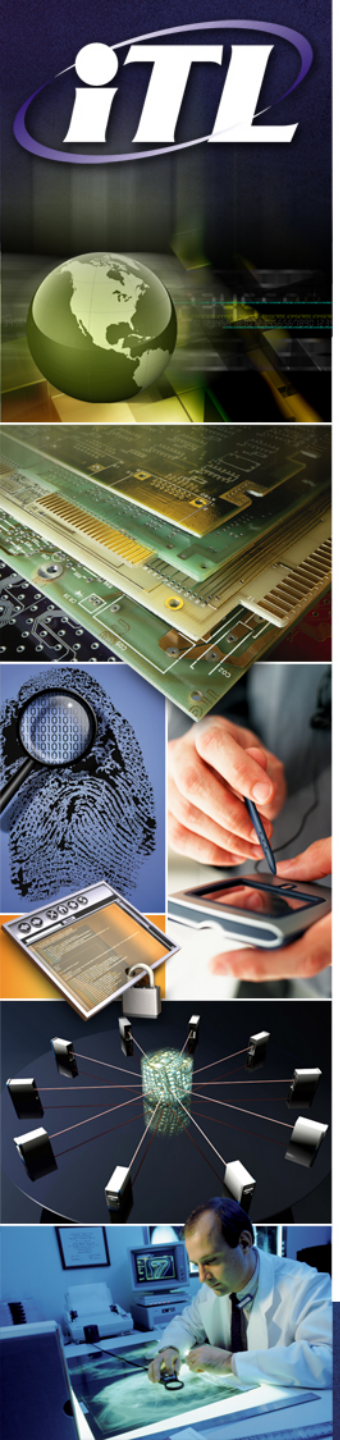
4TH Annual NICE Workshop

Navigating the National Cybersecurity Education InterState Highway

September 2013

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Well, I'll hazard I can do more damage on my laptop sitting in my pajamas before my first cup of Earl Grey than you can do in a year in the field.

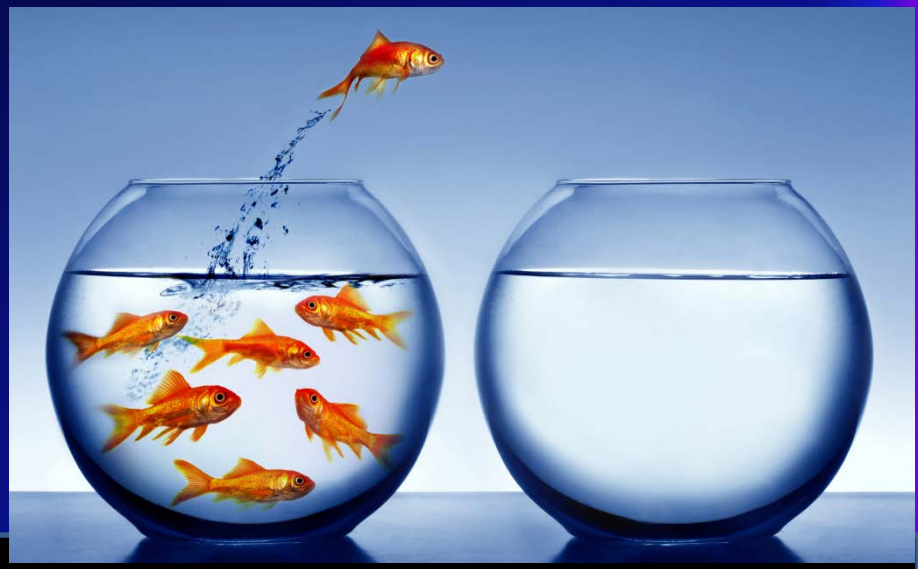


Cyber Security

Cyber Security
What is at stake?

If someone has your information system, they have

- your intellectual property,
- your national/trade secrets,
- your identity,
- YOU, and
- your freedom.



Known Threats

Apart from human behavior, what do we worry about?

- Hostile cyber attacks
- Natural disasters
- Structural failures
- Human errors of omission or commission

the WHITE HOUSE PRESIDENT BARACK OBAMA

BLOG | PHOTOS & VIDEO | BRIEFING ROOM | ISSUES | the ADMINISTRA

Home • Briefing Room • Presidential Actions • Executive Orders

The White House
Office of the Press Secretary

E-Mail | Tweet | Share | +

For Immediate Release — February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Flip side of the coin

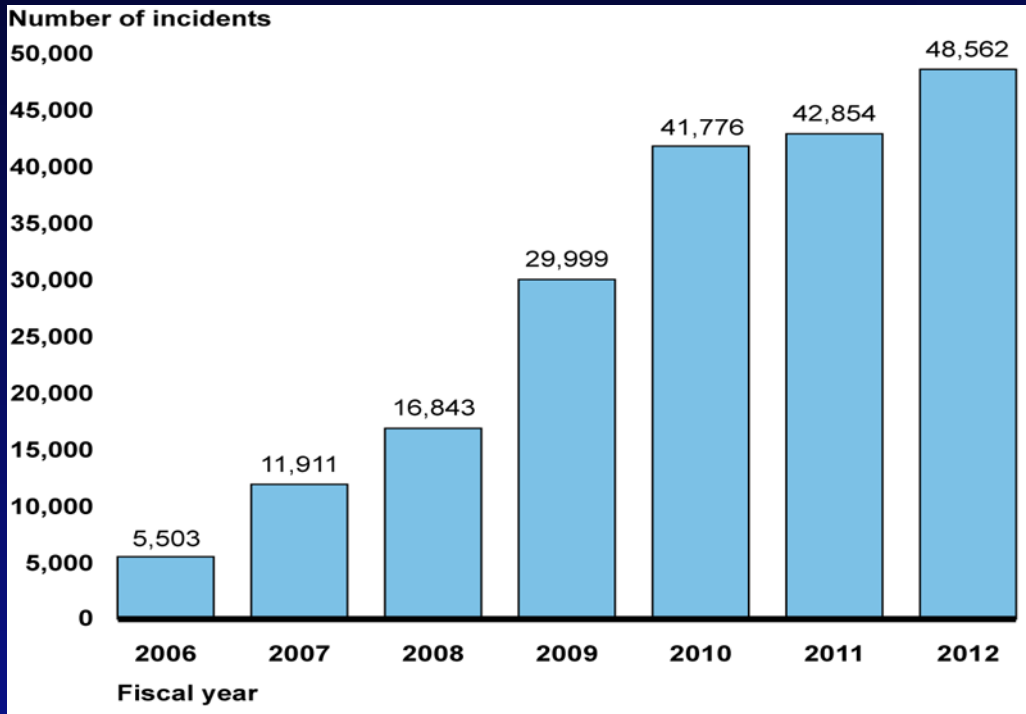
Complexity

Connectivity

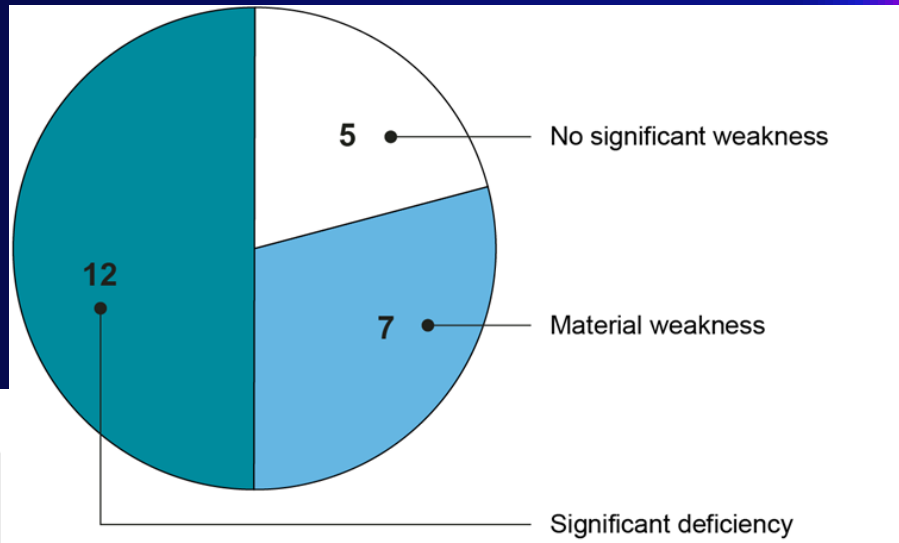
Culture

Reviews

Reported security incidents continue to rise

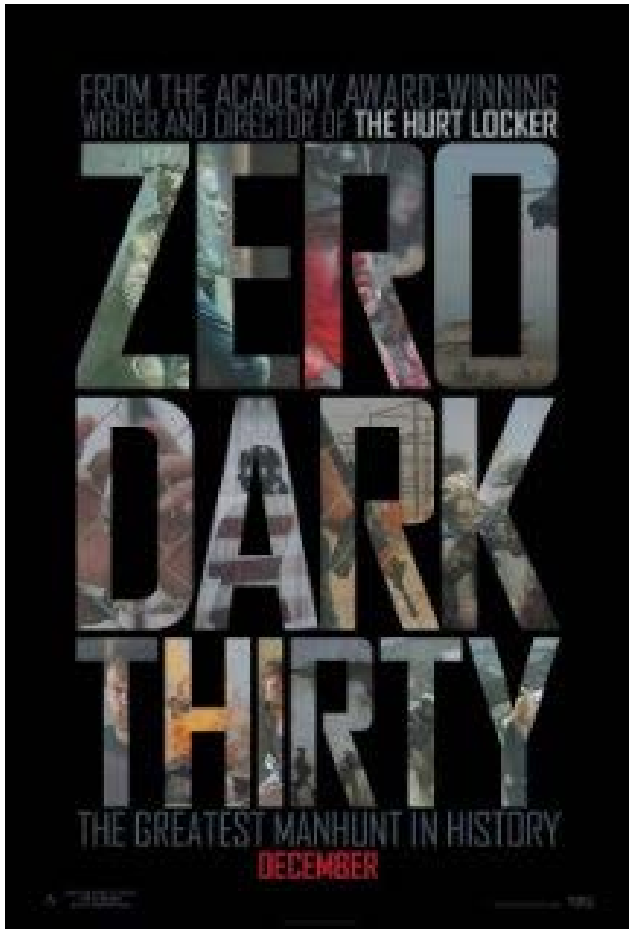


Source: GAO analysis of US-CERT data for fiscal years 2006-2012.



Source: GAO analysis of agency performance and accountability reports, annual financial reports, or other financial statement reports for fiscal year 2012.

Agencies continue to report information security deficiencies for financial systems



Who or what is the target?

Do you remember how long they were looking for clues?

What was the break-through?

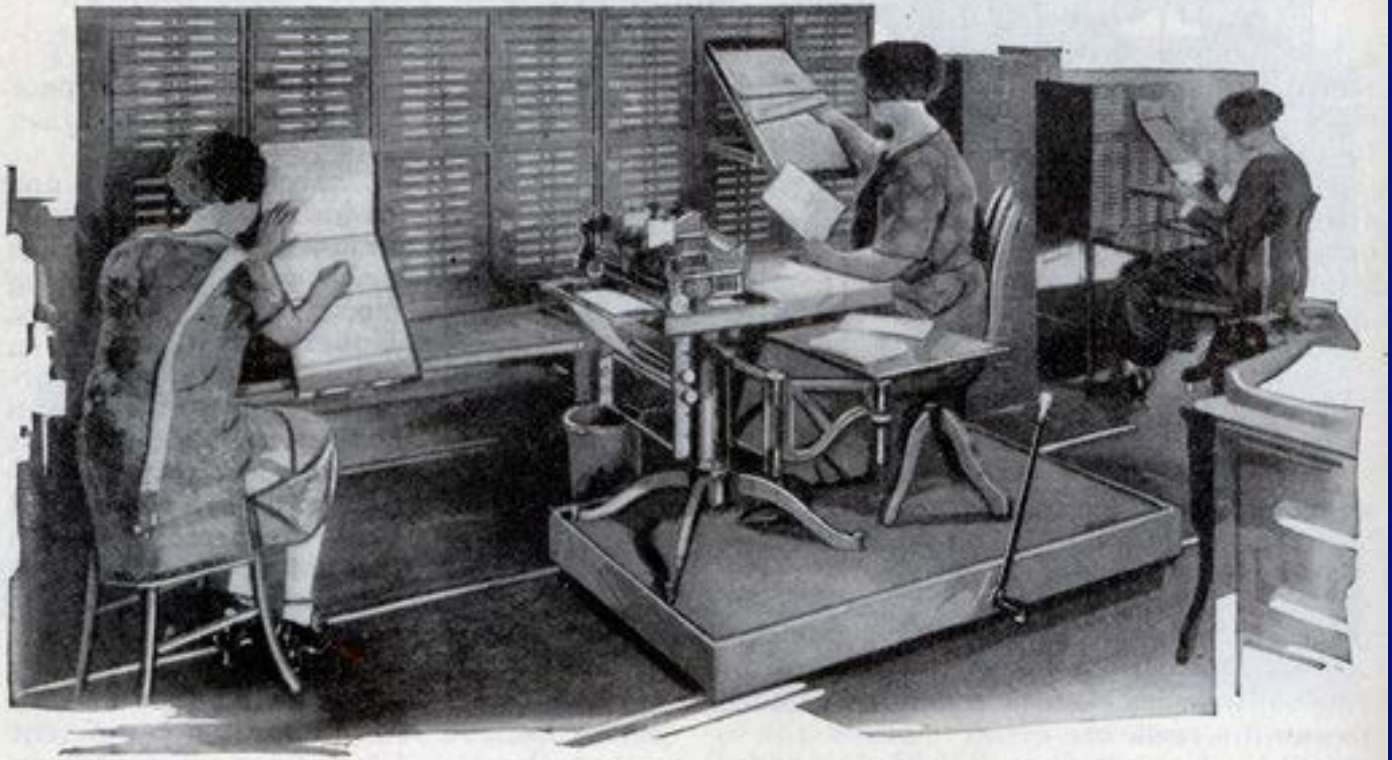
How do threats work?

- Adversary has certain skills and resources
- Design strategic opportunities for specific targets

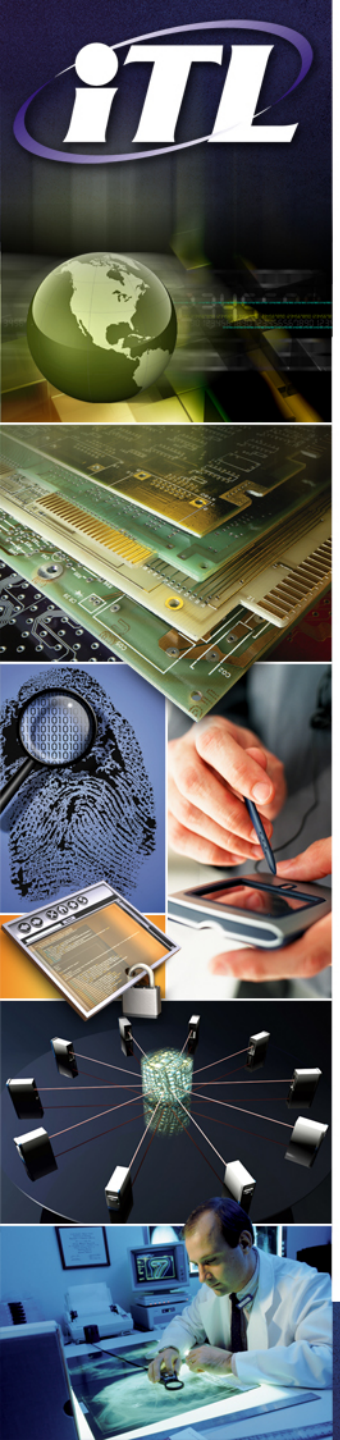
- Continue monitoring for vulnerabilities
- Establishes footholds within IT infrastructure

Bookkeeper on Moving Platform Saves Time in Reaching Files

Time and effort in referring to a large filing index in a busy office are saved by placing a billing machine and its operator on a platform which moves on rails. The carriage is anchored by a hand brake, conveniently placed, and when the operator wishes to move to another case, she releases the handle and pushes herself, machine and all, to the next position.



Moving Platform for Bookkeeper and Billing Machine Rolls, by a Slight Push from the Operator, beside Filing Cabinet on Rails and Is Anchored by Brake



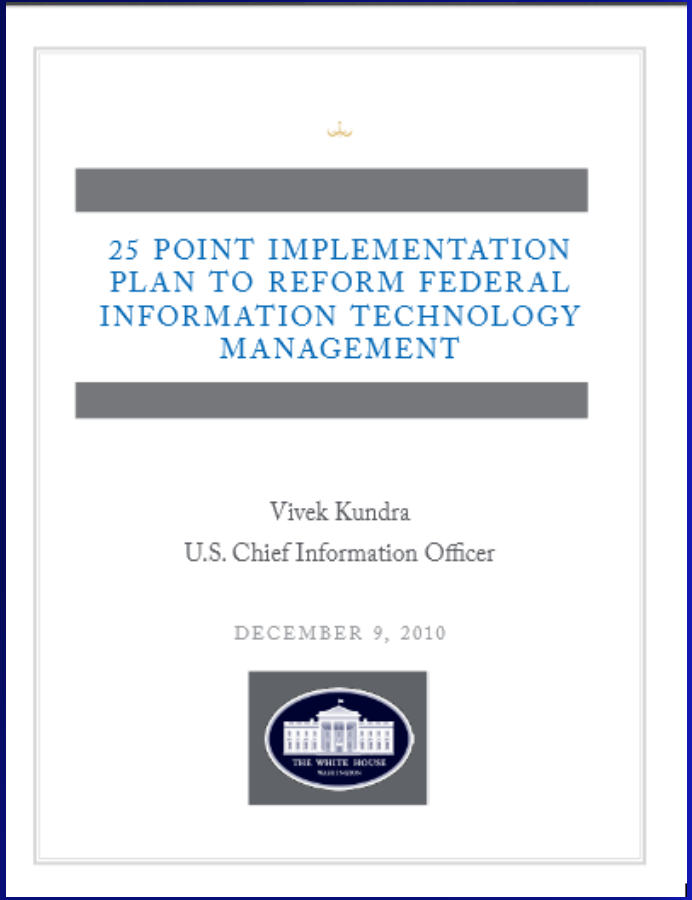
Technology

Cloud First

NIST Cloud Computing Forum and Workshop I, May 2010

Cloud Computing Technology Roadmap, 2011

NIST Cloud Computing Definition, SP 800-145, 2011


25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL INFORMATION TECHNOLOGY MANAGEMENT

Vivek Kundra

U.S. Chief Information Officer

DECEMBER 9, 2010

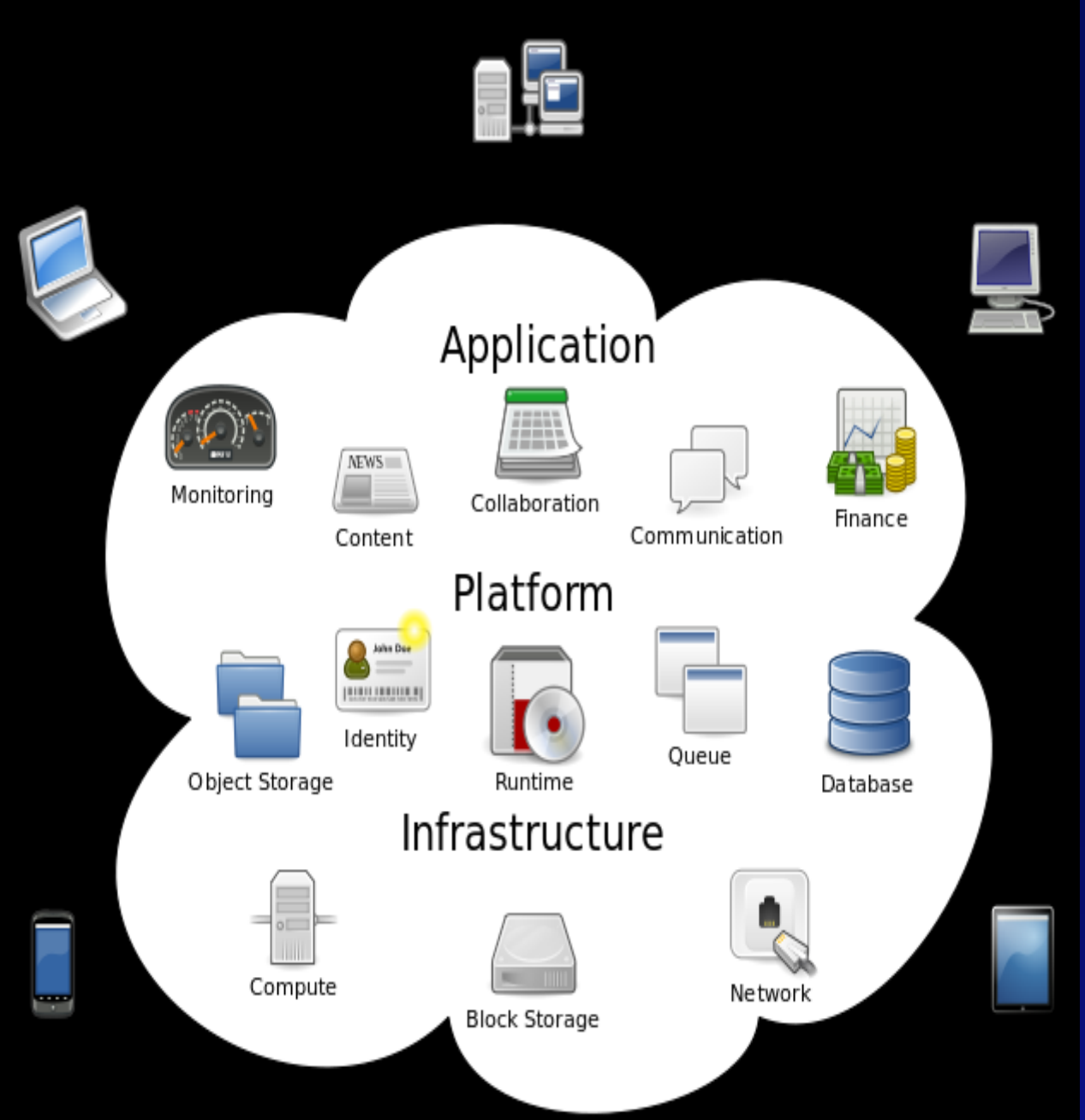
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance



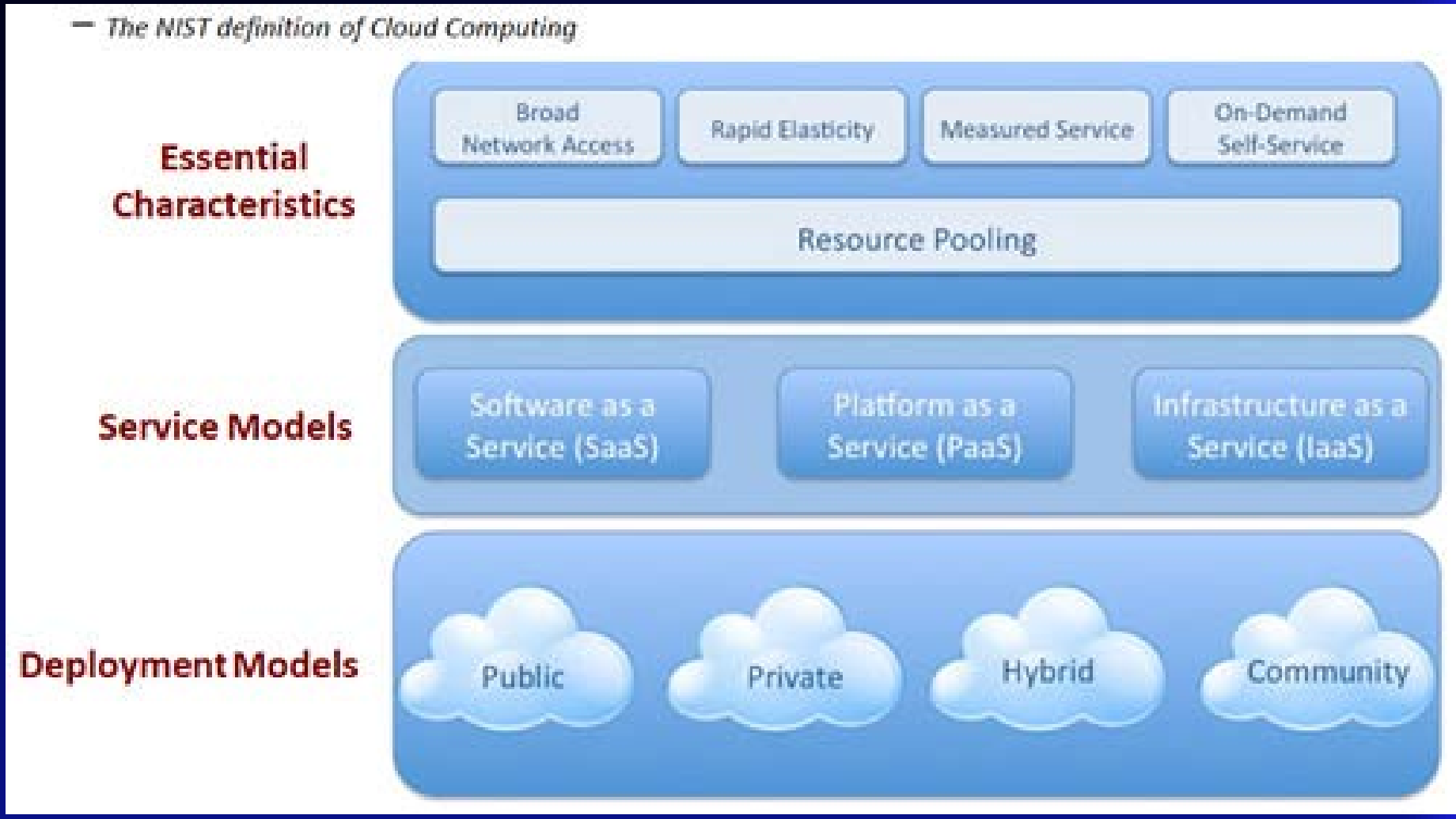
NIST Definition of Cloud Computing

NIST Special Publication 800-145

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. , networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

NIST Definition of Cloud Computing

– *The NIST definition of Cloud Computing*



Cloud Deployment Models

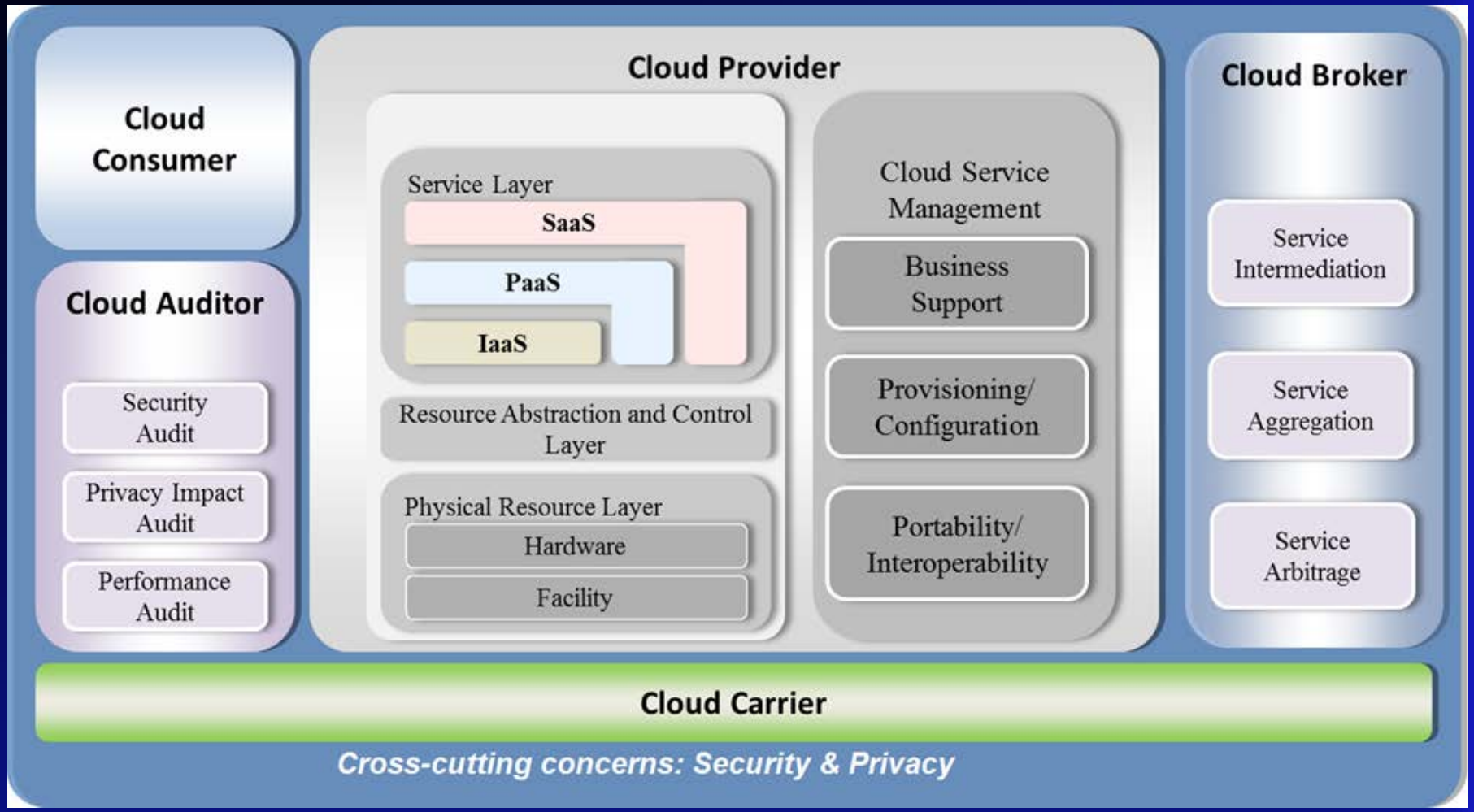
Public The cloud infrastructure is made available to the general public or a large industry group and is owned by a third-party provider selling cloud services.

Private The cloud infrastructure is operated solely for an organization. It may be managed by that organization or a third party and may exist on or off premises.

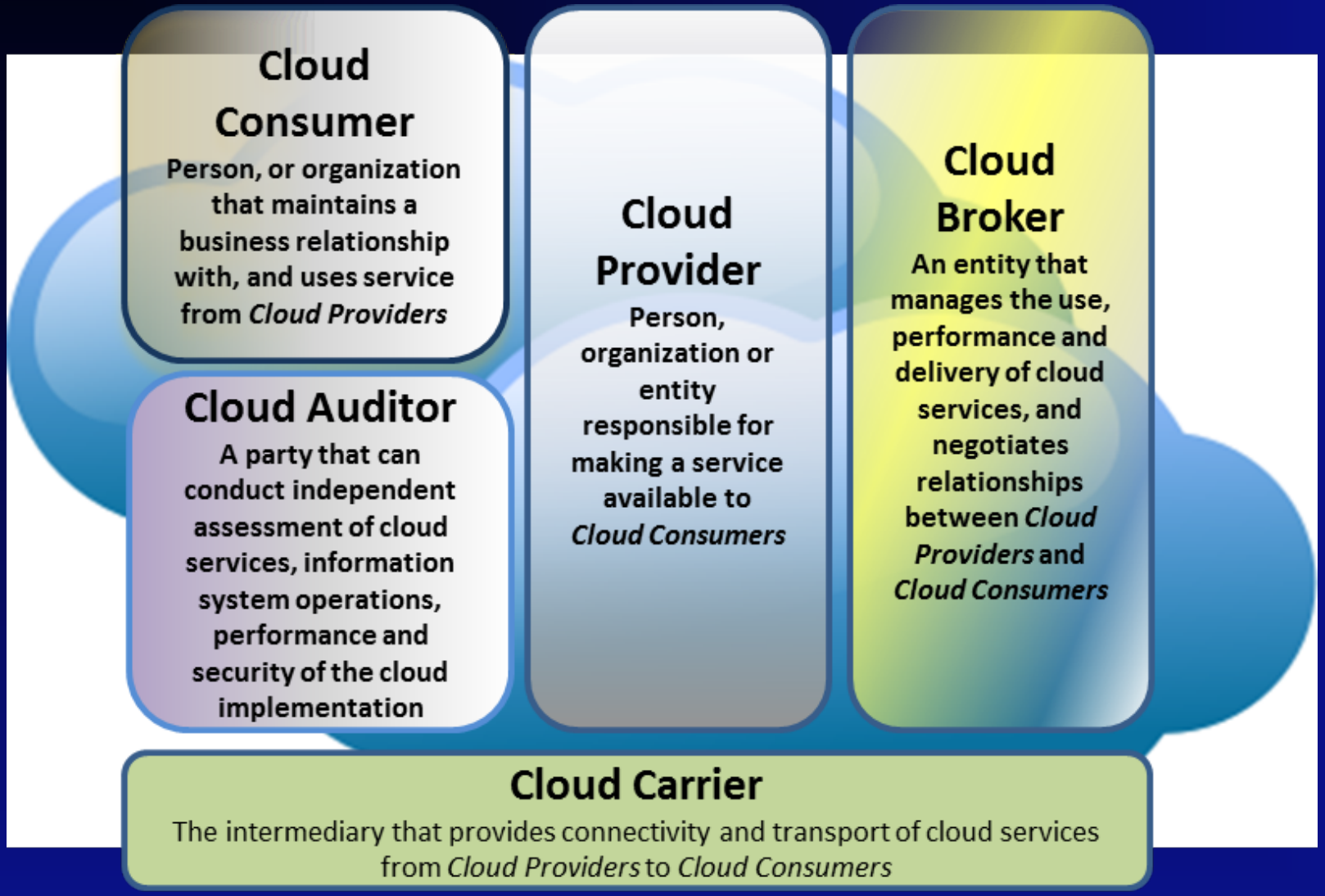
Community The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on or off premises.

Hybrid A composition of two or more clouds (public, private, community) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

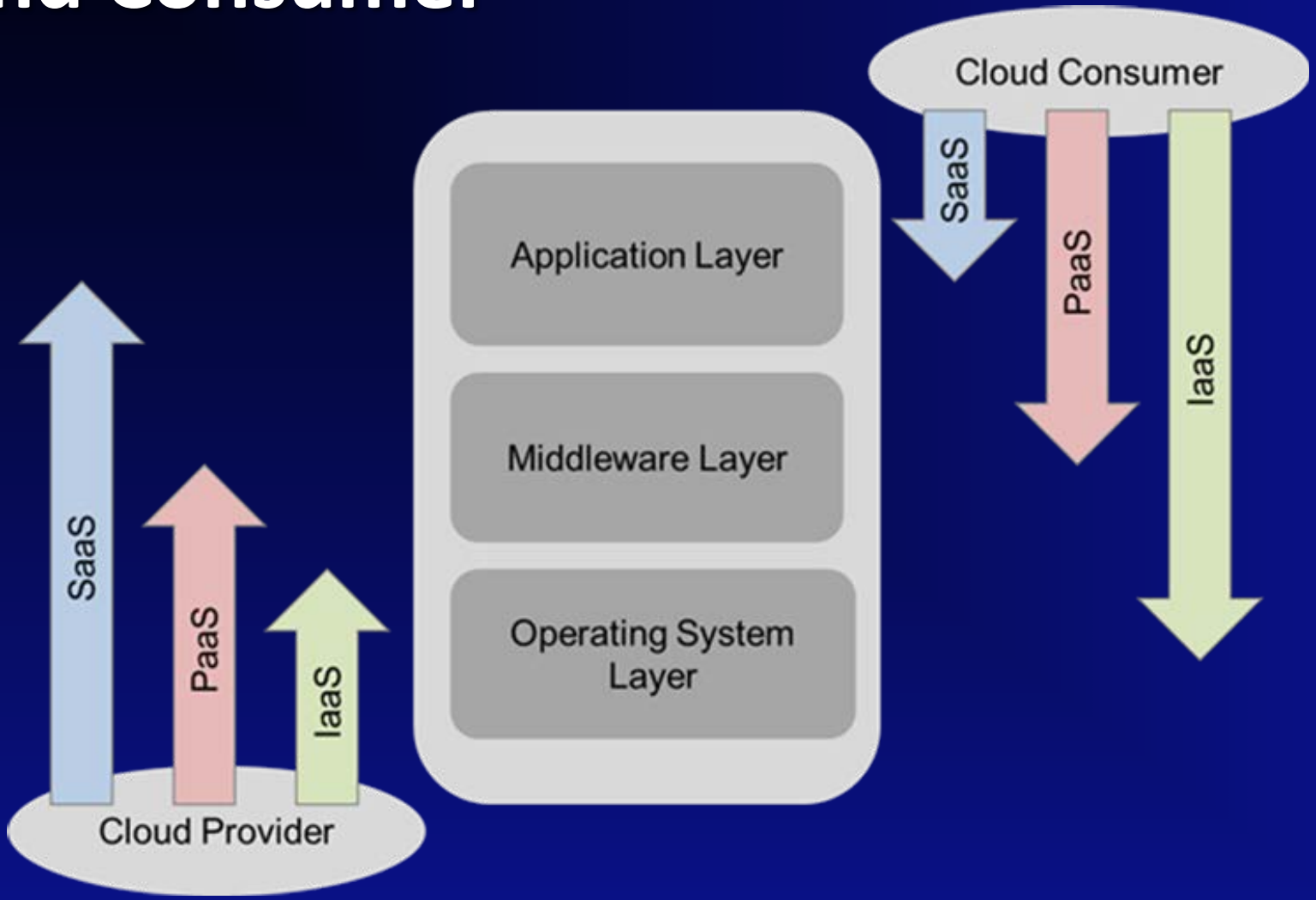
SP 500-292: Conceptual Reference Model



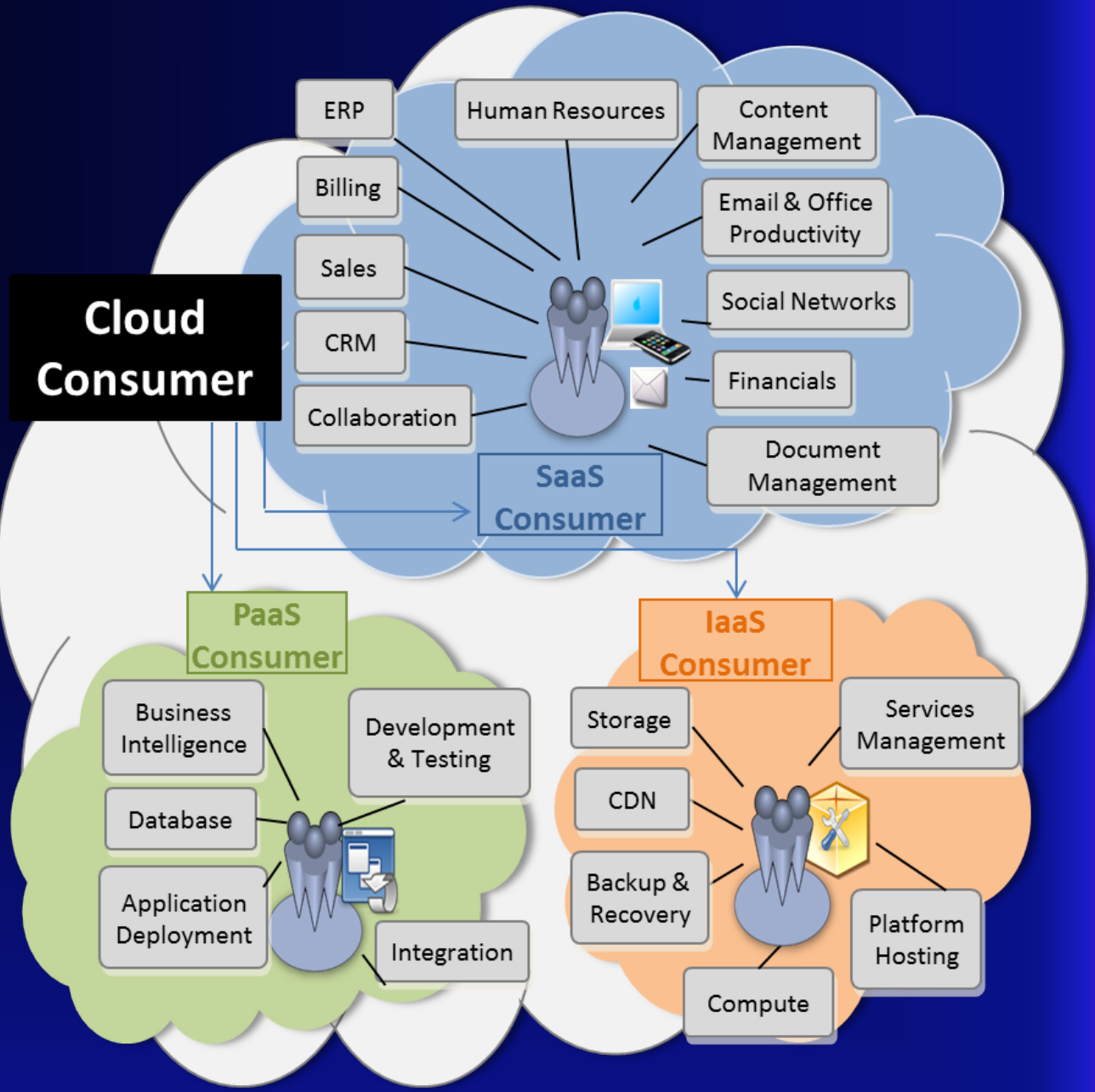
SP 500-292: Five Major Actors



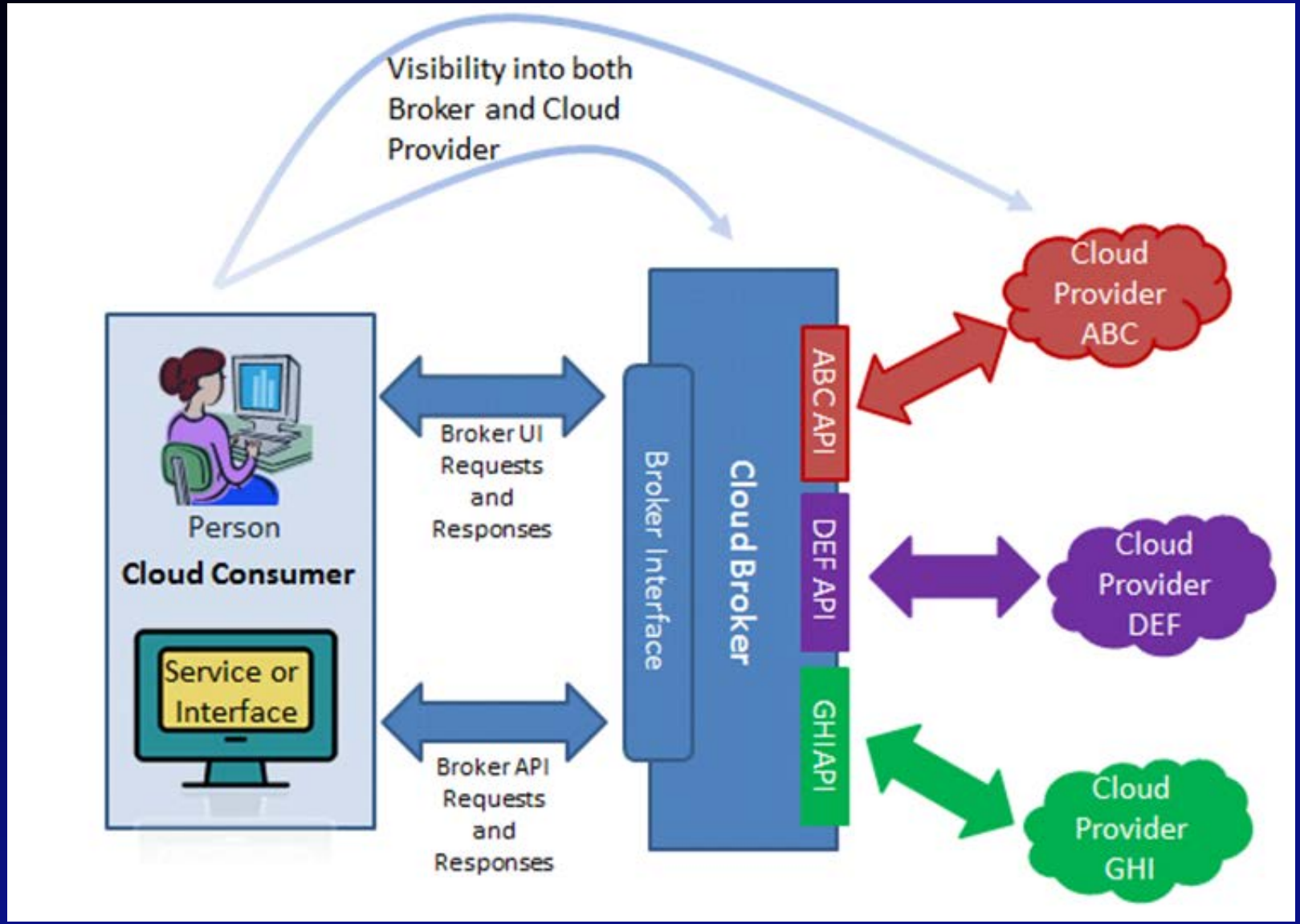
Scope of Controls between Provider and Consumer



Service Models and Actors' Activities



Cloud Broker Interactions



Simple and Complex

Security and Privacy are cross cutting functions of all layers of cloud computing reference architecture.

We have a naïve confidence in the digital environment

We cannot rely on technology makers to think about moral and privacy concerns.

Cloud Deployments

Cloud Deployments in Perspective

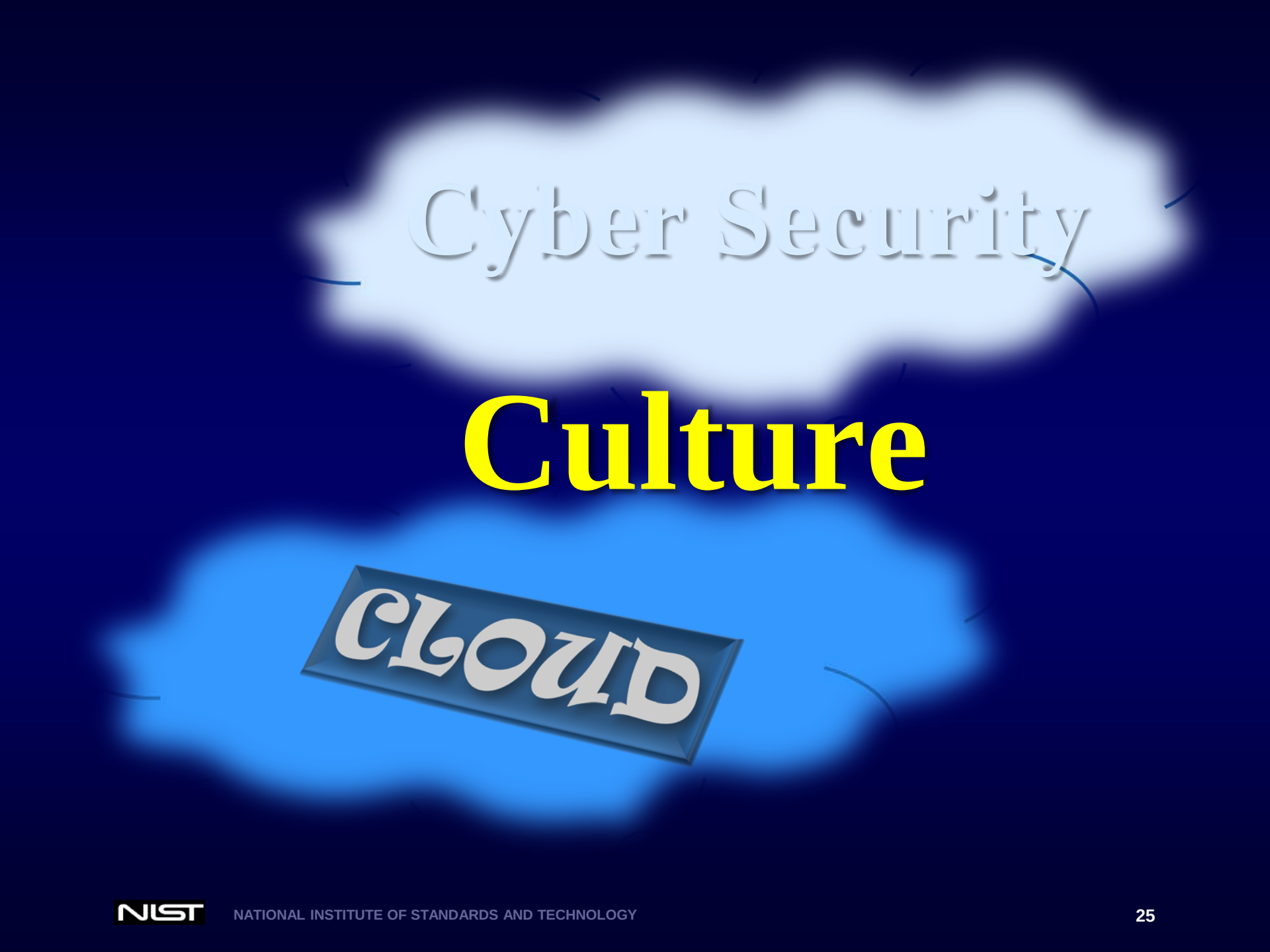
Almost two in five of those surveyed said they would rather get a root canal, dig a ditch, do their own taxes than address network challenges associated with public or private cloud deployments.

(The 2012 Cisco Global Cloud Networking Survey)

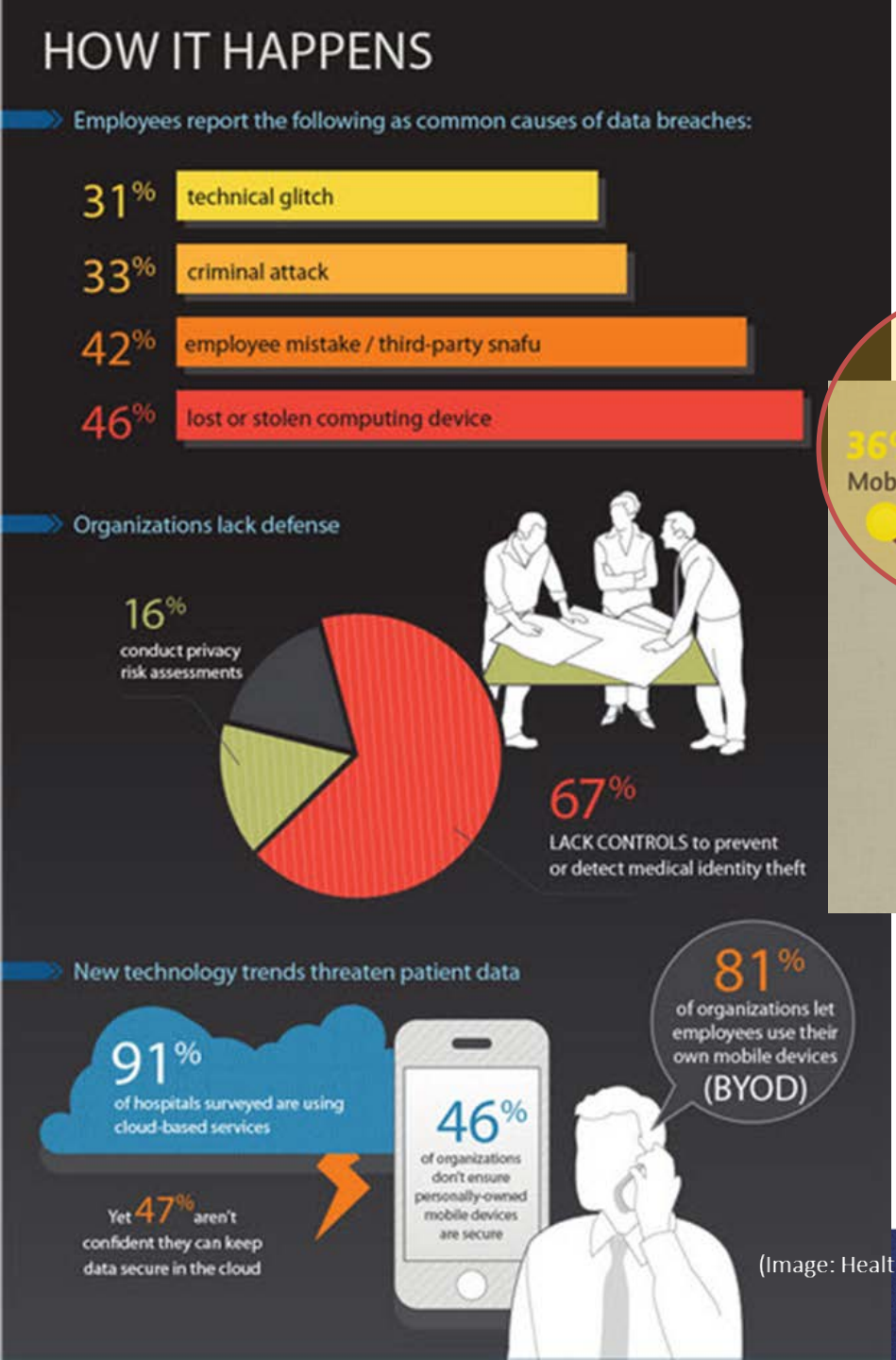
Privacy

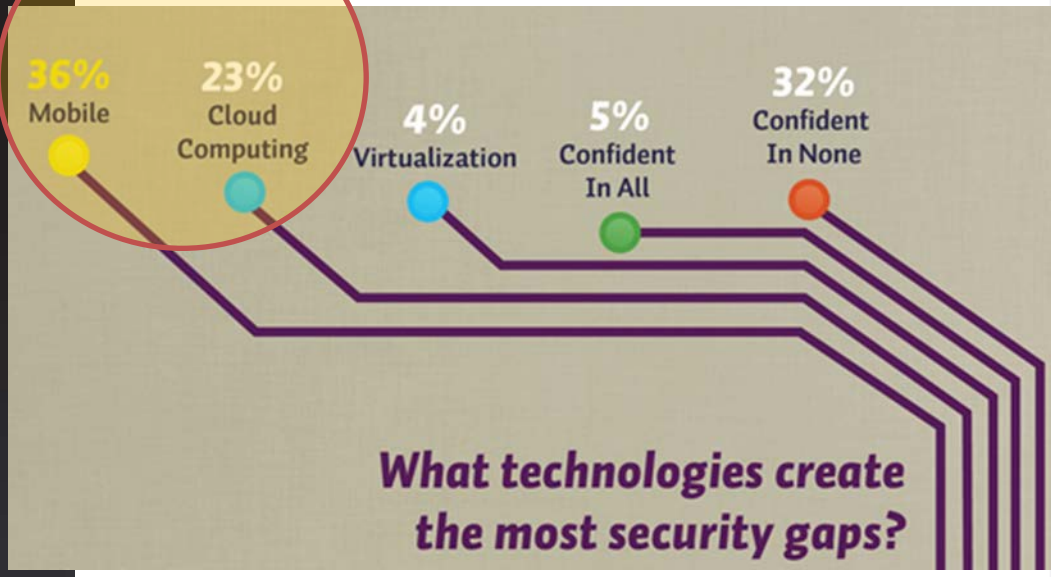
Nearly two in five participants said they would not trust their own personal information –such as medical records and Social Security numbers – with the cloud provider they are currently using

(The 2012 Cisco Global Cloud Networking Survey)


Cyber Security
Culture
CLOUD

What are the weakest links?





(Image: Health breach infographic. Source Ponemon Institute)

Digital use behavior

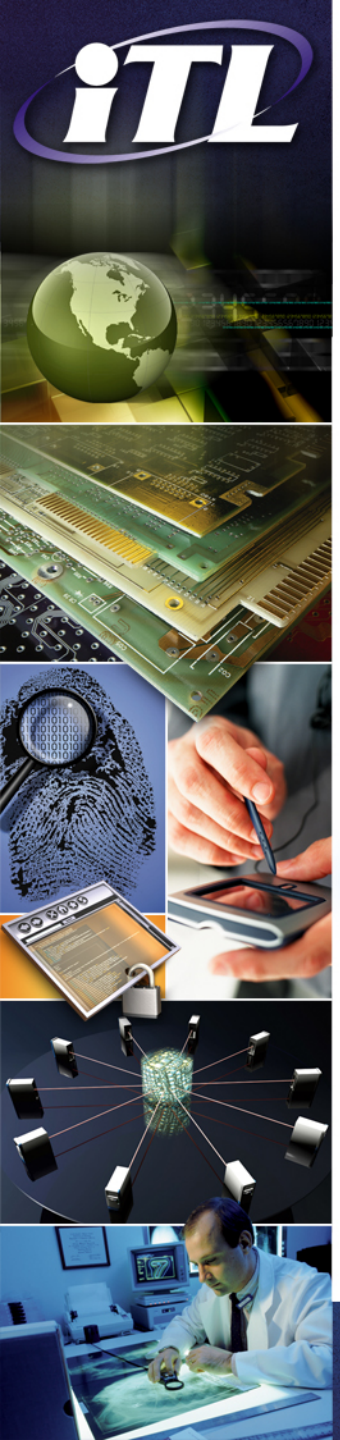
- A new survey has revealed significant differences between millennials and baby boomers when it comes to attitudes towards the internet.
- Consumers rate privacy as more important than ever, yet they have less control over when and where their personal information is shared more than ever before.

some 4-year-olds can download apps before they can put on their own shoes.

Technology is changing behavior

Disruptions: For Teenagers, a Car or a Smartphone?

"Mobile devices, gadgets and the Internet are becoming must-have lifestyle products that convey status," said Thilo Koslowski, lead automotive analyst for Gartner. "In that sense these devices offer a degree of freedom and social reach that previously only the automobile offered." …And maybe one day, the car could even drive itself so teenagers could text away without worrying about driving.



Cyber Security

CLOUD

Incidences

- Stuxnet – was the first cyber attack recognized as being made possible by compromised digital certificates.
- Diginoar – attack on a Certificate Authority (CA) marked a significant point in the history of cyber attacks.
- Malware signed by stolen certificate grow 10x
- Hackers compromised security provider's network
- Trojans launches designed to steal keys and certificates
- Human factor
- .....

2012 Data Breach Investigations Report

WHAT COMMONALITIES EXIST?

79% of victims were targets of opportunity (-4%)

96% of attacks were not highly difficult (+4%)

94% of all data compromised involved servers (+18%)

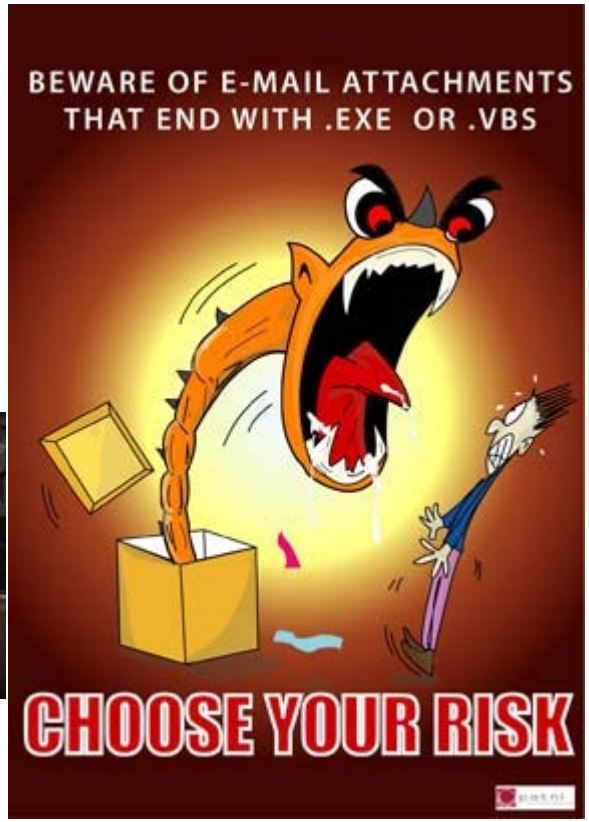
85% of breaches took weeks or more to discover (+6%)

92% of incidents were discovered by a third party (+6%)

97% of breaches were avoidable through simple or intermediate controls (+1%)

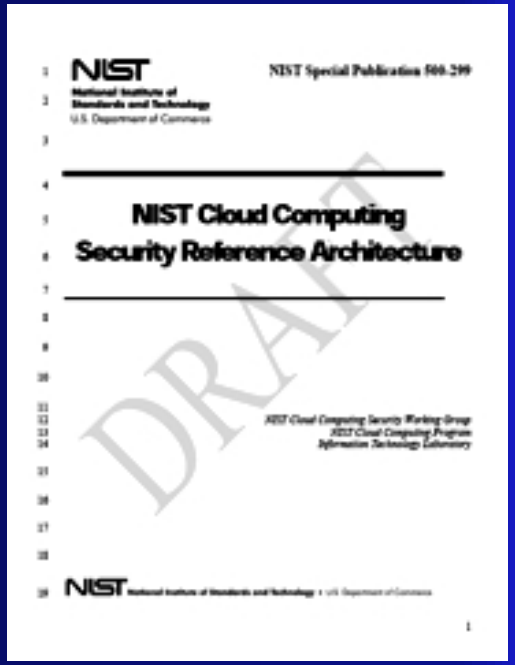
96% of victims subject to PCI DSS had not achieved compliance (+7%)

Is it possible to be 100% protected?



SP 500-299
Security Requirements Challenges

- Visibility for consumers
- Control for consumers
- Data security
- Risk of account hijacking
- Multi-tenancy risks and concerns
- Cloud-based Denial of Service
- Business Continuity and Disaster Recovery



Major Concerns

when thinking about adopting “Cloud”

- Security (and privacy)
  - Traditionally and conceptually:
    - **Confidentiality**: your data is not leaked
    - **Integrity**: your data or system is not corrupted
    - **Availability**: there is no interruption to your system
- Loss of control
- Integration
- Some issues
  - With dynamically changing infrastructure
  - Key management
  - virtualization

Consolidation

Assess requirements and risks

Define Defense and Strategy

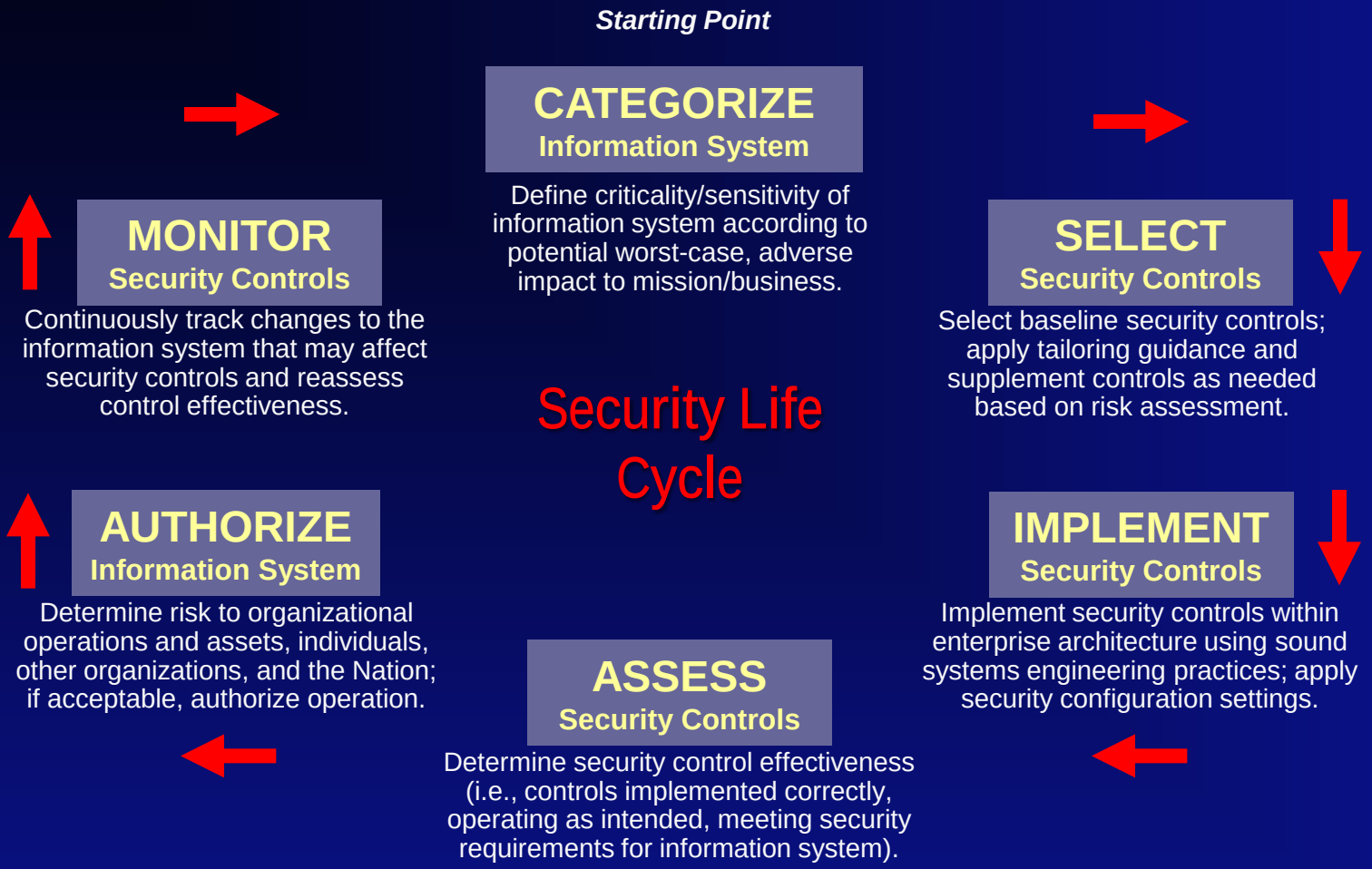
Make it simple and easy

Test and verify

Functionality and Assurance

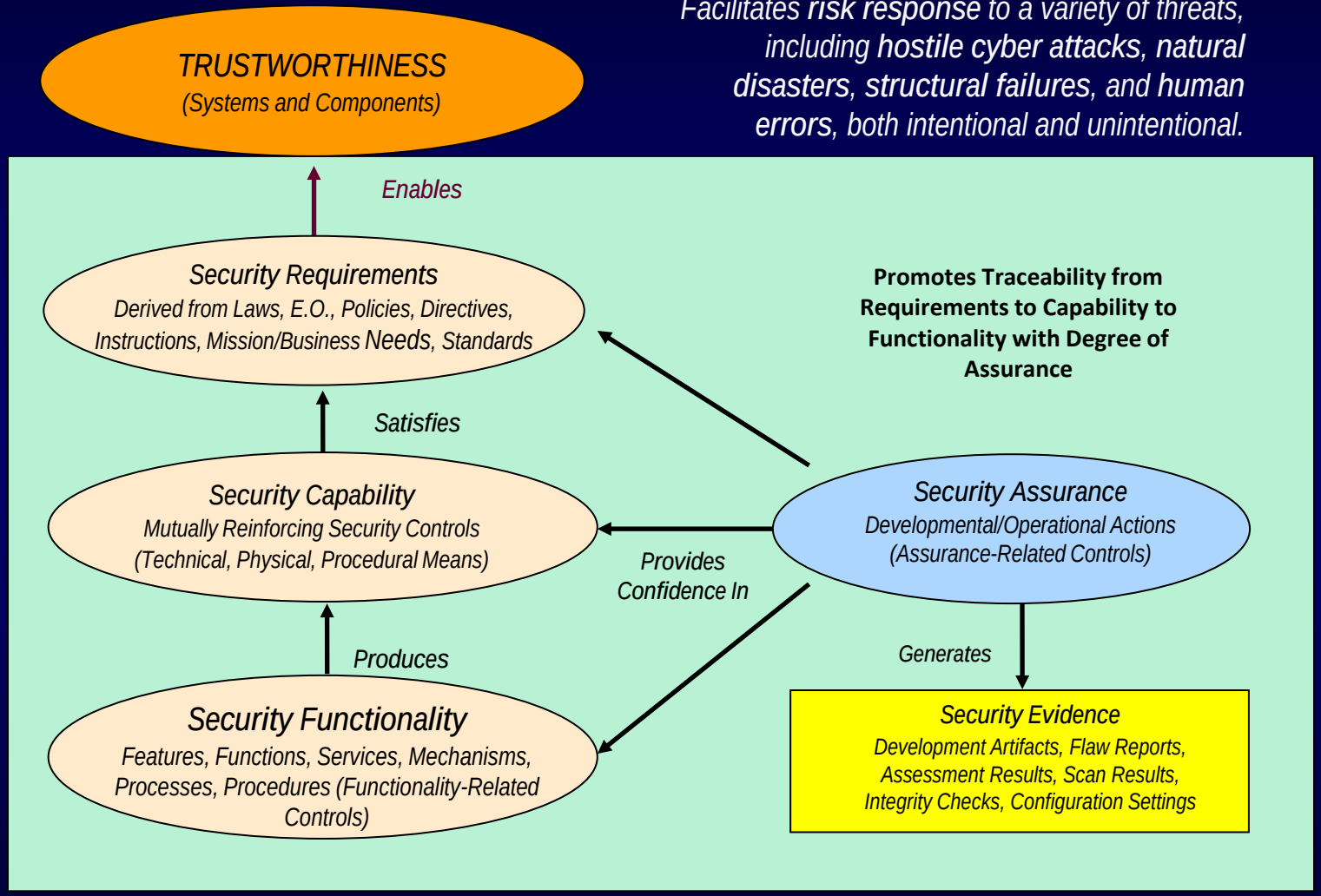
Vulnerabilities and compromises

Risk Management Framework



Assurance and Trustworthiness

*Facilitates **risk response** to a variety of threats, including **hostile cyber attacks**, **natural disasters**, **structural failures**, and **human errors**, both intentional and unintentional.*



Continuous Monitoring

- Determine effectiveness of risk responses.
- Identify changes to information systems and environments of operation.
- Verify compliance to federal legislation, Executive Orders, directives, policies, standards, and guidelines.

Bottom Line: Increase situational awareness to help determine risk to organizational operations and assets, individuals, other organizations, and the Nation.

Considerations for Cloud Strategy

- Costs, Risks, and Needs
- Encryption
- Determine and know location(s) of your server(s)
- Plan cloud strategy and roadmap
  - Made it *simple and flexible*
- Address security and privacy requirements
- Develop use cases and determine service model
- Examine Service Level Agreement
- Integration

It's not the *number* of security controls that matters…

It's having the *right* controls to do the job.

There are profound security challenges not only for clouds but also for traditional technologies.
Your future – the trust in and control over your cloud services depends on you.

Standards and Guidance

Goals of Standards Development

- Develop understanding of reference architecture
- Promote reliability, security, data portability, reversibility and service interoperability
- Provide cloud computing customers and users options in the marketplace
- Establish understanding and confidence to cloud computing customers and users in adopting cloud computing
- Enable production of a coherent set of international standards

- ISO 27000 Series
- ISO 27001 – Specification for an Information Security Management System (ISMS)
- ISO 27002 – code of practice for information security
- ISO 27003 – Implementing an Information Security Management System
- ISO/IEC CD 27018, Information technology – Security techniques – Code of practice for PII protection in public clouds acting as PII processors
- ISO/IEC 27033-1 — Network security overview and concepts
- ISO/IEC 27033-2 — Guidelines for the design and implementation of network security
- ISO/IEC 27033-3:2010 — Reference networking scenarios - threats, design techniques and control issues
- ISO/IEC 62443 – Network and System Security for industrial-process measurement and control

- 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 800-39
  Managing Information Security Risk: Organization, Mission, and Information System View
- 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
- NIST Special Publication 800-144
  Guidelines on Security and Privacy in Public Cloud Computing

REGISTER HERE
No Registration Fee!

The New Frontiers in IT and Measurement Science

Rapid advances in mobile cloud computing are bringing sweeping changes to the way mobile computing and communication services are delivered around the globe. More than an incremental change, mobile cloud computing is expected to radically alter users' working and life styles.

From Cloud & Mobility > To Cloud Mobility

Cloud provides ubiquitous, on-demand, elastic, self-configurable, cost effective computing. Mobile devices are accessible, convenient gadgets, with regional wireless communication services and limited data services that have limited computing and power resources.

Low-end mobile devices access diverse and scalable cloud computing resources and globally connected mobile enabled resources to receive unlimited mobile application services.

As part of its continuing cloud computing series, the National Institute of Standards and Technology (NIST) is hosting a new forum on Cloud and Mobility. Join fellow experts in the fields of cloud, mobility, and measurement for thought-provoking plenary talks, panel presentations, facilitated breakout discussion, poster sessions, and networking around these themes:

- Federal Perspectives on Cloud and Mobility
- The Vision for Cloud and Mobility
- Current State of Cloud and Mobility Intersections
- Intersections of Cloud and Mobility on the Horizon
- Bringing Mobility and Cloud Together
- Challenges and Lessons Learned
- Lessons Learned in Mobility
- Challenges for Cloud and Mobility, including
- Use Cases, Technologies, Consumer Issues
- Domain- and Sector-Specific Perspectives
- Path Forward to a Federated Mobile Cloud

Proactive Participation

The workshop agenda follows. Registrants are asked at registration to select their preferences for the following focused breakout sessions.

Tuesday, October 1	Wednesday, October 2	Thursday, October 3
FUTURE DIRECTIONS	**CHALLENGES**	**PATH FORWARD**
1. Federated Community Cloud Roadmap	2.1 Reliability Design Goals	3.1 Federated Mobile Cloud
2. Accessibility Cloud Roadmap	2.2 Privacy and Security Issues	3.2 Privacy and Security
3. Future Cloud: Implications for Mobility	2.3 Cloud-Enhancing Mobility Applications	3.3 Usability
4. Future Mobility: Implications for the Cloud	2.4 Ubiquitous Computing	3.4 Ubiquitous Computing

9/12/2013

http://www.nist.gov/itl/cloud/intersection-of-cloud-and-mobility.cfm

NIST Cloud Team

Abdella Battou
Robert Bohn, PhD.
Fred deVaulx.
Michaela Iorga, PhD.
Michael Hogan
John Messina
Eric Simmon

Annie Sokol
annie.sokol@nist.gov
301-975-2006