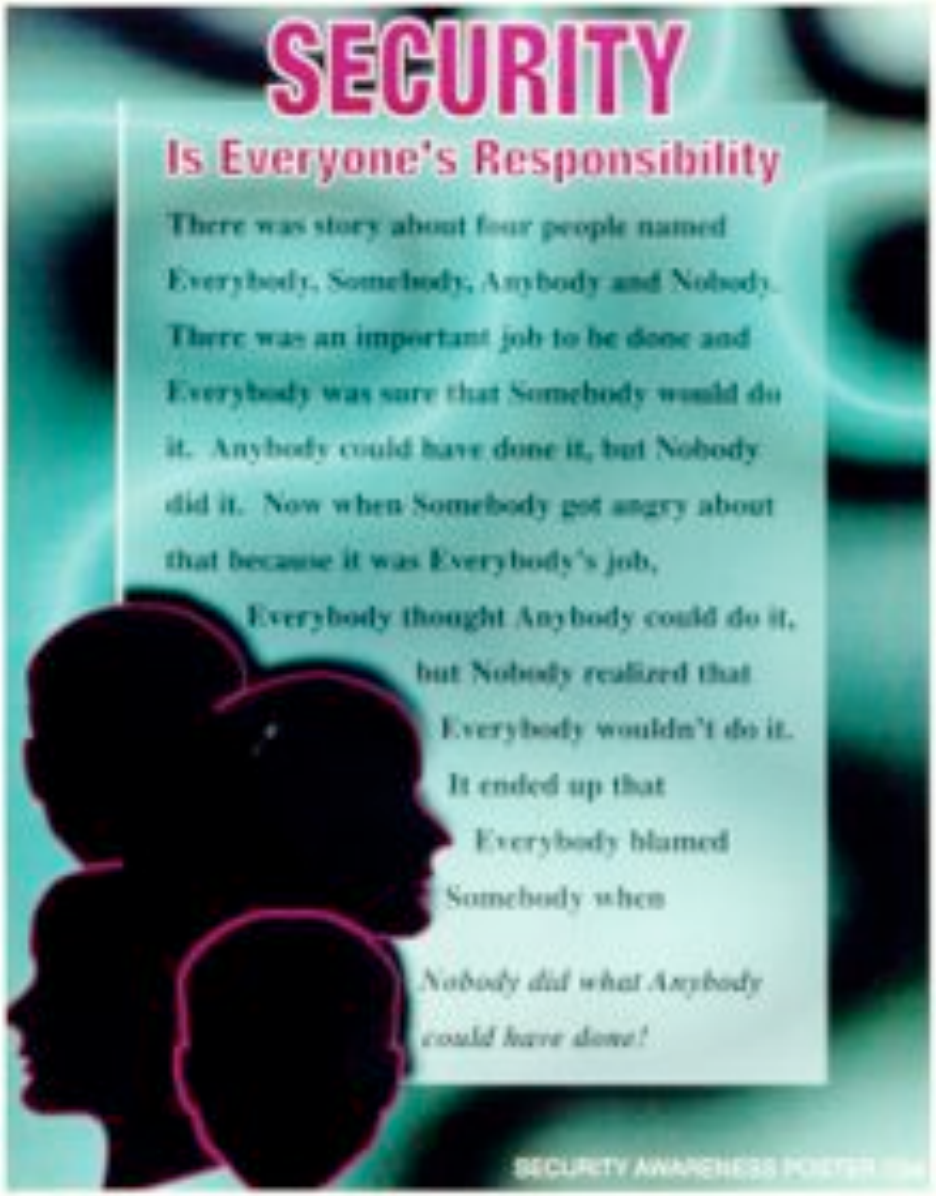


* Poster from US Department of Commerce

This is a little story about four people named Everybody, Somebody, Anybody, and Nobody.

There was an important job to be done and Everybody was sure that Somebody would do it.

Anybody could have done it, but Nobody did it.

Somebody got angry about that because it was Everybody's job.

Everybody thought that Anybody could do it, but Nobody realized that Everybody wouldn't do it.

It ended up that Everybody blamed Somebody when Nobody did what Anybody could have done

Best Practices in Cybersecurity that Might Be Useful to NSF Large Facilities

Ardoth Hassler

Updated: January 2011

A Work in Progress

"Cybersecurity is now a major national security problem for the United States."

- *Securing Cyberspace for the 44th Presidency:*
A Report of the Center for Strategic and International Studies

Washington, DC
December 2008

"…America's economic prosperity in the 21st century will depend on cybersecurity."

President Barack Obama
Washington, DC
May 29, 2009

"Throughout the developed world, governments, defense industries, and companies in finance, power, and telecommunications are increasingly targeted by **overlapping surges of cyber attacks** from ***criminals*** and ***nation-states*** **seeking economic or military advantage**."

– *SANS Institute*

http://www.sans.org/top-cyber-security-risks/

"The government is not going to secure the private sector. [But] we are making sure our [private sector] partners have more security as part of what we're doing."

- Howard Schmidt
White House Cybersecurity Coordinator
RSA Conference March 2, 2010

Introduction

- Community has asked for guidance on cybersecurity
- Cybersecurity Summit Meetings*
  - First Summit held after a major incident affected multiple large facilities
  - Opportunity to gather PIs and security professionals with program directors
  - Fifth Summit held September 2009
  - Next Summit is pending
- Summit outcomes have resulted in:
  - Closer workings within the community
  - NSF developing language about cybersecurity for the Cooperative Agreements

- This presentation is a work in progress.
- Your feedback is most welcome.

* Funded by NSF

Expanded Very Large Array

earth scope

NPACI

NHMFL

NCAR

LIGO

TeraGrid

NEES

Open Science Grid

GEMINI OBSERVATORY

WATERS NETWORK

NCSA

IODP

NNIN

NRAO

University-National Oceanographic Laboratory System

neon

NATIONAL ECOLOGICAL OBSERVATORY NETWORK

BLUE WATERS

SUSTAINED PETASCALE COMPUTING

incorporated research institutions for seismology

IRIS

What is at stake…

- Lost productivity
  - TeraGrid
    - Supports around $300M+ in research annually*
    - STAKKATO Incident ca. 2003-2004
  - McAfee DAT 5958
    - Worldwide impact April 2010
    - Not the first time this has happened

* Information provided by John Towns, NCSA

What is at stake…

- Expensive incident response and notification
  - Laptop stolen from public west-coast research university:
    - $750K out of pocket
  - Research server breach at private east-coast research university:
    - $200K out of pocket
  - External hard drive stolen containing student and alumni data from a locked office at research university:
    - $1M out of pocket

What is at stake…

- Expensive incident response and notification
  - Laptop Stolen from a Large Facility
    - Required notifying a military partner
  - McAfee 5958 at NSF
    - 1,800 PCs impacted; down 6-8 hours; lasted 2-3 days
  - Cost of TeraGrid's STAKKATO Incident in 2003-2004
    - Spanned 11 months
    - Not calculated

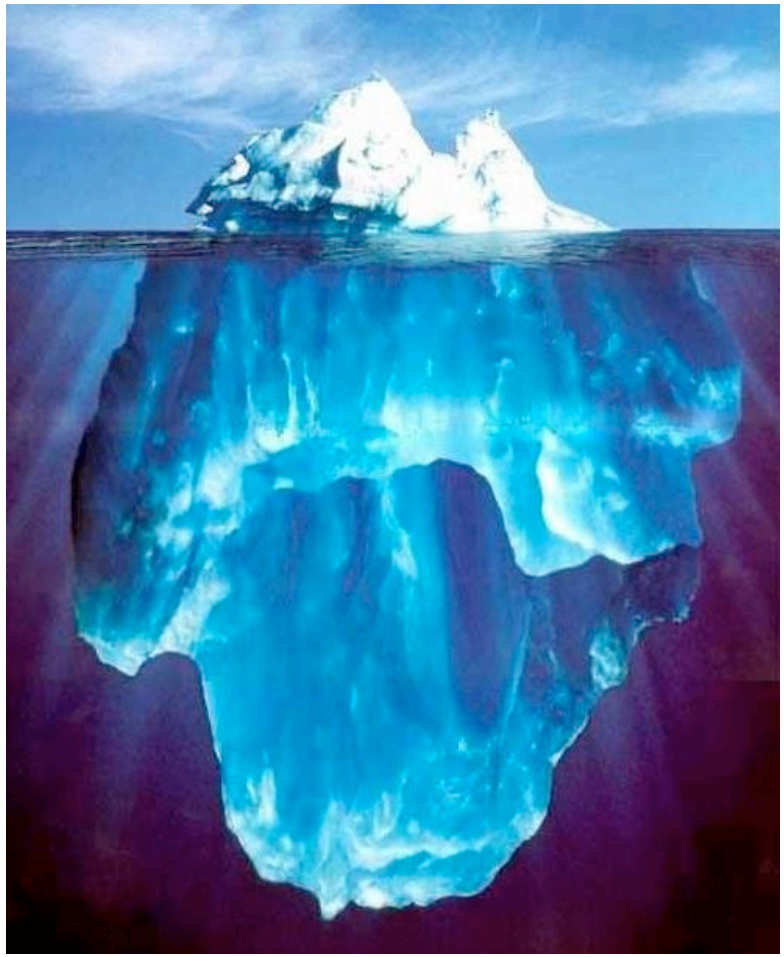
What is at stake…

- Reputational damage
  - Institution or agency: can't estimate
  - PII disclosure of patient or alumni data: priceless
- Data integrity compromise
  - Would you know if a data element was changed?

Facilities need an awareness of security breach implications that could impact the facility, NSF or the United States of America.

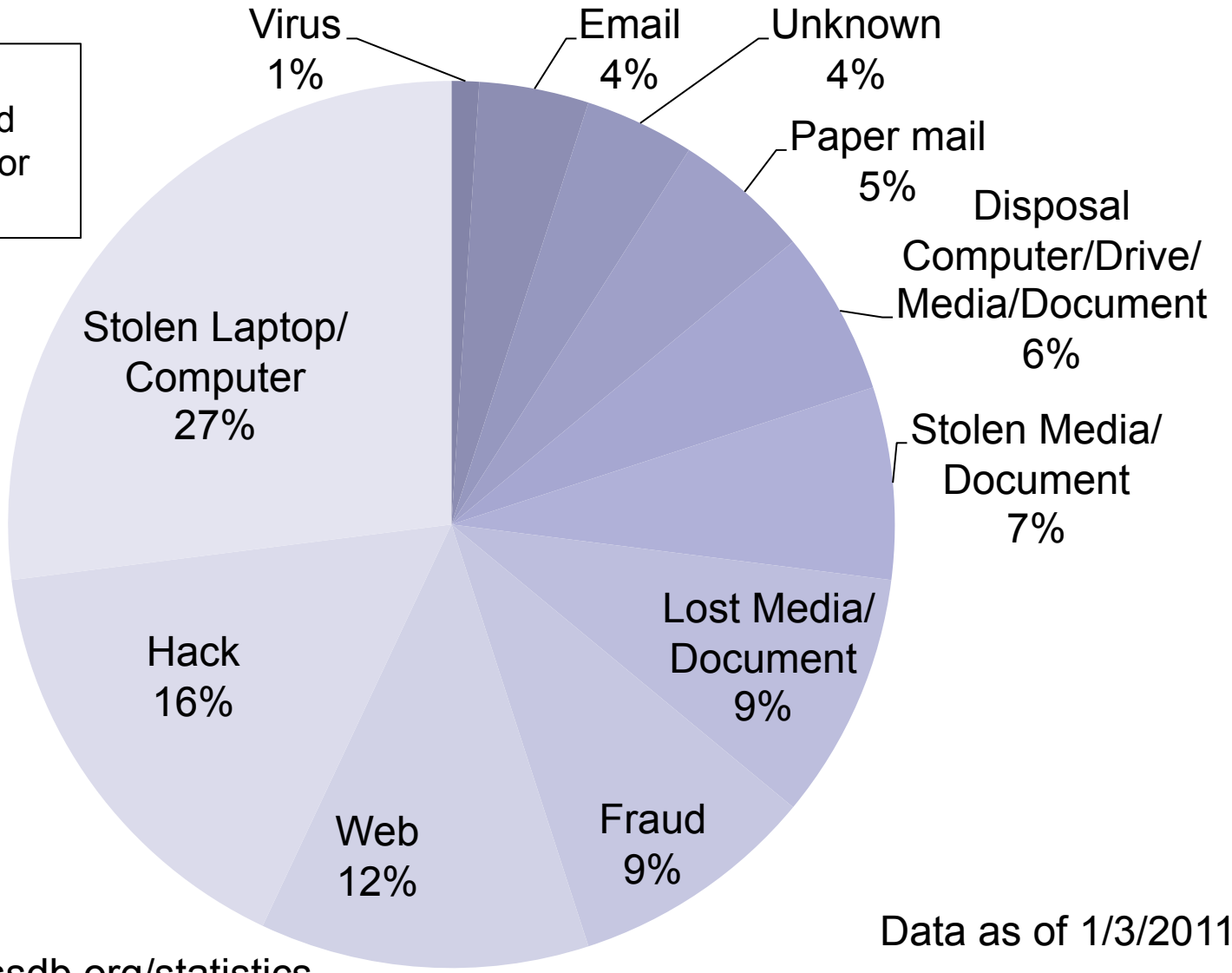
Some data on “Data Loss”

- Source: Open Security Foundation “dataloss db” (see: http://datalossdb.org/)
- Includes:
  - incidents reported in the press, news feeds, blogs, and other websites
  - Freedom of Information Requests from
    - Public Records/Open Records
    - Requests to various US States requesting breach notification documents they receive as a result of various state legislation.
    - NB: 46 states have breach notification laws



Data Loss Incidents by Type

Note: 49% of the incidents involved something “lost” or “stolen”.

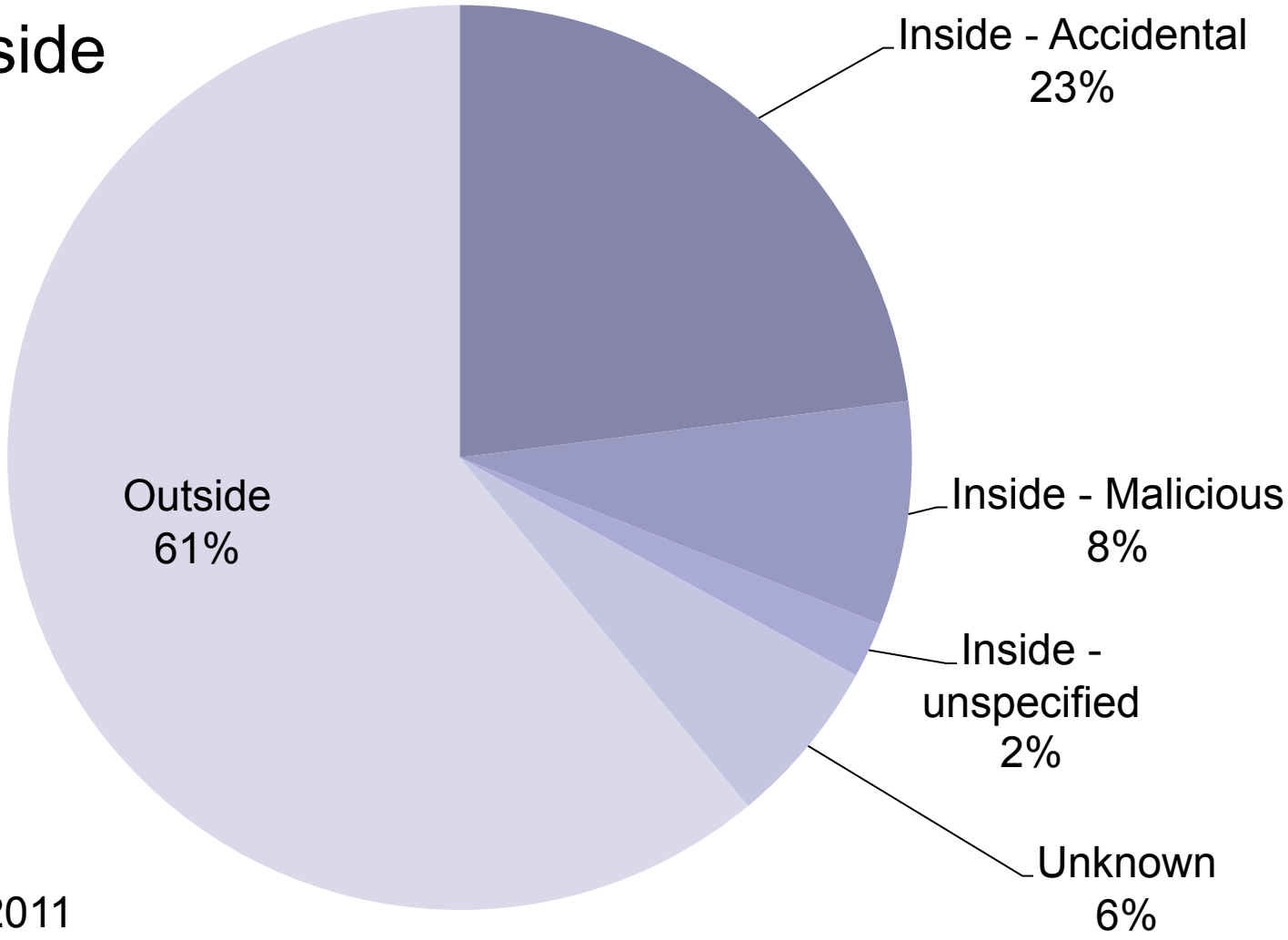


Data as of 1/3/2011

http://www.datalossdb.org/statistics

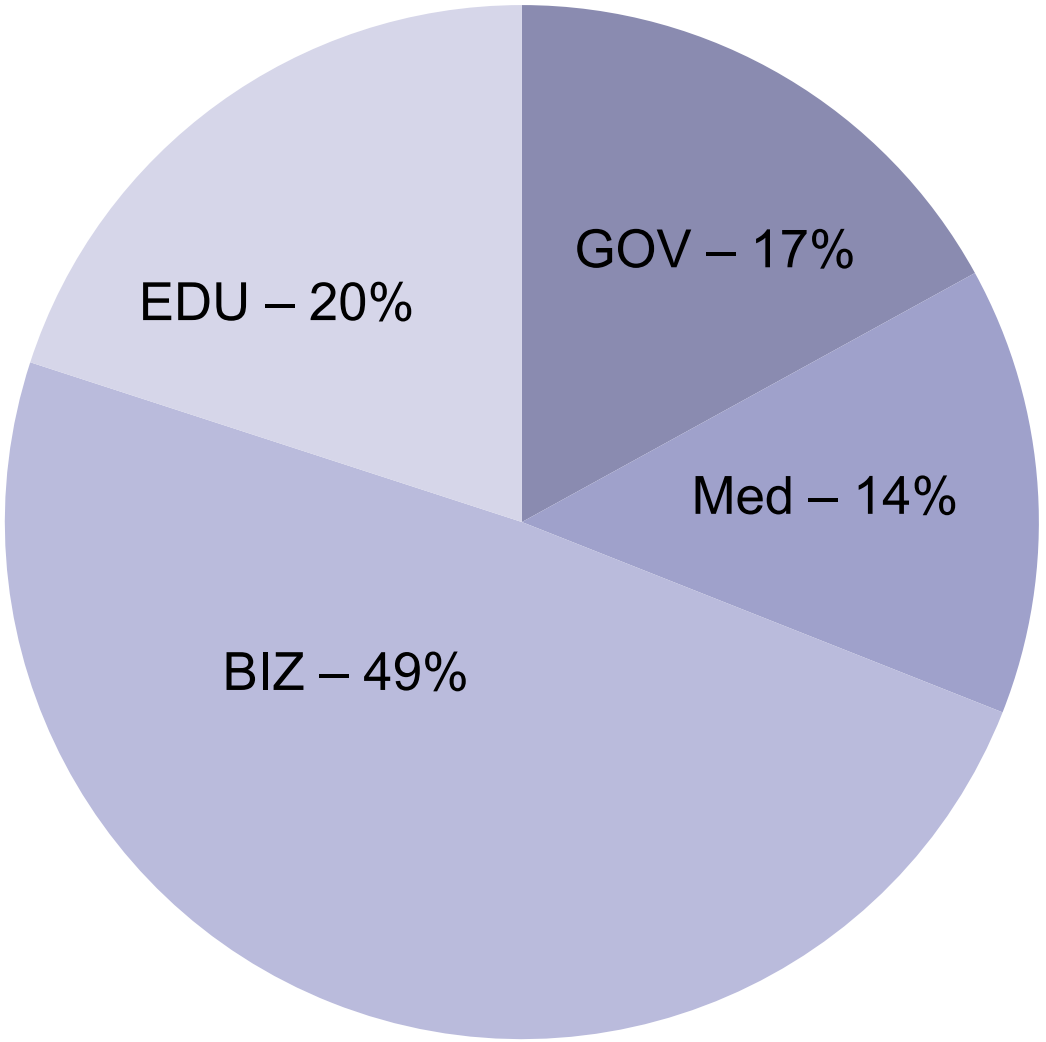
Data Loss Incidents by Vector

1/3 are Inside



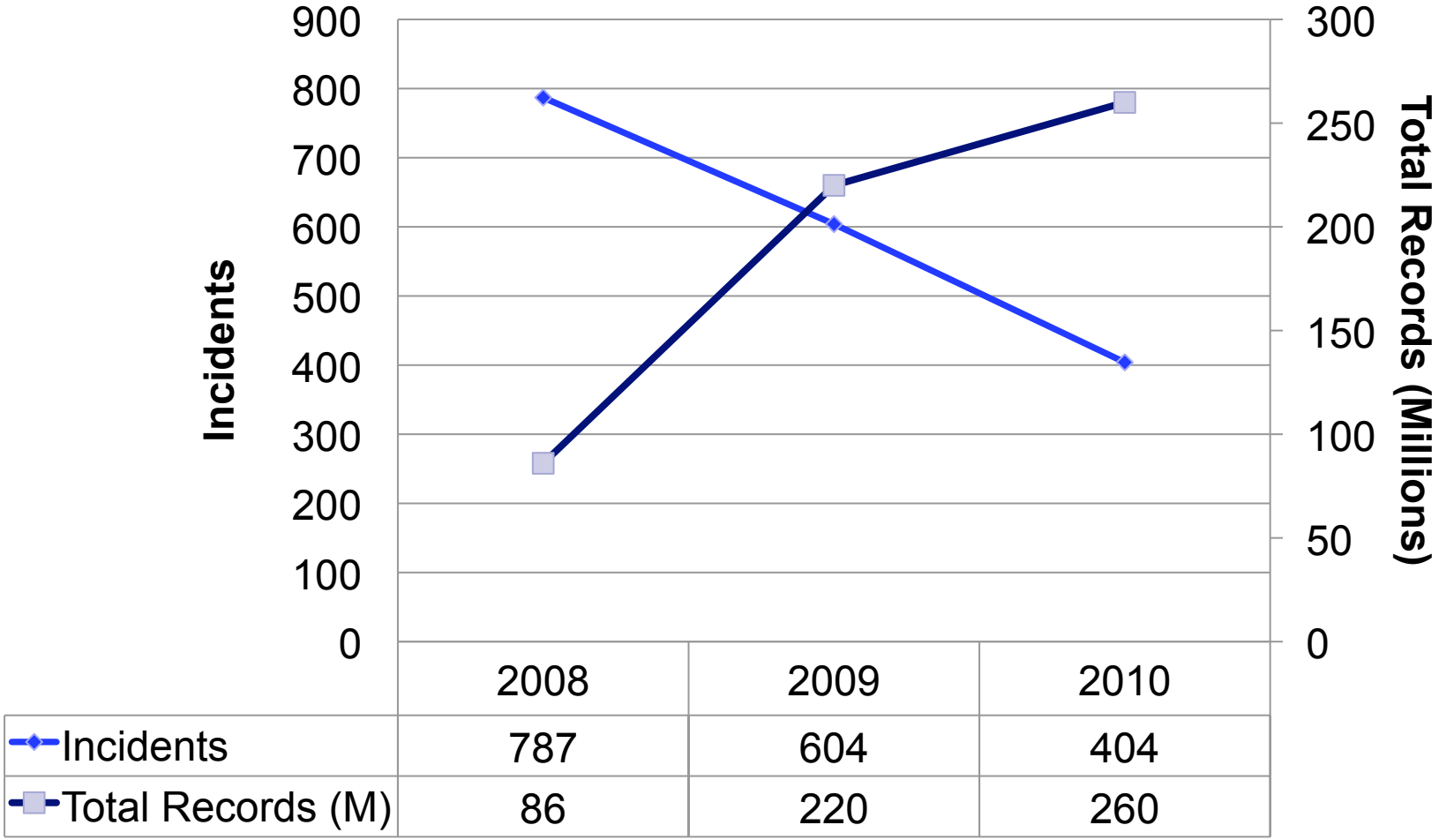
Data as of 1/3/2011

Data Loss by Business Type



http://www.datalossdb.org/statistics

REPORTED *Data* Loss



	2008	2009	2010
Incidents	787	604	404
Total Records (M)	86	220	260

Expanded Very Large Array

earth scope

NPACI

NCAR

LIGO

TeraGrid

NHMFL

NEES

Open Science Grid

GEMINI OBSERVATORY

WATERS NETWORK

NCSA

IODP

NNIN

NRAO

University-National Oceanographic Laboratory System

neon

NATIONAL ECOLOGICAL OBSERVATORY NETWORK

BLUE WATERS

SUSTAINED PETASCALE COMPUTING

incorporated research institutions for seismology

IRIS

First Principles

- Information security is a journey not a destination.
  - The challenges keep coming. Security programs evolve and improve.
- Security budgets are limited
  - Priorities must be established; tradeoffs must be made.
- Good IT practices foster good security
  - Good IT security reflects good IT practices.
- Information security is more than an “IT issue.”
  - It is an issue for everyone.
- Information Security starts with policy.

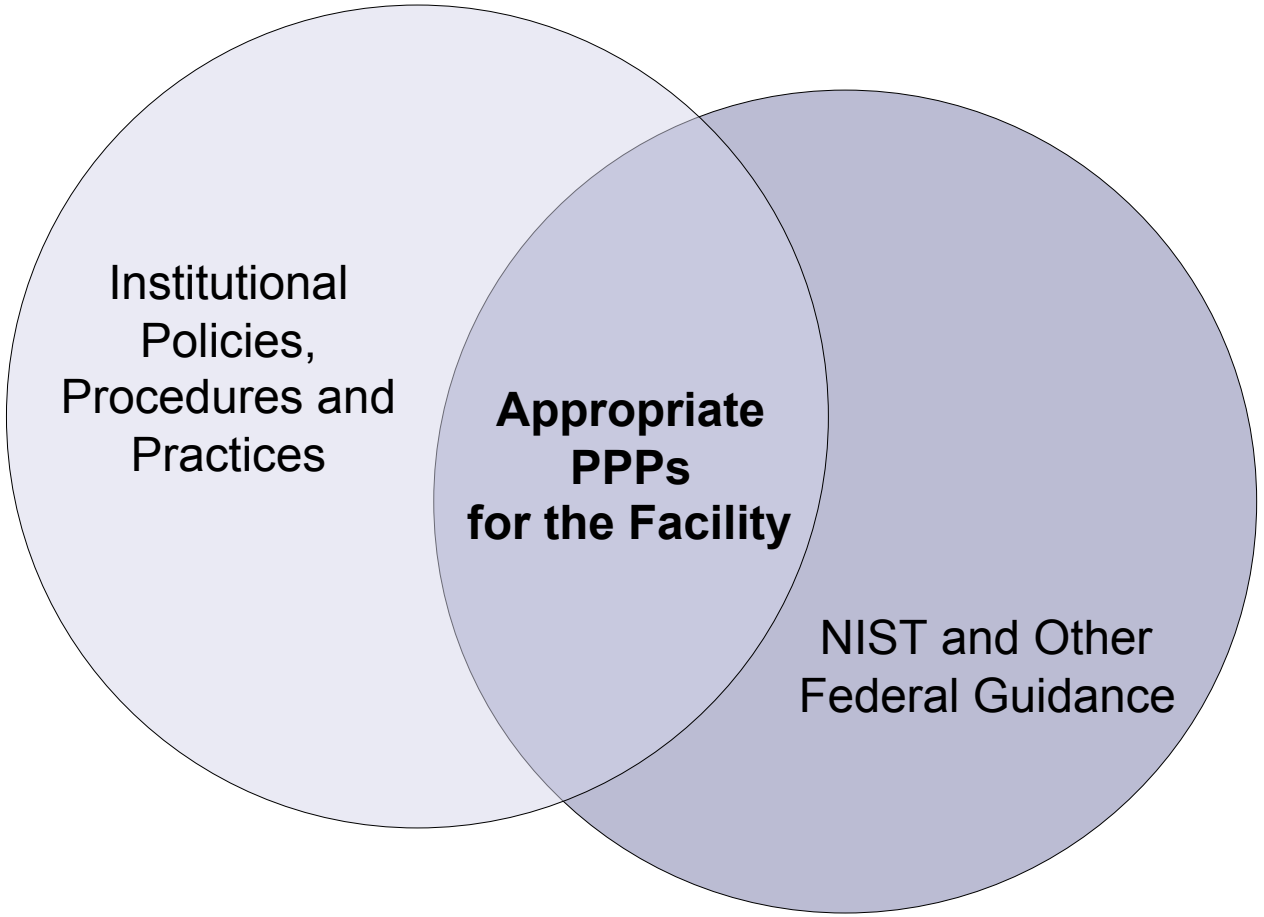
Starting with Policies

If the facility is:

- …part of a larger organization, the facility should defer to the policies of its parent organization. This could be a “floor” with the facility needing to augment the policies to address specific regulations, issues or needs. It might also be a “ceiling” with the facility needing to tailor policies to its needs.
- …a Consortium, the Consortium needs to have a policy that all of the members will have policies.
- …not part of a Consortium and doesn’t have a parent organization, it needs to develop its own policies.

Facility Cybersecurity:

Do What Makes Sense and is Appropriate for Identified Risks



Cybersecurity is a Balance

Open, Collaborative Environment for Research and Discovery

Confidentiality
Integrity Availability
Security
Privacy

Facilities must weigh the cost of impact vs the cost of remediation.

Sources for Reference

Links provided at end of presentation

- National Institutes of Standards and Technology
  - ***Guidance*** may be obtained from many documents
- EDUCAUSE/Internet2 Security and Network Task Force Wiki
  - Excellent outlines and examples
- Best practices from several Large Facilities and universities
- SANS (SysAdmin, Audit, Network, Security) Institute
- International Standards Organization
- Wikipedia
  - Excellent security and IT descriptions, especially for the non-IT professional
- And many more…

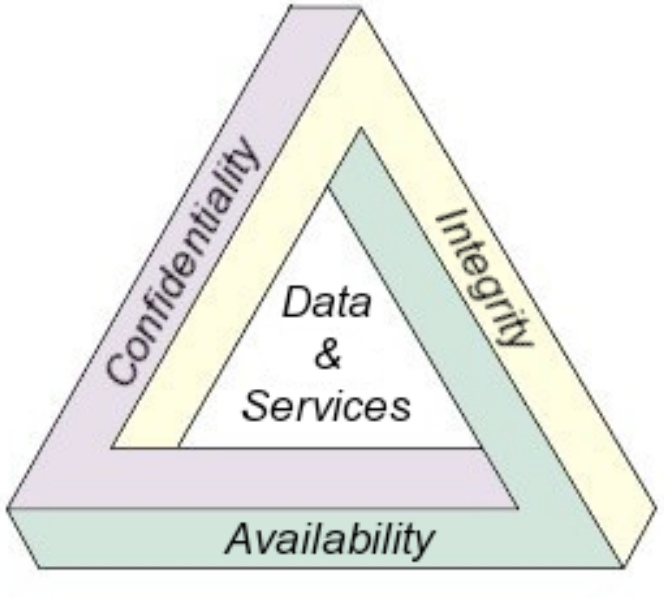
Background

Security Fundamentals

- Goal: Ensure access to services and information

- Three principles of a Security Program:
  - Confidentiality
  - Integrity
  - Availability

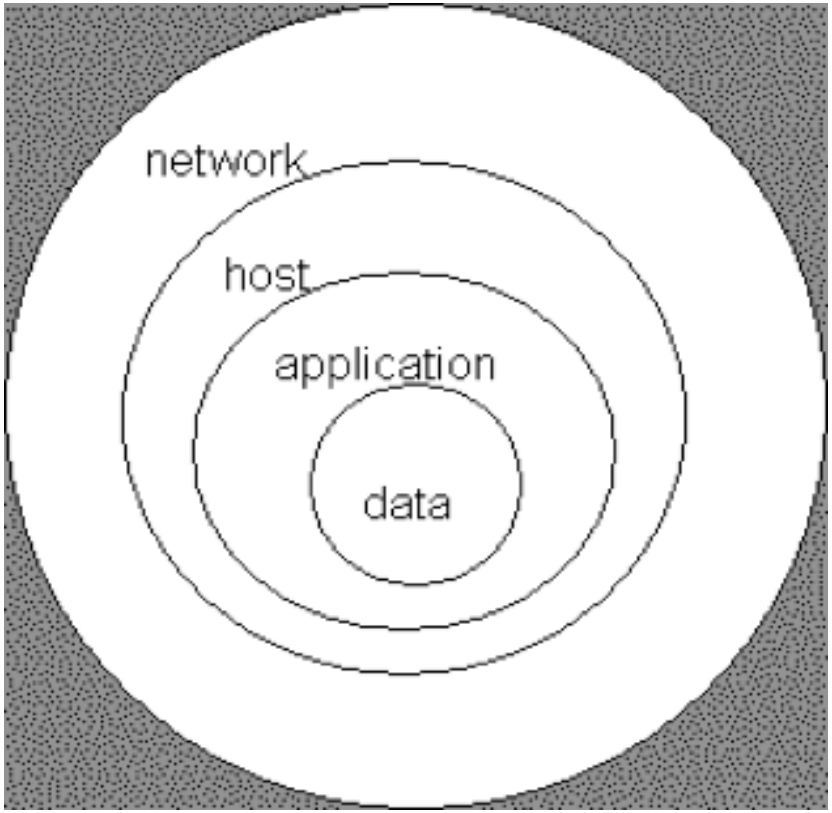
- Levels of security will vary as security goals and requirements differ from facility to facility



* Confidentiality, Integrity and Availability definitions taken from Wikipedia.
See: http://en.wikipedia.org/wiki/Information_security#Confidentiality.2C_integrity.2C_availability.
Site known good April 2010. Diagram is in the public domain.

Principle of Defense in Depth

- There are multiple safeguards in place so that if one fails, another will continue to provide protection.



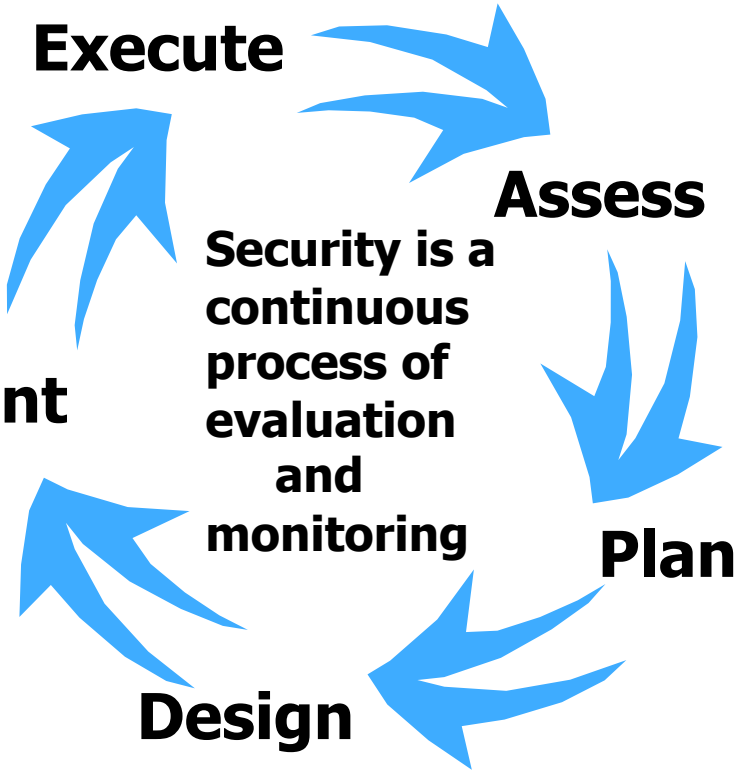
Simple DiD Model*

*Public domain document from http://en.wikipedia.org/wiki/Information_security. *Site known good April 2010.*

Security Fundamentals

- Security controls must be deployed commensurate with assessed risk.
  - They are a balance between regulations and common sense.
  - “Security Controls” are usually thought of as “administrative, technical (or logical) and physical”
- Security and Privacy must be considered together.
  - Security and Privacy
  - Privacy and Security

Information Security is a Continuous Process



- Managed Security Services
- Intrusion Detection
- Firewall Management
- Incident Reporting
- Vulnerability Management
- Penetration Testing

- Security Assessments
- Risk – Threats
- Privacy
- Security Test & Evaluation
- Compliance

- Risk-based Strategy
- Business Continuity
- Solution Planning
- Resource Allocation

- Policy
- Standards
- Enterprise Architecture
- Configuration Standards

- Product Selection
- Product Implementation
- Top-down Security
- Management

Security Fundamentals

- Goals
  - Prevent: an intrusion or incident
  - Defend: if prevention fails
  - Respond: if defense fails

NSF Cooperative Agreements Information Security Requirement

- Incorporated in NSF's Supplemental Financial/ Administrative Terms and Conditions for
  - Large Facilities - Article 52
  - Managers of Federally Funded Research and Development Centers (FFRDCs) – Article 55
  - See: Cooperative Agreement Conditions

- Purpose is to help ensure that NSF large facilities and FFRDCs have policies, procedures and practices to protect research and education activities in support of the award.

- Influenced by recommendations from awardees at previous NSF-sponsored Cybersecurity summits.

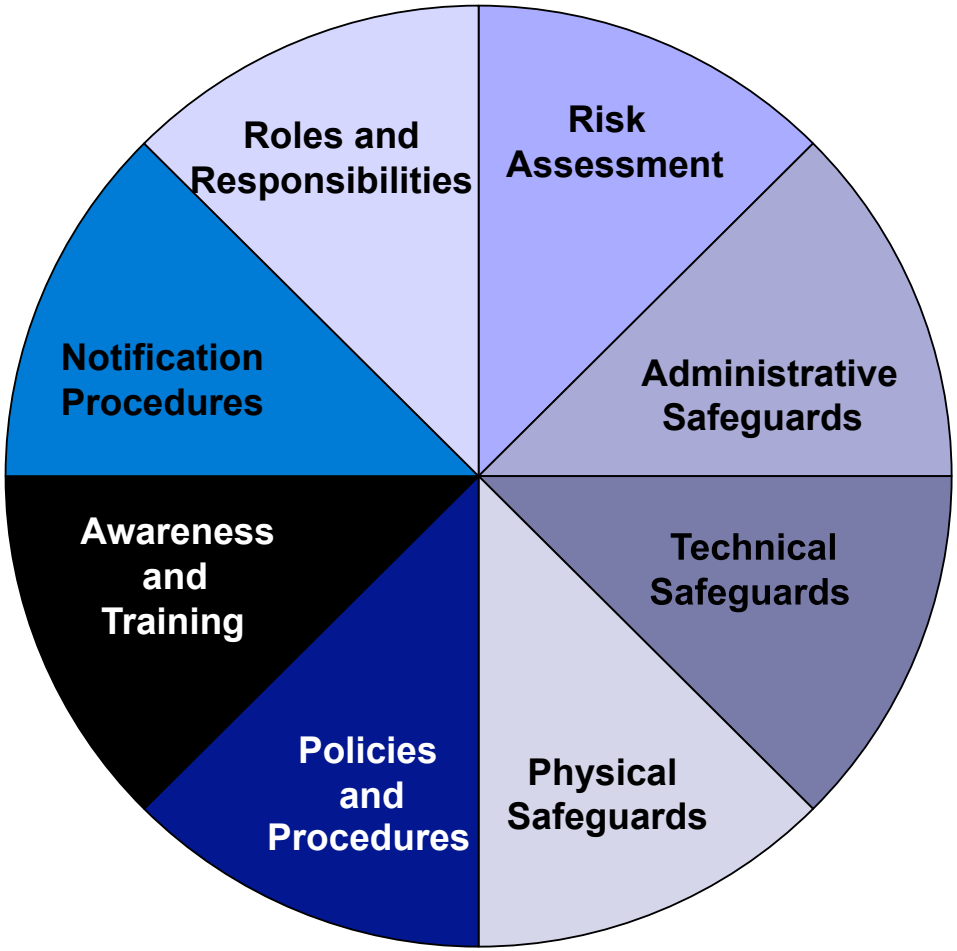
Information Security Responsibilities

- Security for all IT systems is the *Awardee's responsibility*.
  - Includes equipment, data and information
- Awardee is required to provide a summary of its IT Security program, including:
  - Roles and responsibilities, risk assessment, technical safeguards, administrative safeguards; physical safeguards; policies and procedures; awareness and training; notification procedures.
  - Evaluation criteria employed to assess the success of the program
- All subawardees, subcontractors, researchers and others with access to the awardee's systems and facilities shall have appropriate security measures in place.
- Awardee will participate in ongoing dialog with NSF and others to promote awareness and sharing of best practices.

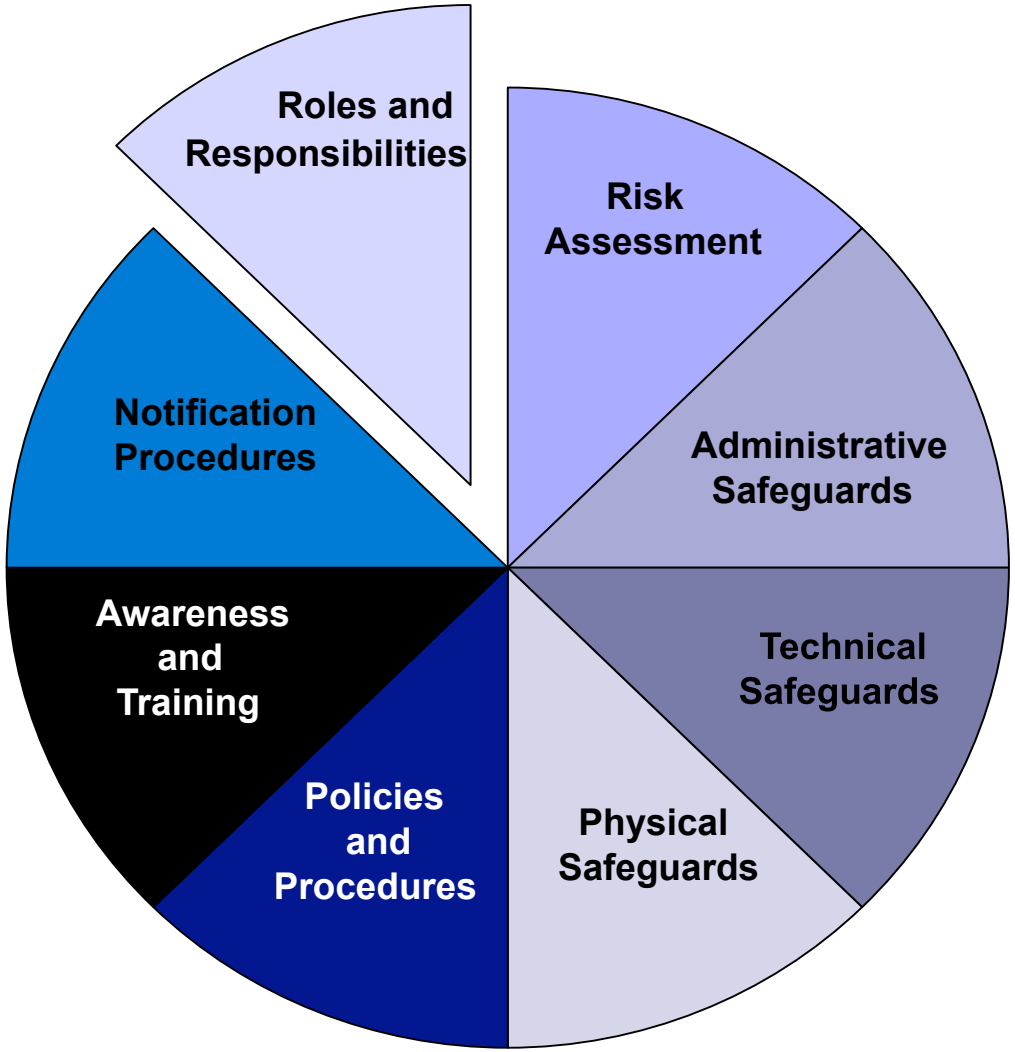
Cybersecurity Best Practices that Might be Useful for Large Facilities

Awardee Responsibilities under the Cooperative Agreement

Summary of IT Security Program
• roles and responsibilities • risk assessment • technical safeguards • administrative safeguards • physical safeguards • policies and procedures • awareness and training • notification procedures



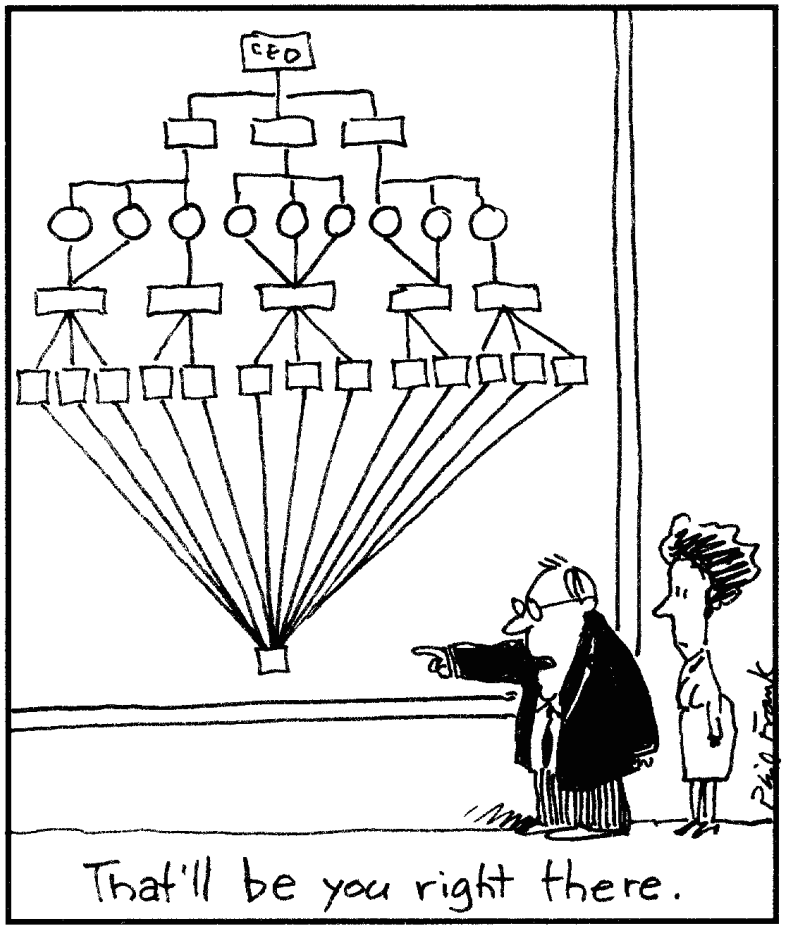
Roles and Responsibilities



Roles and Responsibilities

Principles

- One person cannot do it all
- *Everyone* in the facility has a responsibility for cybersecurity
- Cybersecurity is not just a technical or “computer geek” responsibility

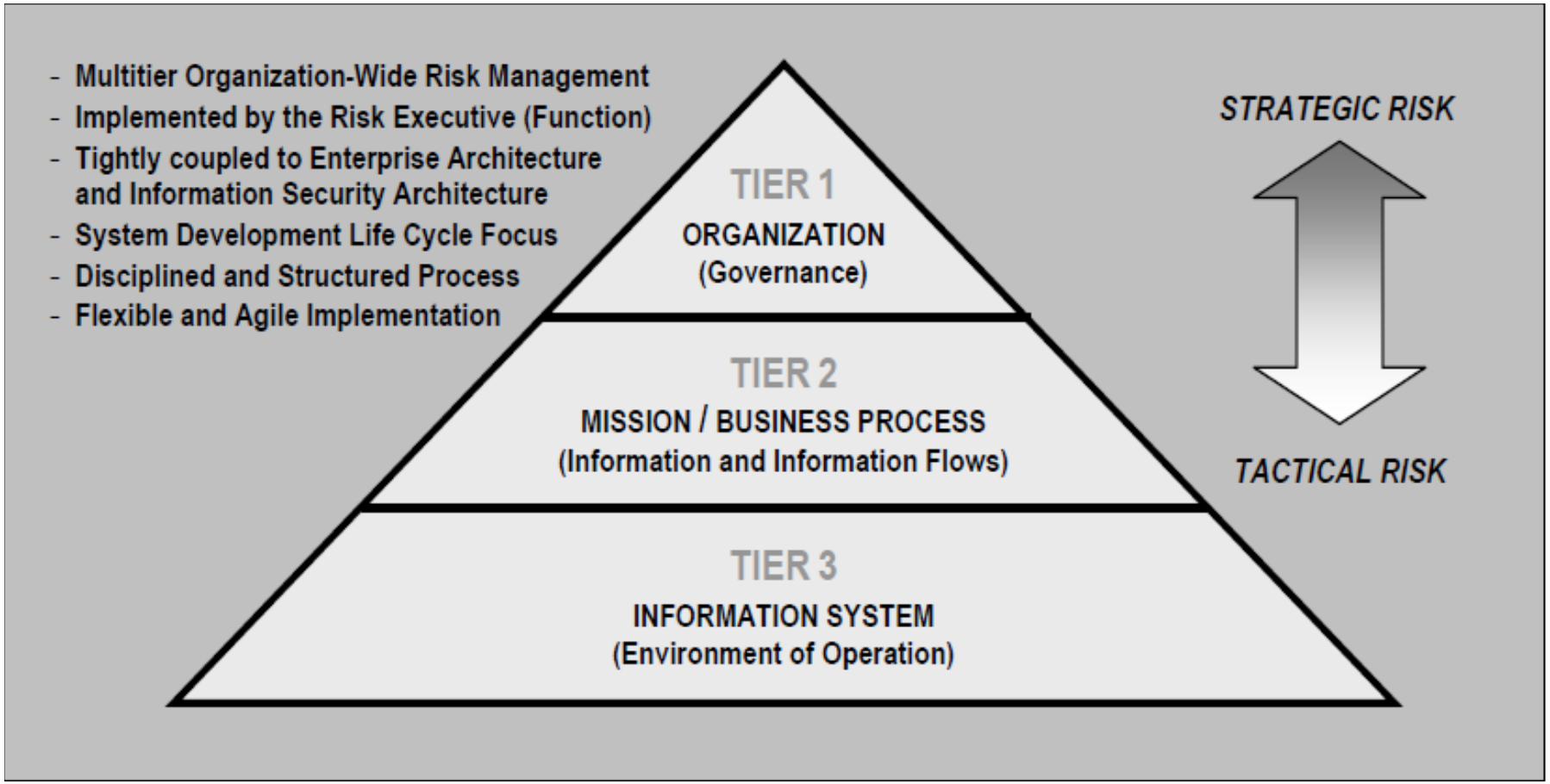


Roles and Responsibilities

Examples of identified roles include:

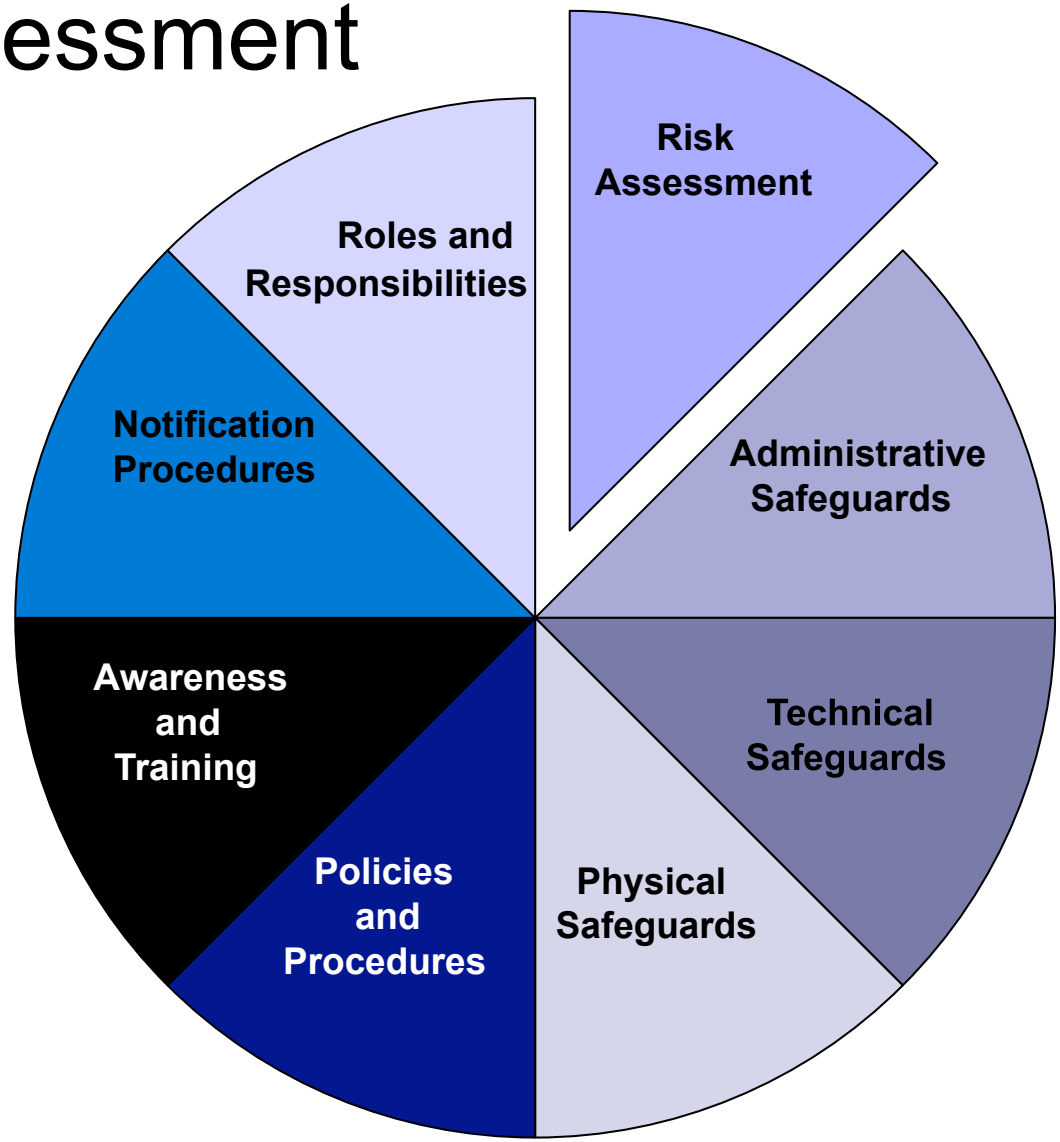
- Upper Management
- System and Network Administrators
- Information Security Support Staff
- Users
  - Internal
  - External

Integrated Organization-wide Risk Management



Ref: NIST 800-37 rev 1. Guide for Applying the Risk Management Framework to Federal Information Systems

Risk Assessment



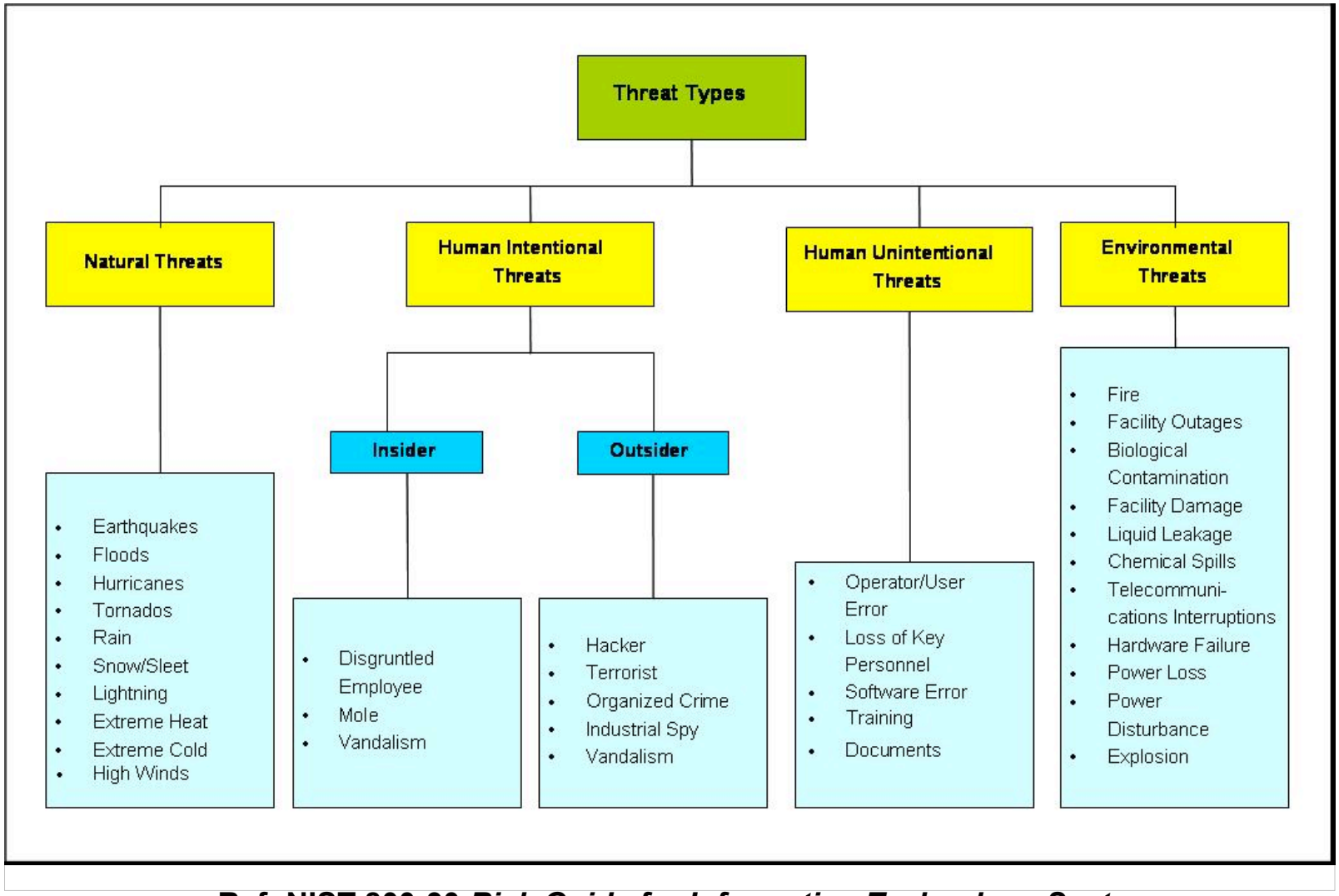
Risk Assessment:
IT Security Needs a Risk-Based Approach

Confidentiality
Integrity Availability
Security
Privacy

Open, Collaborative
Environment for
Research and
Discovery

Risk-Based Approach:
Risks are Assessed, Understood and
Appropriately Mitigated

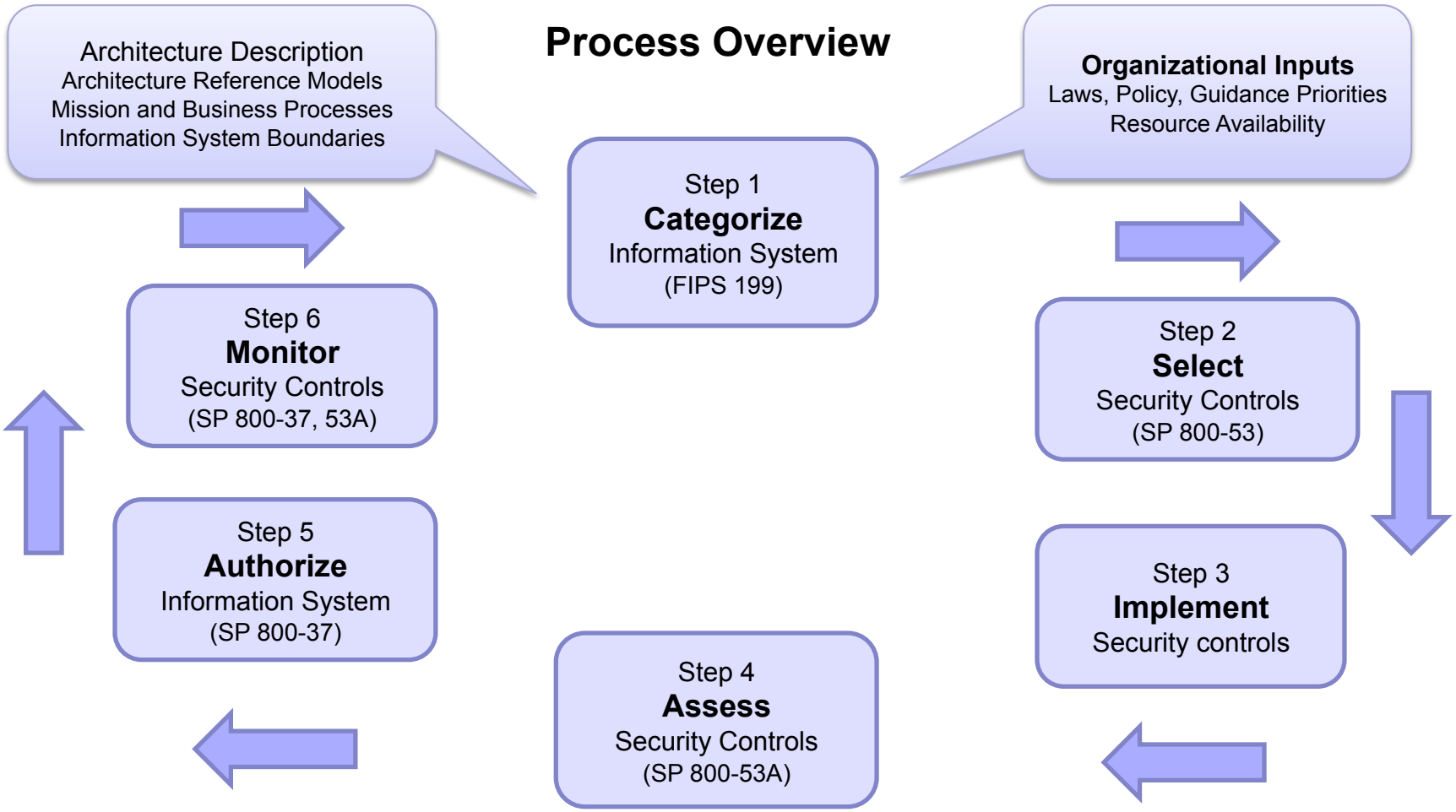
Examples of Threat Types



Ref: NIST 800-30 *Risk Guide for Information Technology Systems*

Risk Management Framework

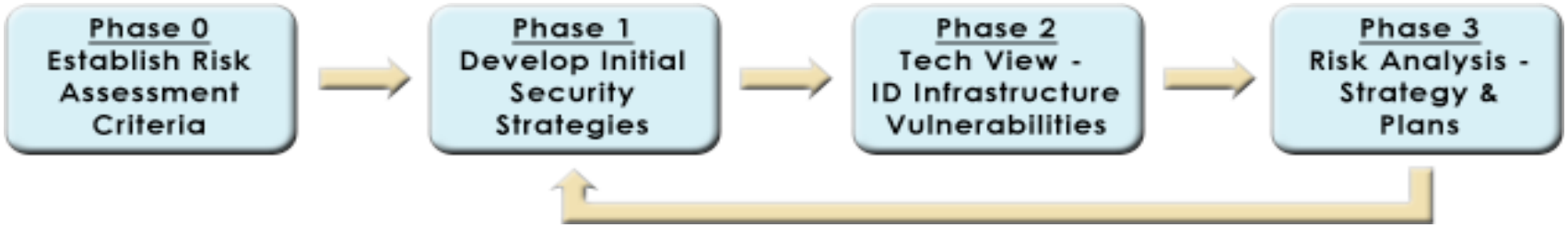
Federal Information Security Management Act (FISMA)



Ref: NIST 800-37 rev 1. Guide for Applying the Risk Management Framework to Federal Information Systems

A Model for ***Risk Assessment***:

EDUCAUSE/Internet2 Higher Education Security Council



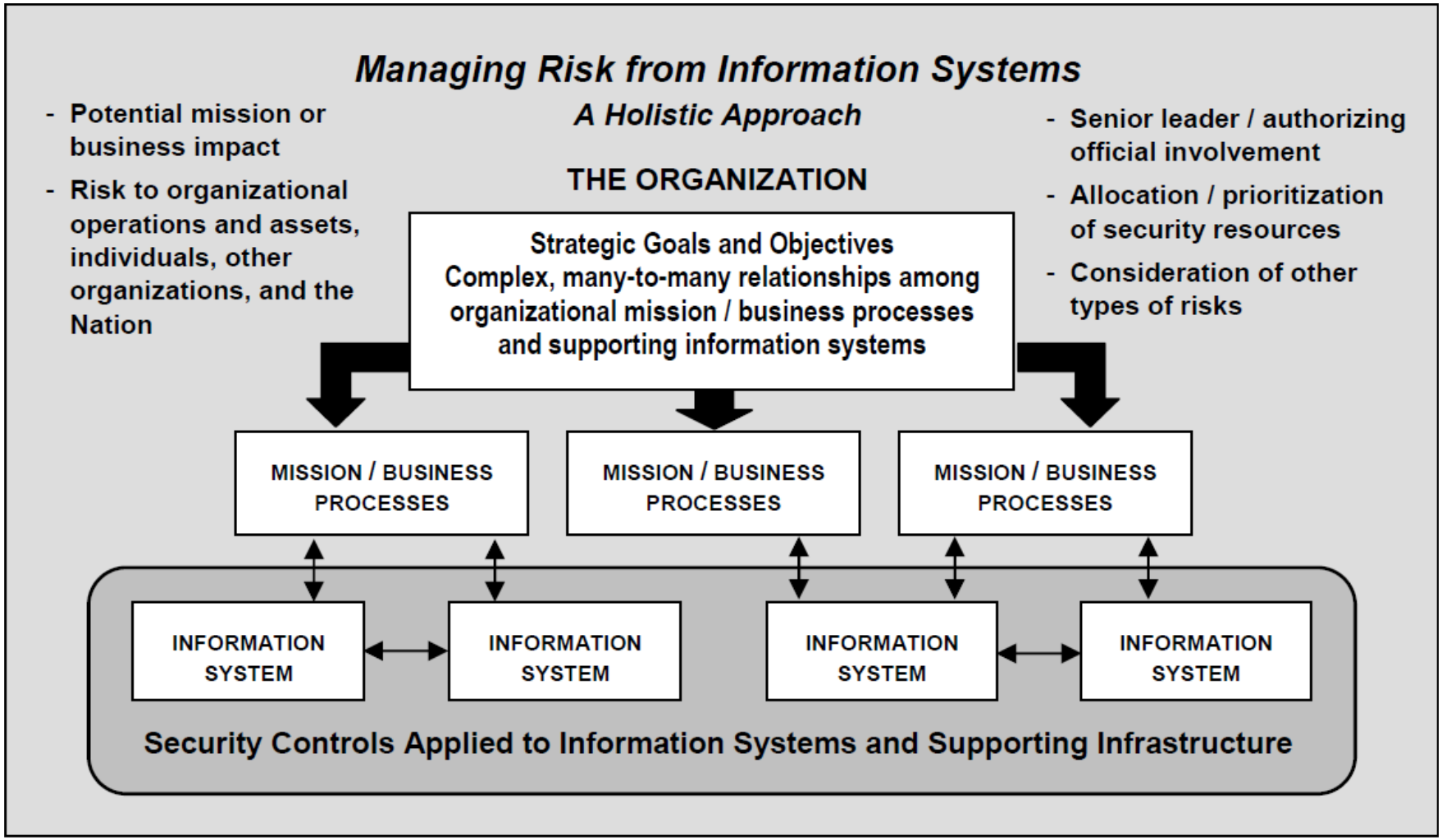
- Phase 0: Establish Risk Assessment Criteria for the Identification and Prioritization of Critical Assets - Asset Classification
- Phase 1: Develop Initial Security Strategies
- Phase 2: Technological View - Identify Infrastructure Vulnerabilities
- Phase 3: Risk Analysis - Develop Security Strategy and Plans

* Source: EDUCAUSE/Internet2 Higher Education Information Security Council: Risk Assessment Framework.
Site known good April 2010.

Risk Based Approach

- Fundamental Risk Management Philosophy
  - Risks are assessed, analyzed, understood and appropriately mitigated
    - Balance of operation and economic costs of protective measures with the commensurate gains in mission capability made through IT security controls
    - Requires a thorough understanding of overall environment
    - Risk analysis throughout systems development lifecycle, certification & accreditation process, vulnerability management, proactive reviews
  - Layered approach to overall security
    - Defense-in-depth with layers of security controls to assure most significant systems and assets are protected with the most extensive controls
    - Preventative, technical, operational, detection and recovery controls
  - Certification and accreditation is a risk management approach
    - Provides a continuous monitoring process
    - Provides management information to make cost-effective, risk-based decisions

Managing Risk from Information Systems

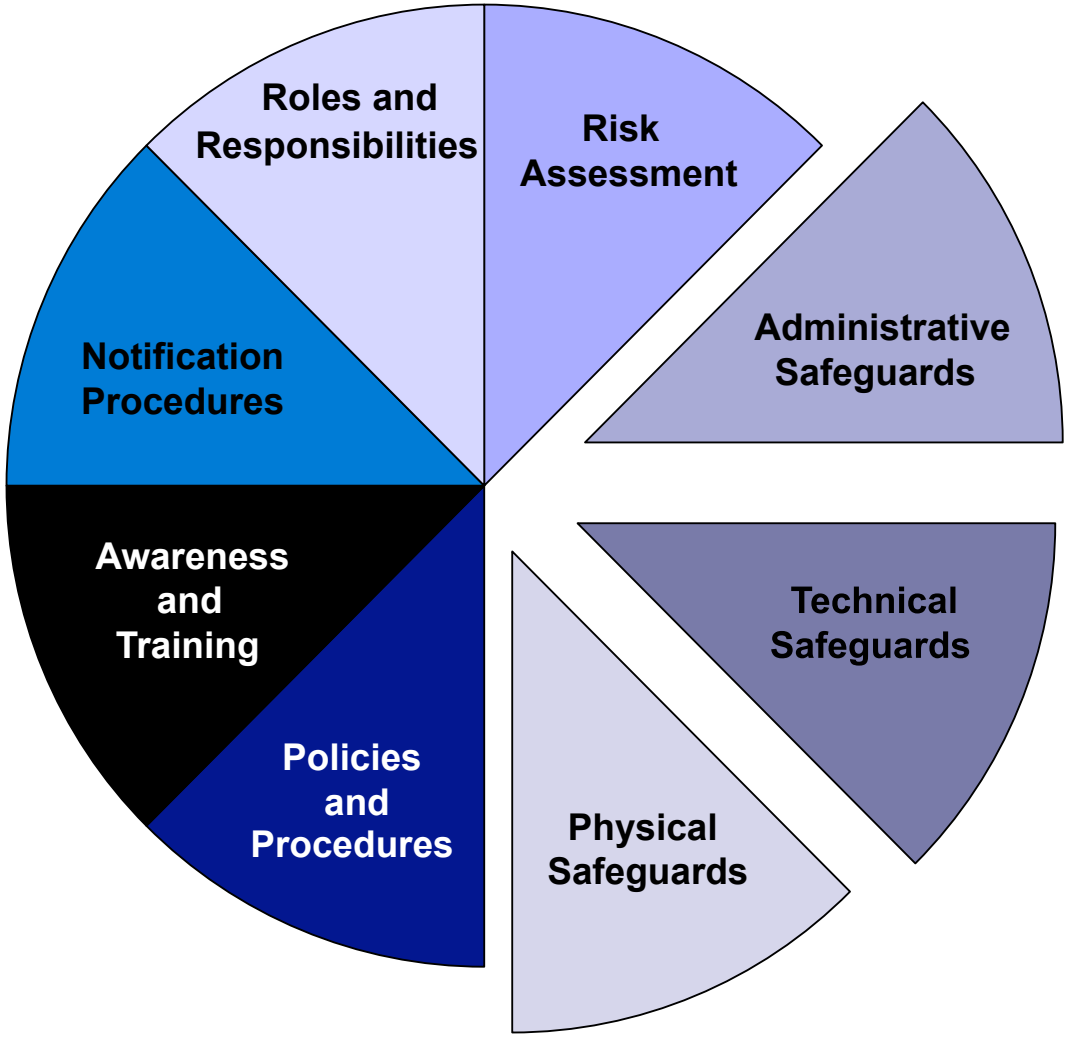


NIST 800 – 39 (draft)

NIST Security Controls

- The management, operational and technical safeguards and countermeasures which, taken together, adequately protect the confidentiality, integrity, and availability of the system and information
- Management Controls
  - Safeguards and countermeasures employed by an organization to manage the security of the information system and the associated risk to the organization's assets and operations
- Operational Controls
  - Safeguards and countermeasures employed by an organization to support the management and technical security controls in the information system (typically executed by people, not systems)
- Technical Controls
  - Safeguards and countermeasures (typically described as security mechanisms) employed within the information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction

Administrative, Technical and Physical Safeguards



Administrative, Technical and Physical Safeguards (Examples; not all inclusive)

- Controls are implemented to mitigate risk and reduce the potential for loss

	Prevention	Detection	Response
Administrative	Policy and requirements	Procedures Background checks	Procedures Supervision
Technical / Logical	Passwords Authorizations Encryption	Intrusion Detection Systems Tripwire "like" Log Analysis	Recovery from backups System re-imaged
Physical	Locks Barricades	Guards Video feeds	Physical Response

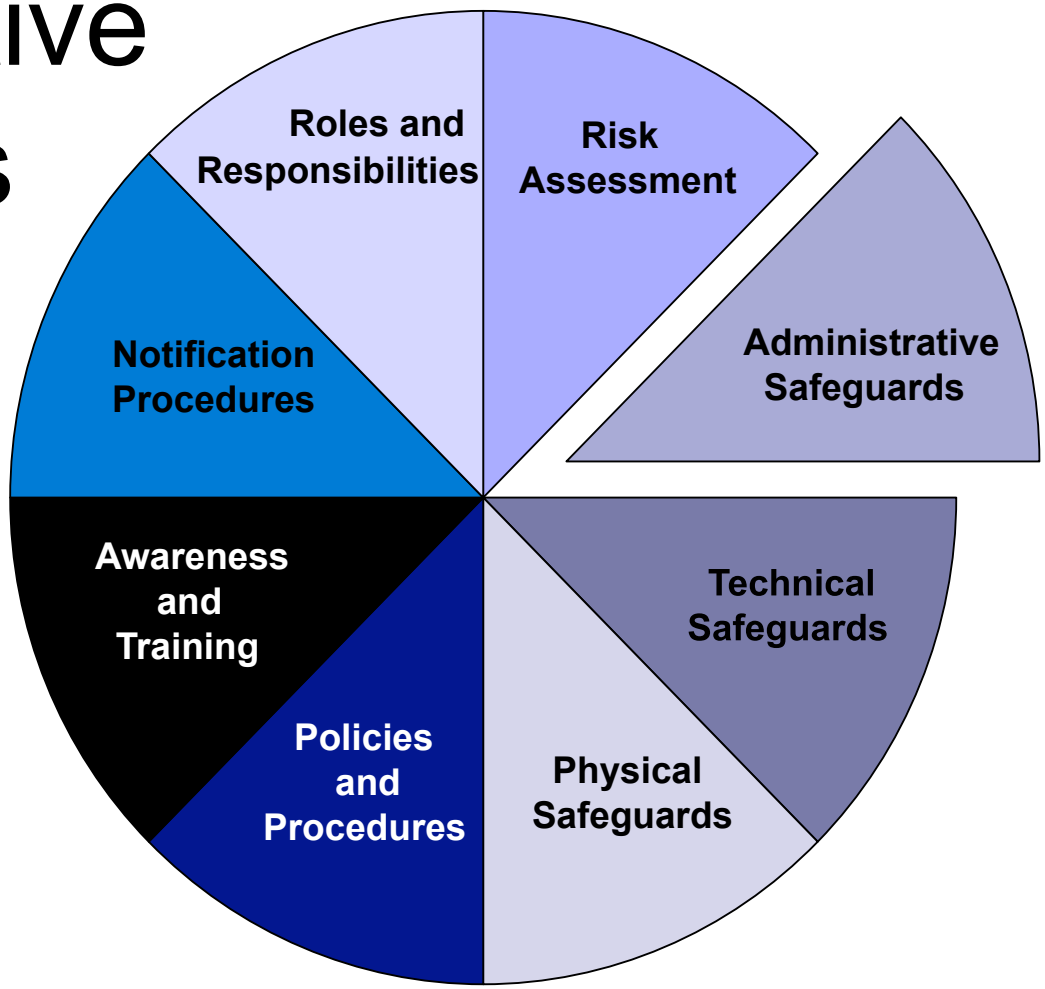
Adapted from a presentation by David C. Smith, UISO, Georgetown University 2010

Administrative, Technical and Physical Safeguards: Important Concepts

- Concept of least privilege: an individual, program or system process should not be granted any more privileges than are necessary to perform the task

- Concept of separation of duties: one individual can not complete a critical task by herself

Administrative Safeguards



Administrative Safeguards

Examples

- Compliance and Legal Issues
- ***Policies and Procedures***
- ***Awareness and Training***
- ***Risk Assessment and Management*** *(previous section)*
- Continuity of operations (discussed later)

Compliance and Legal Issues

Know and understand the federal and state laws under which the facility (and institution) must operate. For example:

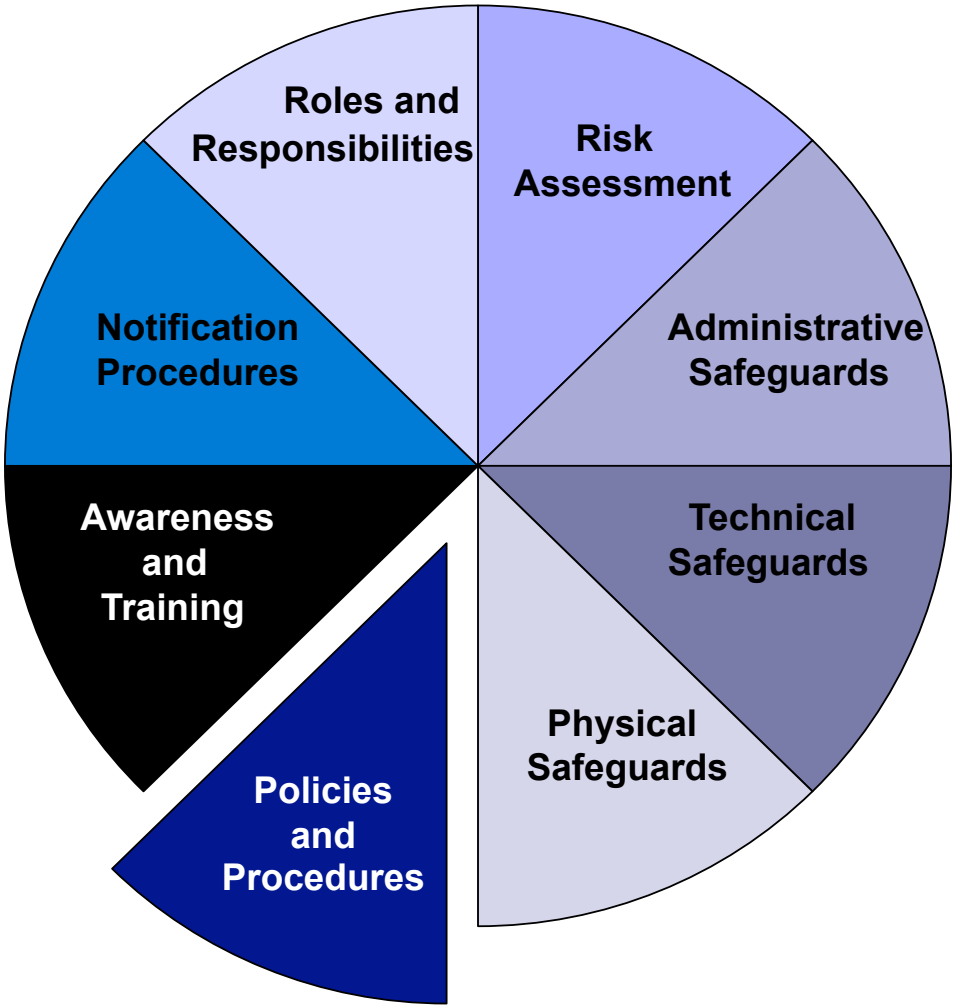
- Regulatory Compliance
  - Environmental Health and Safety
  - DOE/DOD
- Export Control regulations
  - US Department of Commerce, State Department and Treasury
- HIPAA (Health Insurance Portability and Accountability Act)
  - Health
- FERPA (Family Educational Rights and Privacy Act)
  - Student information
- GLBA (Gramm-Leach-Bliley Act)
  - Privacy and security of financial information
- Sarbanes-Oxley Act of 2002 (SOX).
  - Financial controls: could be extended to non-profits
- Privacy Laws/State Breach Notification Laws
  - If you don't need personally-identifiable information, don't ask for it, don't keep it.

Compliance and Legal Issues

Know and understand the federal and state laws under which the facility (and institution) must operate. For example:

- ***Regulatory Compliance***
  - ***Environmental Health and Safety***
  - ***DOE/DOD***
- ***Export Control regulations***
  - ***US Department of Commerce, State Department and Treasury***
- HIPAA (Health Insurance Portability and Accountability Act)
  - Health
- FERPA (Family Educational Rights and Privacy Act)
  - Student information
- GLBA (Gramm-Leach-Bliley Act)
  - Privacy and security of financial information
- Sarbanes-Oxley Act of 2002 (SOX).
  - Financial controls: could be extended to non-profits
- ***Privacy Laws/State Breach Notification Laws***
  - ***If you don't need personally-identifiable information, don't ask for it, don't keep it.***

Administrative Safeguards: Policies and Procedures



Examples of Policies

- Security Policies and Procedures*
  - 1.0 Security Policy (This section is policy about security policy)
  - 2.0 Organizational Security
  - 3.0 Asset Classification
  - 4.0 Personnel Security
  - 5.0 Physical and Environmental Security
  - 6.0 Communications and Operations Management
  - 7.0 Access Control
  - 8.0 System Development and Maintenance
  - 9.0 Business Continuity Management
  - 10.0 Compliance
  - 11.0 Incident Management
  - 12.0 Security Plans

*Source: Outline taken from EDUCAUSE/Internet2 Information Security Guide.
Site known good April 2010.

More Example Policies

- Responsible/Acceptable Use Policy (AUPs)
  - Typically define what uses are permitted and what are not. (e.g., no personal commercial gain, no illegal behavior, follow export control mandates, etc.)
- "Agreement of Use" or "Rules of Behavior."

  Facilities need to make sure that:
  - Only authorized users are using resources and know how they are using them
  - Users are accountable for the actions of others they may designate as users
  - Users are aware of consequences of misuse

Facilities need an awareness of security breach implications that could impact the facility, NSF or the United States of America.

* Examples may be found on the SDSC and TeraGrid web sites.

More Example Policies

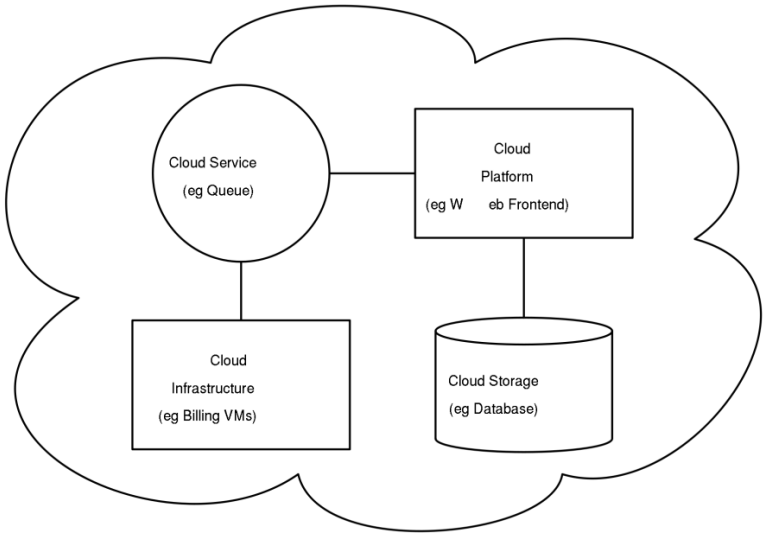
- Laptop and Portable Device Encryption Policy
  - Describe what can be stored on a laptop, thumb drive or other device
  - Protect against loss of scientific information
  - Protect administrative information, especially PII (personally-identifiable information)
  - Don’t store it if you don’t need it

Remember: this is facility information, not agency information.

* NB: DOD Bans Use of Thumb Drives, November 2008

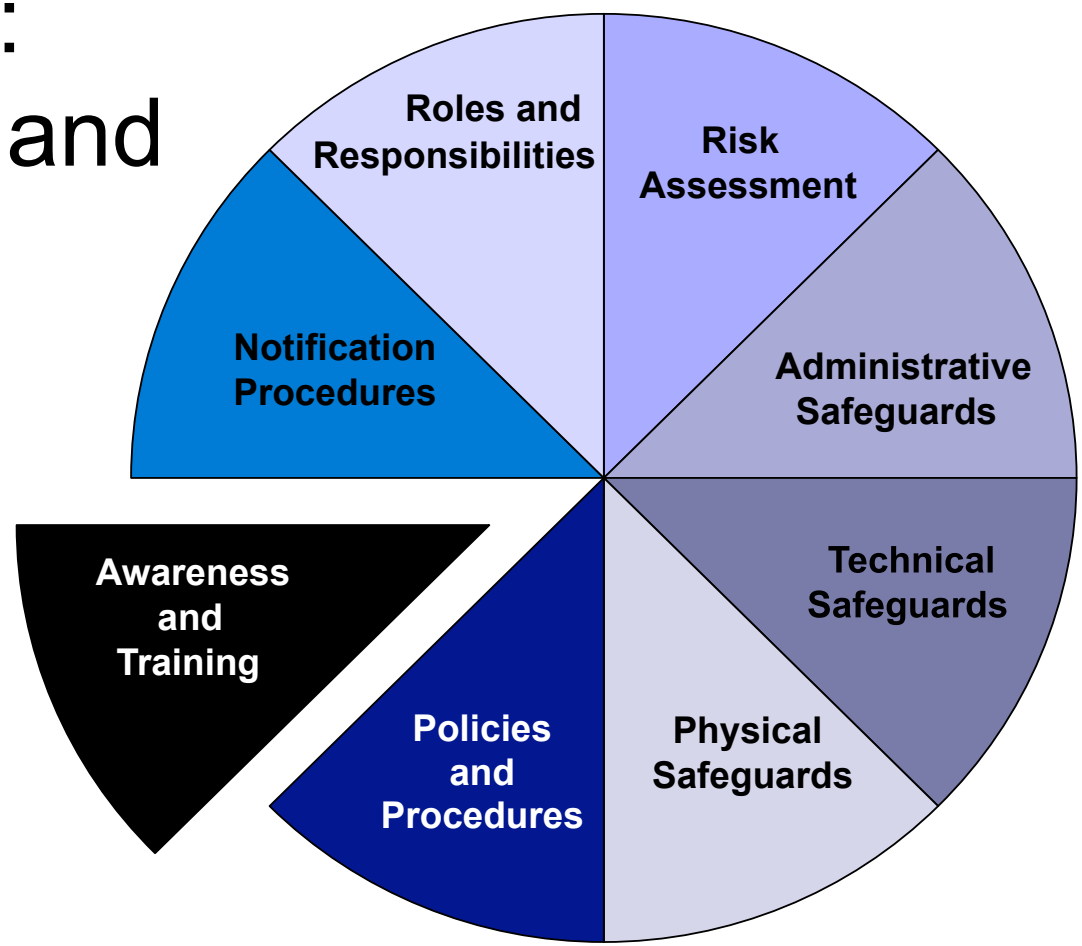
More Example Policies

- Cloud Computing
  - How do you:
    - Decide which kinds of data to store in the cloud
    - Stay compliant with government regulations
    - Maintain control and protect your data



- Where in the world is your data stored?
- How and where is it backed up?
- What happens to your data if the “cloud company” goes out of business?

Administrative Safeguards: Awareness and Training



Examples: Security Awareness Training How It Needs to Focus on Many Levels

- Upper Management: needs to learn about the facility and institutional risks
- Users: must be taught how to protect their own information, systems and portable media
- Information or System “Stewards”: the PIs, researchers, managers or others are responsible for the “data”, “content” or the “process” or even the “science” but not necessarily the technology that undergirds it

Examples: Security Awareness Training How It Needs to Focus on Many Levels

- System and Network Administrators: require training to help them maintain and improve the security of the systems they oversee
- Information Security Support Staff: all of the above as well as having a solid understanding of
  - Vulnerability assessment
  - Intrusion detection, incident response
  - Encryption
  - Authentication
- All IT professionals have a professional responsibility to keep *themselves* current on cybersecurity

Security Awareness Training (SAT) Resources

- SAT Training Materials
  - Facilities should be able to utilize materials that already exist within the community
  - The community could tailor training materials to the large facilities

A Google search in the .edu domain brought up 142,000+ hits on security training!

Security Awareness: How to Leverage Access Points that Exist at Many Levels*

- The CEO/President's Chief of Staff.
  - S/he sets the Board agenda and Cabinet agenda
- The Distributed Systems Administrators
  - If they support what you are doing, they will let their leaders know – and vice versa
- The technology thought leaders in Departments or project leaders in Research Units.
  - The department heads (or deans) listen to them.
- The auditors.
  - They report to the Board.
- The Budget Group.
  - Duh! they have the money.

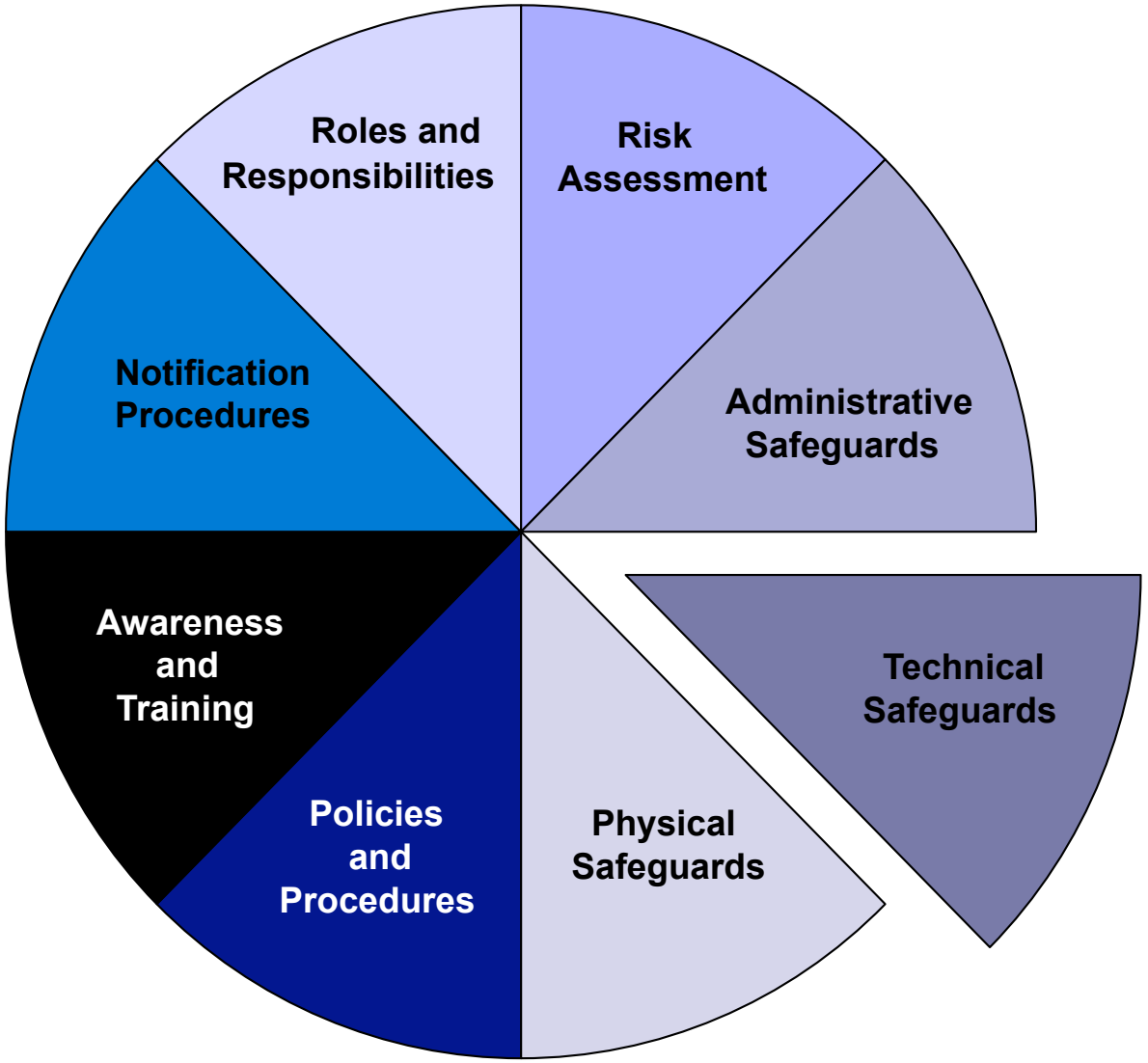
* Adapted from a presentation by Joy Hughes and Jack Seuss, EDUCAUSE 2005

Examples: Security Awareness and How to Leverage Interest and Access*

- CEO/President
  - His/her concern is maintaining good relationships with NSF, parent institution, legislative audits (if applicable)
- Provost
  - Her/his concern is academic integrity
- Head/VP of Research
  - Data integrity
  - Availability and access of information
  - Regulatory compliance
- Engage Central IT staff
  - A broad understanding of cybersecurity
- Engage Departmental IT Staff
  - A facility-specific understanding of cybersecurity

* Adapted from a presentation by Joy Hughes and Jack Seuss, EDUCAUSE 2005

Technical Safeguards



Technical Safeguards
Examples

- Access Management and Oversight
- Security Architecture
- Telecommunications and Network Security
- Applications and Systems Development
- Business Continuity (discussed later)

Technical Safeguards
Identity and Access Management and Oversight

- Facilities need to establish solutions to:
  - **Identify** a person, program or computer
  - **Authenticate** or verify that the person, program or computer is who she/he/it claims to be
  - **Authorize** what resources they are permitted to access and what actions they will be allowed to perform

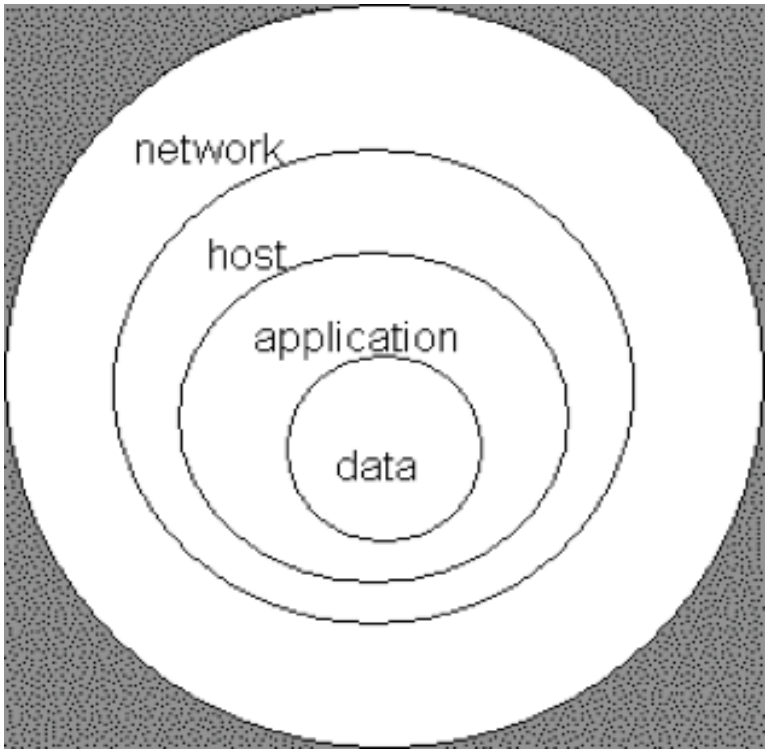
What is identity management?*

- Organization: The policies, processes, and tools used to “assure” that IT systems and applications are made available only to appropriate persons
- Individual: The persons I am working with and the systems I am using really are who/what they say they are. And no one can impersonate me, or read or change my information
- Identity Management has greatly increased in importance as IT systems and applications are used to perform more and more of the work of society and commerce

Discussion of “Federated Identity” at end with Supplemental Materials

Technical Safeguards
Security Architecture & Telecom and Network Security

- **Principle of Defense in Depth:** There are multiple safeguards in place so that if one fails, another will continue to provide protection.



Simple DiD Model*

*Public domain document from http://en.wikipedia.org/wiki/Information_security.
Site known good April 2010.

Overview of NCSA Security

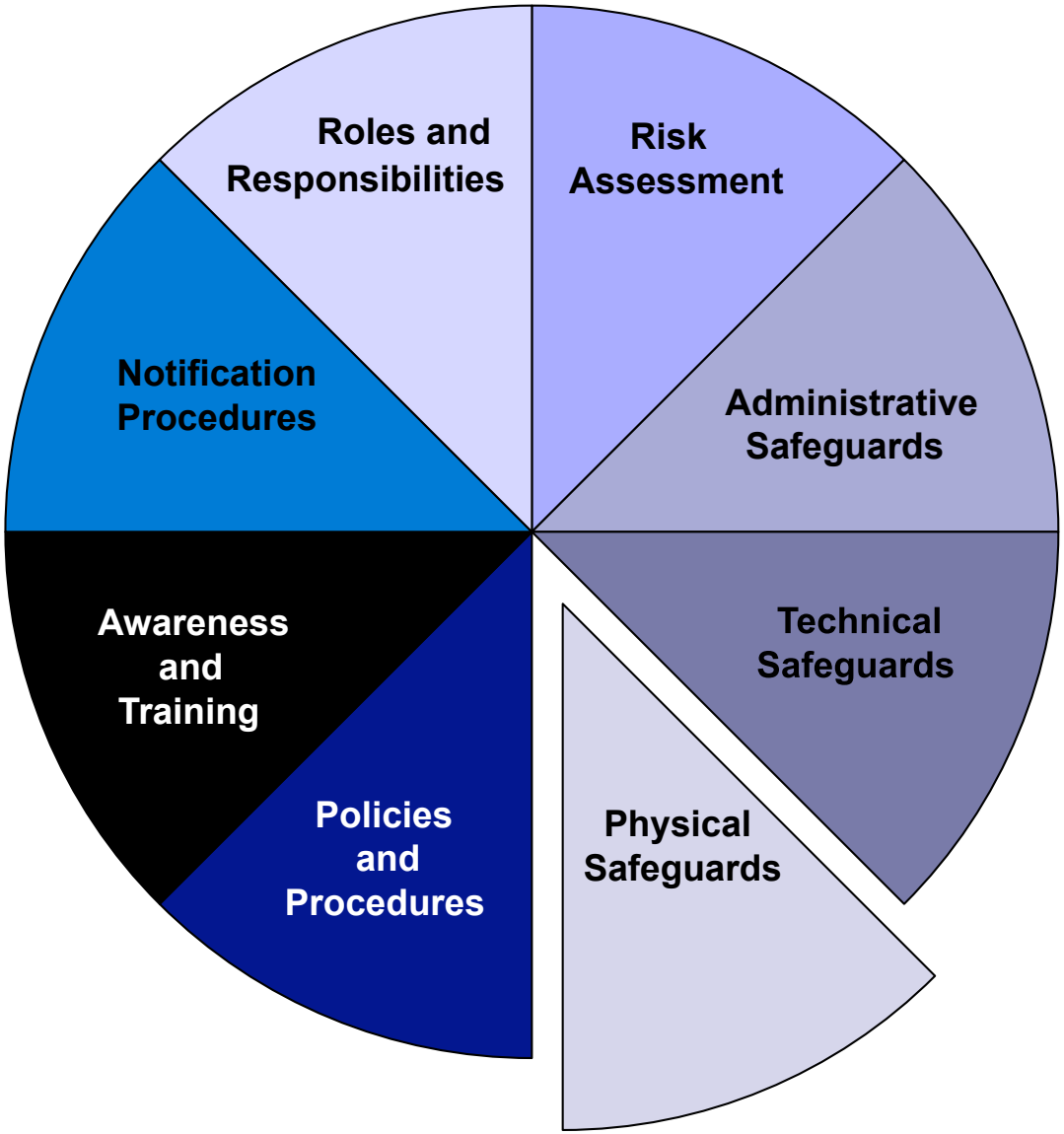
- **Prevention:**
  - no cleartext passwords (SSH and Kerberos)
  - one-time passwords for critical assets
  - active scanning for vulnerabilities
  - email virus and Trojan cleaning
  - firewall prevents access to vulnerable services from outside
- **24-hour on-call Security Officer**
- **Detection:**
  - host- and network-based IDS's (Tripewire, Bro)
  - network flow monitoring (Argus, Cisco)
  - central syslog server
  - honeypot and "DarkNet" monitoring
- **Response**
  - incident response team with strong forensics expertise
    - often consulted with by FBI and other law enforcement
  - firewall dynamically used to contain or keep out compromised hosts

National Center for Supercomputing Applications

NCSA

* Slide provided by John Towns, NSCA

Physical Safeguards



Physical Safeguards: Facilities Vary

ALMA
ATACAMA LARGE MILLIMETER ARRAY

Elements of Physical Safeguards Examples

- Administrative, Physical and Technical Controls
- Facility location, construction and management
- Physical security risks, threats and countermeasures
- Electric power issues and countermeasures
- Fire prevention, detection and suppression
- Intrusion detection systems

It's all about risk mitigation that is appropriate for the facility.

Examples of Elements of Physical Safeguards*

- Layers of security
  - Design
  - Access control
  - Intrusion detection
  - Monitoring

With minor tweaking, these layers and examples can apply to technical controls as well.

- Elements of Security Engineering
  - Obstacles:
    - to frustrate trivial attackers and delay serious ones
  - Alarms, security lighting, security guard patrols or closed-circuit television cameras
    - to make it likely that attacks will be noticed
  - Security response:
    - to repel, catch or frustrate attackers when an attack is detected.

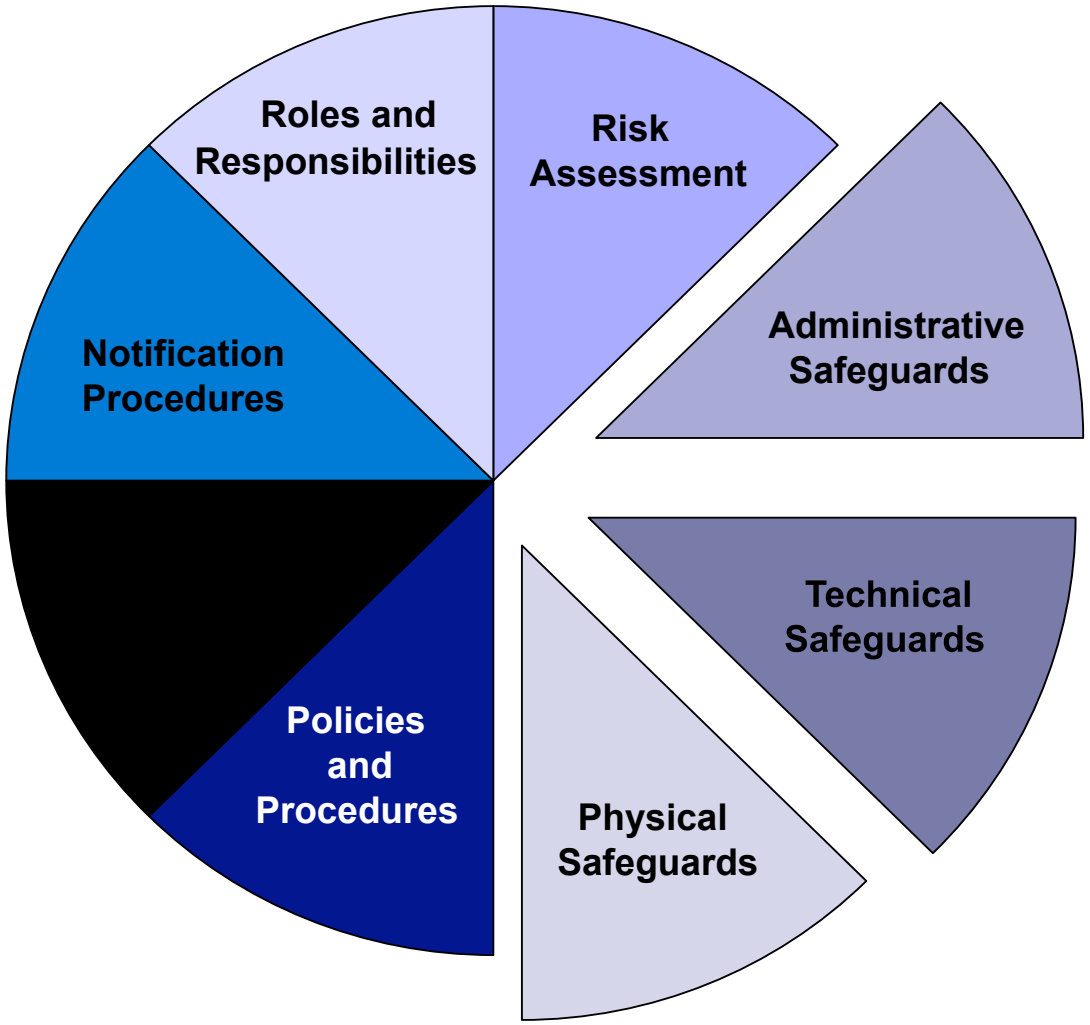
*Physical Security, http://en.wikipedia.org/wiki/Physical_Security.
Site known good April 2010.

Elements of Physical Safeguards
Example Goals

- Operations security
- Sound IT practices and security practices relevant to the operation are applied by the facility
- The safeguards that are appropriate for the facility

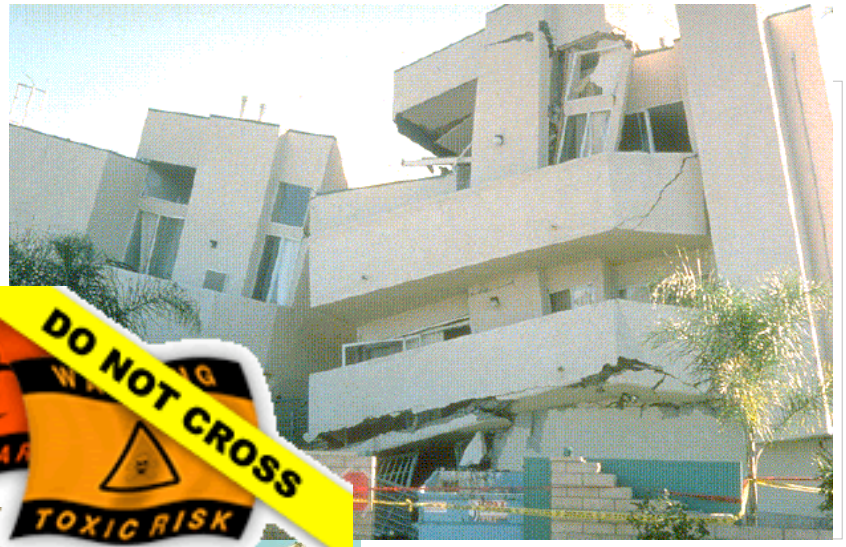
Work with program officer to define appropriate safeguards.

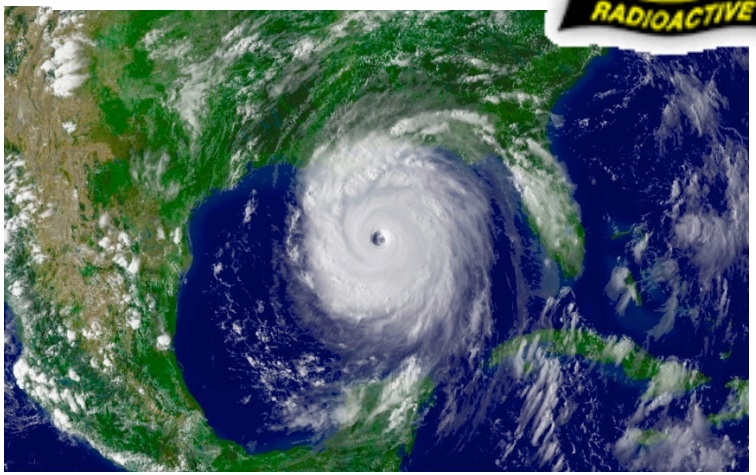
Administrative, Technical and Physical Safeguards (revisited)



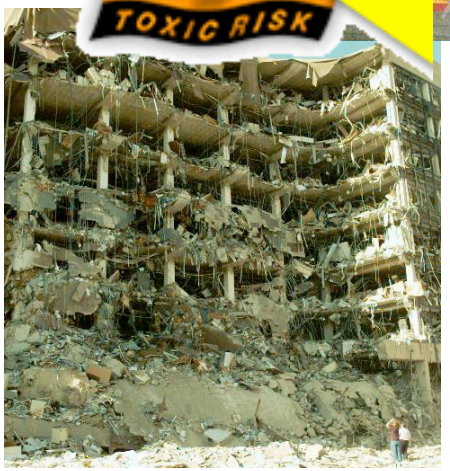
Administrative, Technical and Physical

Is it continuity of operations, disaster recovery or designing resiliency into systems OR all of the above ?





Hurricane Katrina 2005



Oklahoma City 1995

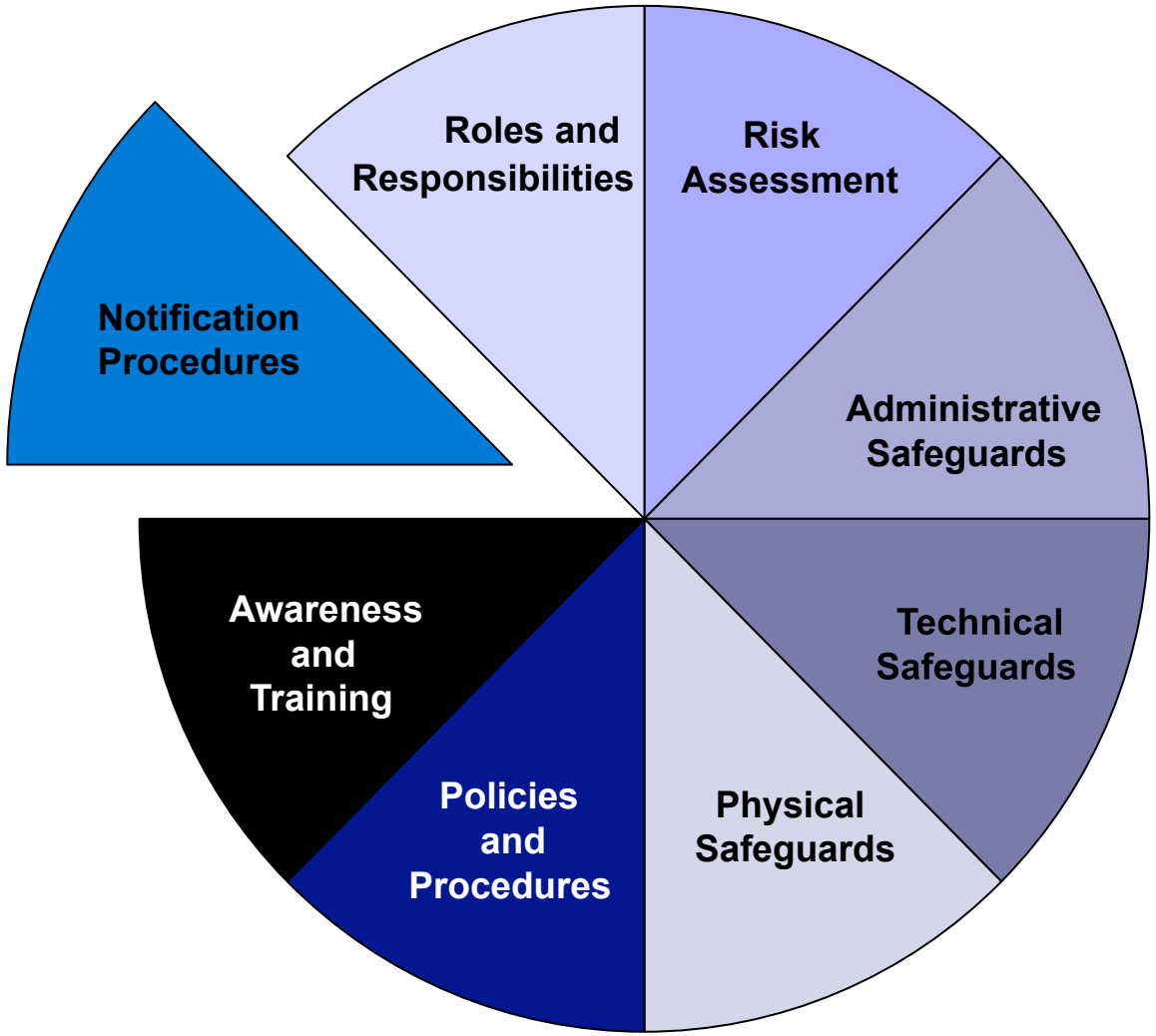
Technical, Administrative and Physical

Continuity of Operations
Business Continuity Planning
Resilient Systems

Working with the NSF Program Director, the Facility should determine:

- What is needed when
- How long a system or service can be “down”
- How to ensure data integrity
- Impacts
  - Inside the facility
  - Outside the facility
- And…

Notification Procedures in the Event of a Breach or Security Incident



Notification Procedures

- Understand the impact and ramifications of an incident or breach
- Ensure that everyone knows their roles and responsibilities, for example:
  - If you are a systems administrator, what do the IT security people need and want to know? And when?
  - If you are the IT security person, what does management want to know? And when?
- Develop procedures about notifications before an incident or breach occurs
- EDUCAUSE/Internet2 Cybersecurity Initiative Wiki has a great Data Incident Notification Toolkit

** Site known good April 2010.*

Examples Notification Procedures

- Internal to the facility
- External to the facility
  - Parent organization (if one exists)
  - Comparable facilities, especially if connected to the affected facility
- Law enforcement
- NSF (and other agencies)
- Users/customers

TeraGrid has procedures and processes
that could be used as a model.

Whether to report to NSF…

- Work with your Program Officer to decide
- Depends on the type or nature of the event
- Considerations
  - Email down: No
  - Device stolen: Yes, if not encrypted and depending on content
  - Data integrity is compromised: Yes
  - Egregious behavior or inappropriate use: Maybe
  - Cross-site incidents: Yes
  - Compromise: Yes
  - Facility will be “down”: Yes
  - Potential for legal action: Yes

When to report to NSF…

If…

- US CERT (Computer Emergency Response Team) is notified (Maybe)
- Other facilities are involved (Yes)
- Other agencies are being notified (Yes)
- Law enforcement is involved (Yes)

Or, if there is

- Risk of adverse publicity or press is/will be aware (YES)
- Reputational risk to the facility or its parent organization (if one exists) (Yes)
- Reputational risk to the National Science Foundation (YES)
- Potential for legal action (YES)
- …

Who to contact at NSF…
Define *a priori* with your Program Officer

Who to contact at NSF:

- NSF Program Officer(s)
- S/he notifies NSF Division Director
  - Discuss with NSF's FACSEC Working Group for guidance on further escalation

As Appropriate…

- NSF Division Director notifies NSF Assistant Director
- NSF Assistant Director notifies Deputy Director who notifies the Director
- …

How to report to NSF…
Define *a priori* with your Program Officer

Who will be contacting the Program Officer

- Some will want to hear from the PI
- Others may want to hear from the cyber-security officer

Establish a secure mechanism for communication

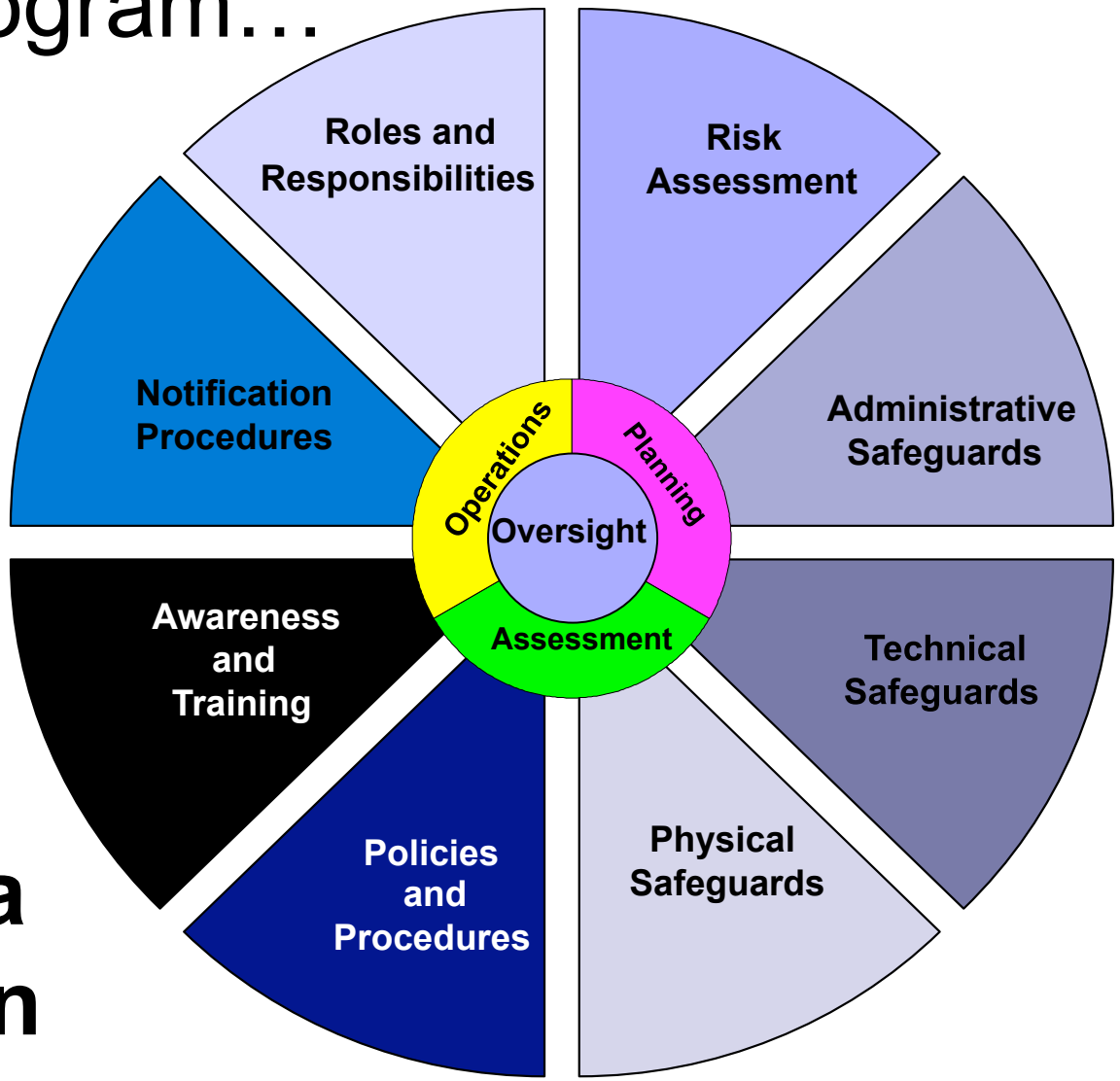
- If your computer, systems or network is compromised, don't sent email from it! (Duh!)
- Use encrypted email
- Telephone
- FAX

IT Security Program…

Elements of an IT Security Program

- Good planning
- Sound operations
- Continuous assessment

Good Management or Oversight



…becomes a Security Plan

In summary…

- Information Security is the awardee's responsibility
- Facility Security programs should be:
  - Sufficient to meet the needs of the facility
  - Appropriate to identified risks
- Facilities should:
  - Be encouraged to have good IT management practices
  - Recognize Information Security is one part of good IT operations
- Facilities need to recognize the roles of executives, management, technical staff, users

Don’t reinvent the wheel…

- Facilities have many resources available for their use:
  - Expertise and existing policies and procedures from their parent organization or institution (if they have one)
  - Example security programs of some other Large Facilities
  - Community best practices
    - EDUCAUSE, Internet2, universities
  - Published standards and guidance from NIST, SANS and other organizations

Remember…

- It's about risk mitigation
- Information security programs and plans will improve over time
- Information security is a journey not a destination

Good IT practices foster good security.

Good IT security reflects good IT practices.

Questions?

Ardoth Hassler
Associate Vice President,
University Information Services
Georgetown University
hasslera@georgetown.edu

Senior IT Advisor (1/2007 – 1/2011)
Division of Information Systems
Office of Information and Resource Management
National Science Foundation

Supplemental Materials and References

Identity Management: What problems are we trying to solve?

- Reduce the need for multiple usernames and passwords
- Reduce amount of personal data held by third parties
- Reduce the duplication of effort across multiple institutions
- Enable publishers, service and network providers to have a common interface for multiple systems
- Ease the difficulty in sharing resources between institutions and organizations
- Enable citizens to access government services

What is federated identity?

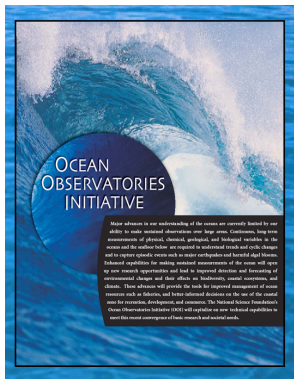
- “Federated identity management allows users to log in using their local authentication credentials (username and password assigned by their institution) to access electronic resources hosted at other institutions belonging to the same identity federation.” *www.incommonfederation.org*
- Federated identity is designed to address:
  - Multiple passwords required for multiple applications
  - Scaling the account management of multiple applications
  - Security issues associated with accessing third-party services
  - Privacy
  - Interoperability within and across organizational boundaries

InCommon

"InCommon eliminates the need for researchers, students, and educators to maintain multiple, passwords and usernames. Identity providers manage the levels of their users' privacy and information exchange. InCommon uses SAML-based authentication and authorization systems (such as Shibboleth®) to enable scalable, trusted collaborations among its community of participants."

- InCommon Federation *www.incommonfederation.org*
  - Mission: create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the US
- US Research and Education Federation
  - Separate entity with its own governance
  - Operations managed by Internet2
  - Members are degree granting accredited organizations and their partners
    - 197 universities and colleges are members as of 1/2011

Large Research Facilities are Already Joining InCommon



Ocean Observatories Initiative

TeraGrid

Fermi National Accelerator Laboratory

Argonne National Laboratory

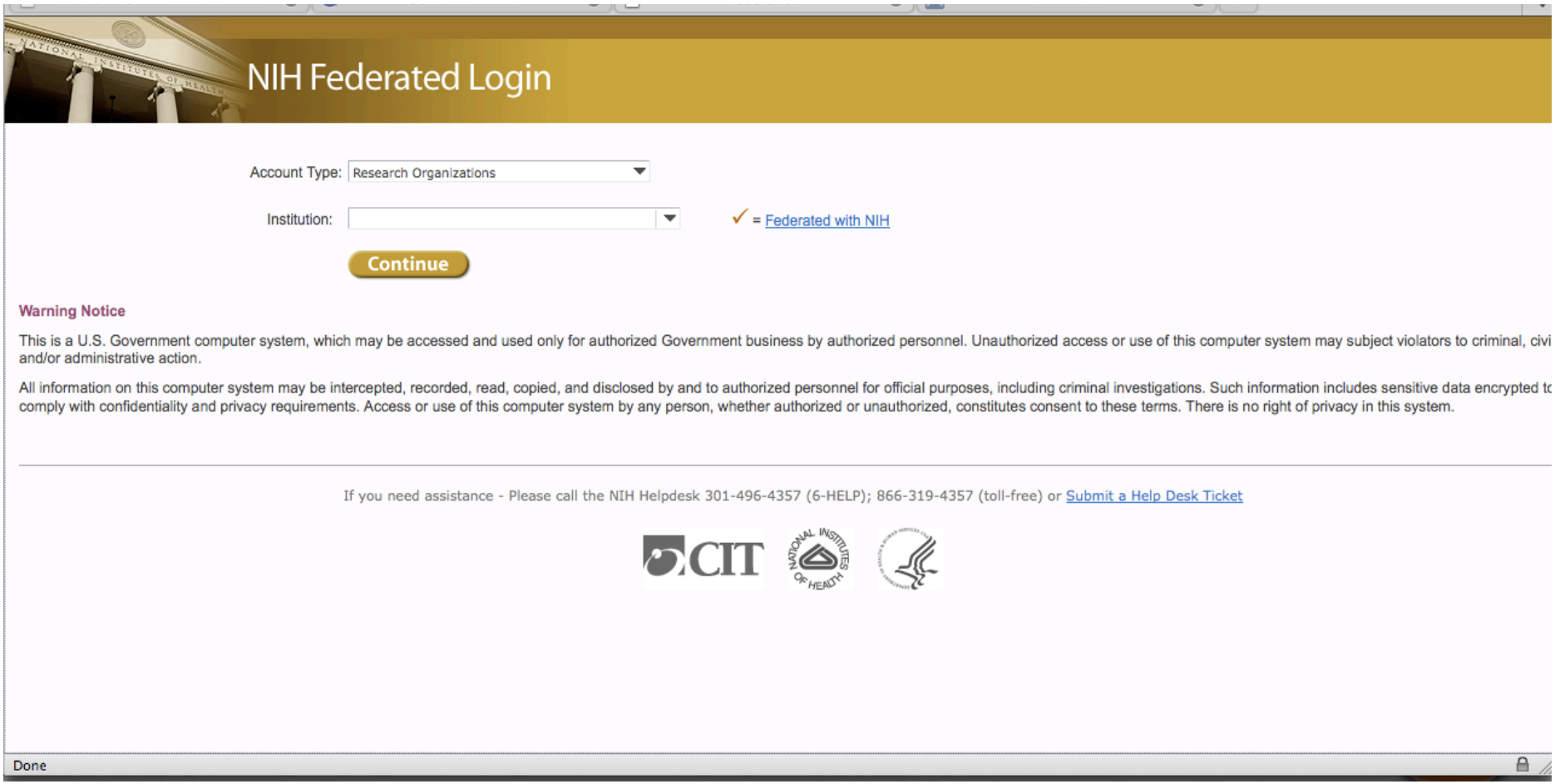
Lawrence Berkeley National Laboratory

Considering InCommon membership:
- Laser Interferometer Gravitational-Wave Observatory (LIGO)
- Long Term Ecological Research (LTER)
- National Ecological Observatory Network (NEON)
- Open Science Grid (OSG)

Example of Research.gov access at NSF when Federation is fully implemented

User selects login path

National Institutes of Health



Sources of Best Practices

- Consortia
  - NEES
- Security Policies
  - EDUCAUSE Resource Center
  - EDUCAUSE/Internet2 Wiki
  - Other similar institutions
- Incident Handling and Response
  - TeraGrid Security Working Group
  - Yale University
- From prior Summits: Carnegie-Mellon, UT Austin, Cornell
- And many more…

Access Management and Oversight Initiatives

- InCommon Federation
- Internet2 Middleware Initiatives
  - Shibboleth Project
- JA-SIG Central Authentication Service (CAS)
- International
  - UK Joint Information Systems Committee (JISC)
  - Internet2 lists 18 Federations

References

- NIST Computer Security Resource Center
- EDUCAUSE/Internet2 Computer and Network Security Task Force Security Guide
- The Center for Internet Security
- International Standards Organization
- SANS (SysAdmin, Audit, Network, Security) Institute SANS
- Control Objectives for Information and related Technology (COBIT)
- Wikipedia

Photos and Graphics Courtesy:

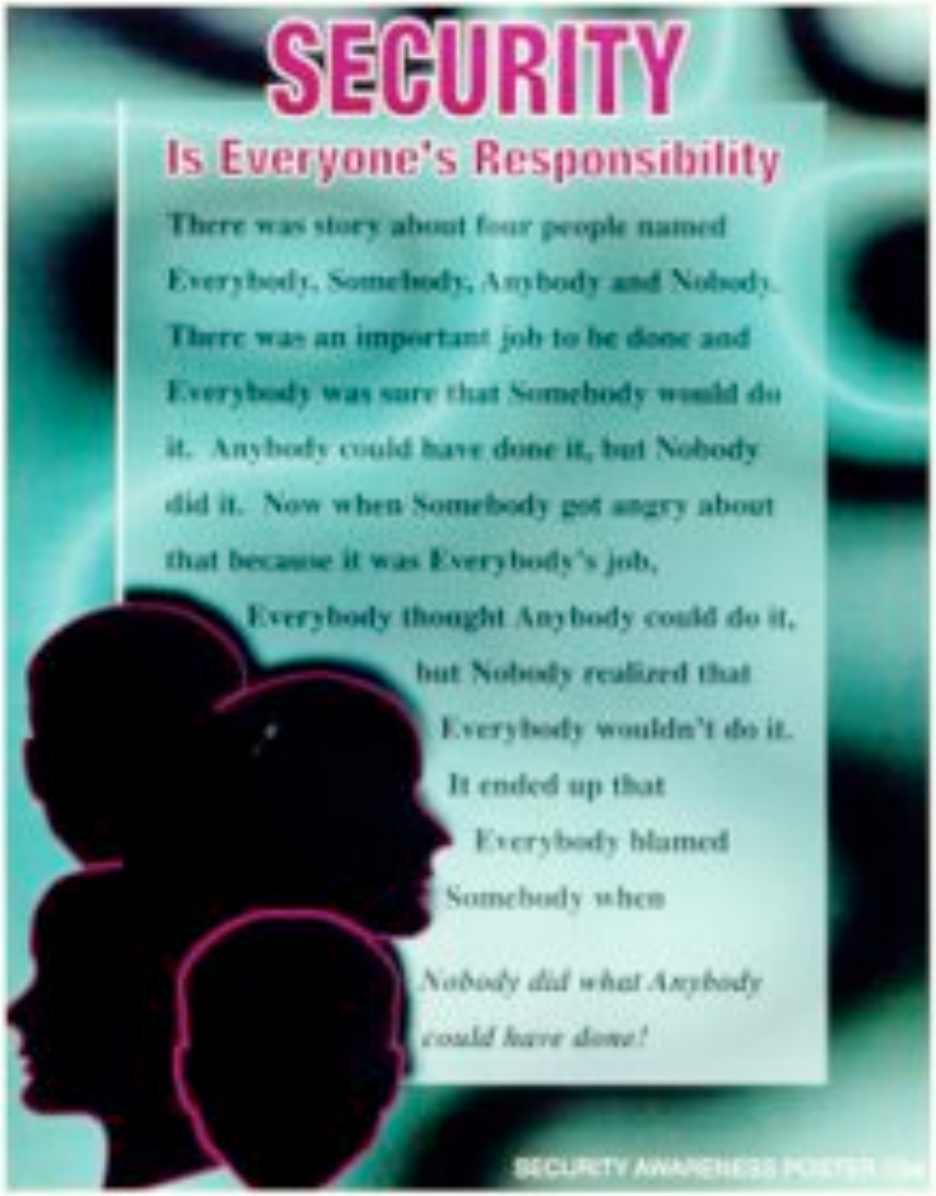
- EDUCAUSE and Internet2
- NSF and the Large Facilities
- Datalossdb Open Security Foundation
- Wikipedia (public domain or permission to use)
- Oklahoma City: oklahomacitybombing.com
- US Department of Commerce

A word about Wikipedia…

CNET says about Wikipedia*:

- "The good: Wikipedia is free and easy to access; extensive information; evolving constantly; multiple languages; enormous collection of articles and media; works in any browser."
- "The bad: Not always accurate or complete; vulnerable to vandalism or bias; uninspiring interface; inconsistent writing; editing inaccuracies not intuitive; requires Web access for recent content."
- "The bottom line: Wikipedia offers rich, frequently updated information online, but you might need to verify some of its facts."
- For IT security: Definitions are consistent with other sources and reference links are to sources IT professionals would expect to find and use.

* CNET Network: http://reviews.cnet.com/general-reference/wikipedia/4505-3642_7-31563879.html.
Site known good April 2010



* Poster from US Department of Commerce

This is a little story about four people named Everybody, Somebody, Anybody, and Nobody.

There was an important job to be done and Everybody was sure that Somebody would do it.

Anybody could have done it, but Nobody did it.

Somebody got angry about that because it was Everybody's job.

Everybody thought that Anybody could do it, but Nobody realized that Everybody wouldn't do it.

It ended up that Everybody blamed Somebody when Nobody did what Anybody could have done