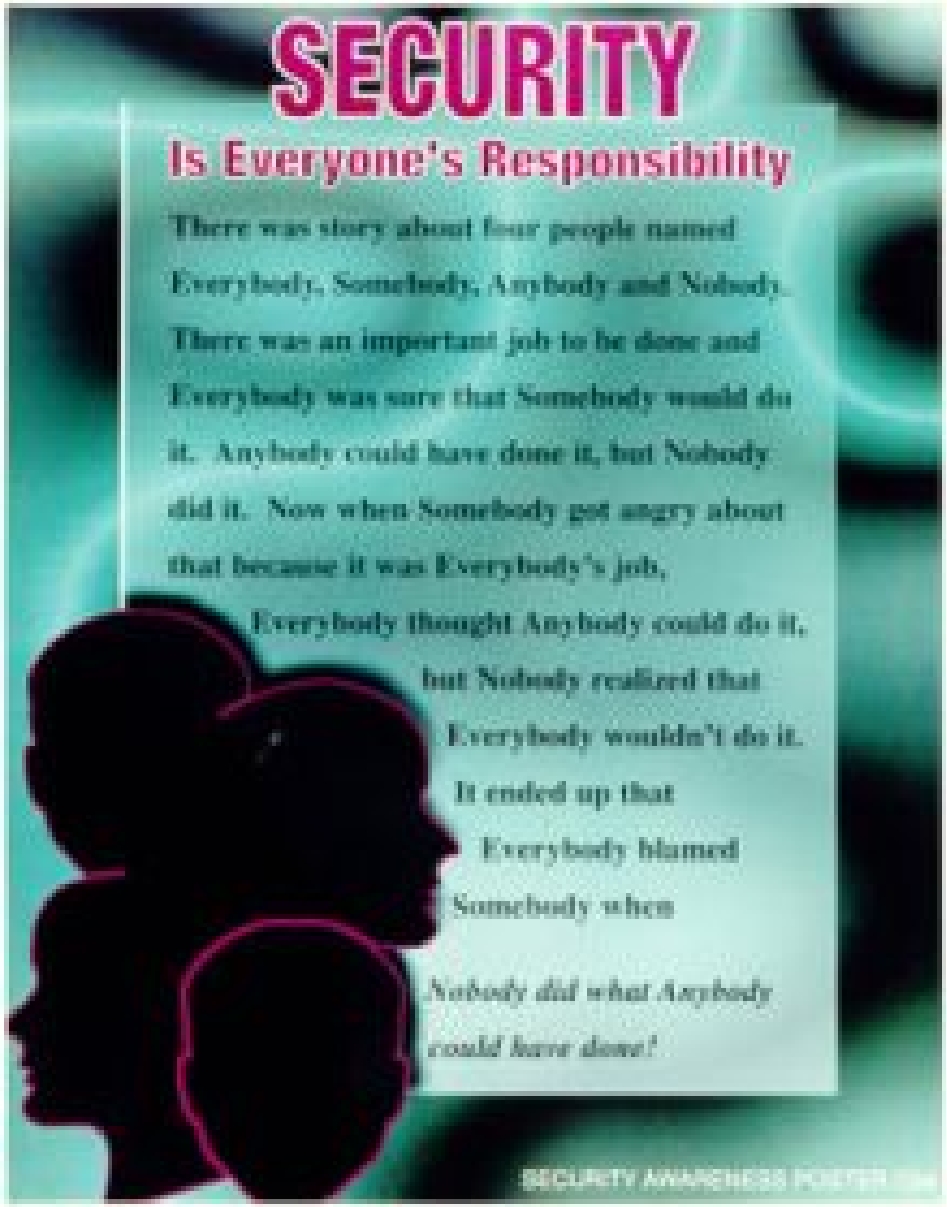


* Poster from US Department of Commerce

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

Cybersecurity 2010… and beyond

What Makes a Good Security Plan?

Ardoth Hassler
Senior IT Advisor
National Science Foundation

Associate VP University Information Services
Georgetown University

“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

Top Cyber Security Menaces:
#3 – "*Cyber Espionage Efforts To Extract Large Amounts of Data - Particularly Using Targeted Phishing*"

"…massive penetration of federal agencies and defense contractors and theft of terabytes of data by the Chinese and other nation states [reported] ."

"…Economic espionage will be increasingly common as nation-states use cyber theft of data to gain economic advantage in multinational deals."

Top Ten Cyber Security Menaces for 2008
SANS Institute. http://www.sans.org/2008menaces/

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

President Barack Obama
Washington, DC
May 29, 2009

"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

Expanded Very Large Array

LIGO

NCAR

NPACI

TeraGrid

IODP
INTEGRATED OCEAN DRILLING PROGRAM

NNIN

NEES

GEMINI OBSERVATORY

WATERS NETWORK

NATIONAL NANOFABRICATION USERS NETWORK

NRAO

University-National Oceanographic Laboratory System

Open Science Grid

NCSA

incorporated research institutions for seismology

IRIS

neon
NATIONAL ECOLOGICAL OBSERVATORY NETWORK

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
  - Cost of TeraGrid's STAKKATO Incident in 2003-2004
    - Not calculated

What is at stake…

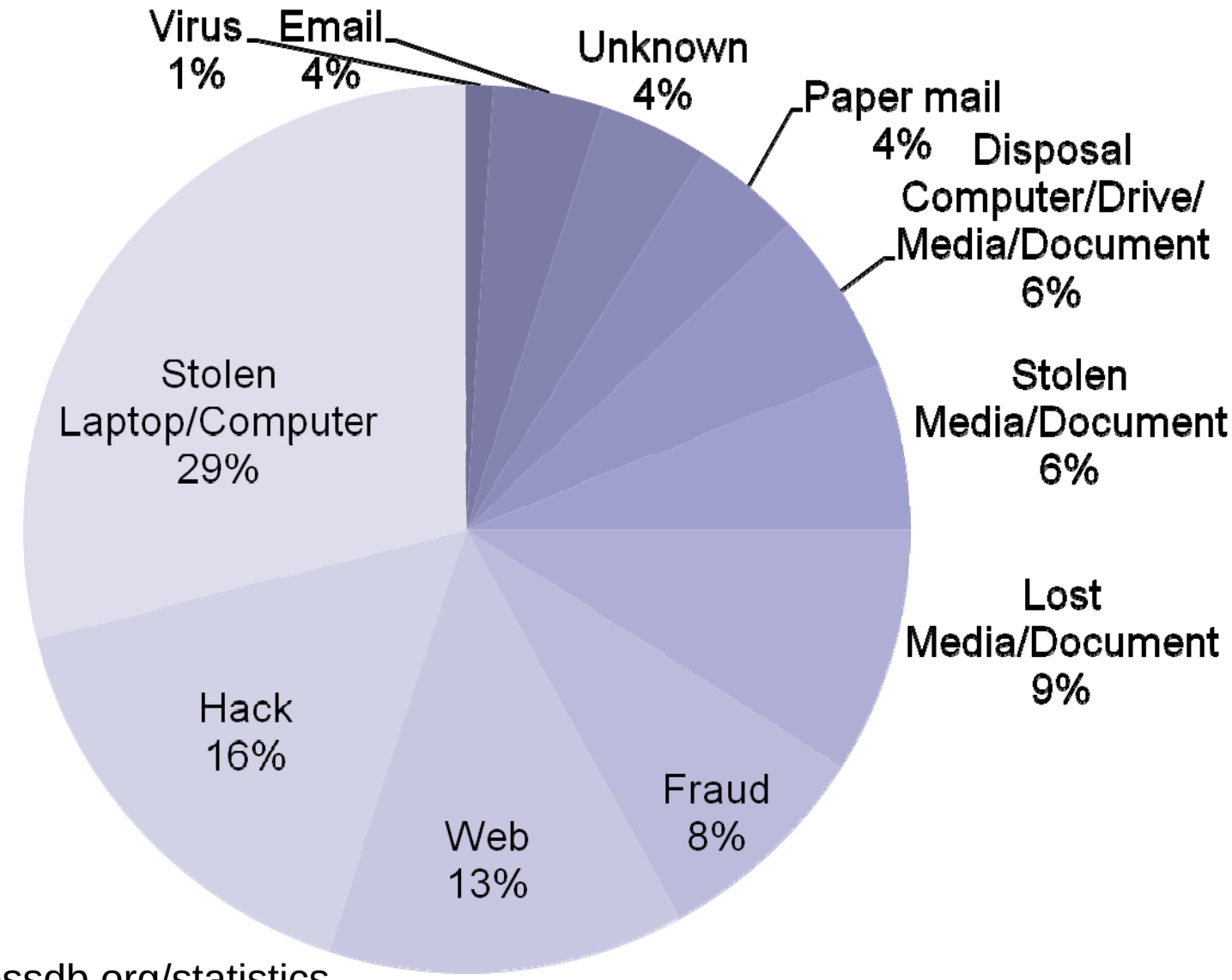
- Reputational damage
  - Institution or agency: can’t estimate
  - PII disclosure of patient or alumni data: priceless
- Data integrity compromise
  - Would you know if a data element was changed?

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

REPORTED *Data* Loss

- 2009
  - Total Incidents: 480
  - Total Records Affected: 220,596,330
- 2008
  - Total Incidents: 732
  - Total Records Affected: 86,774,154

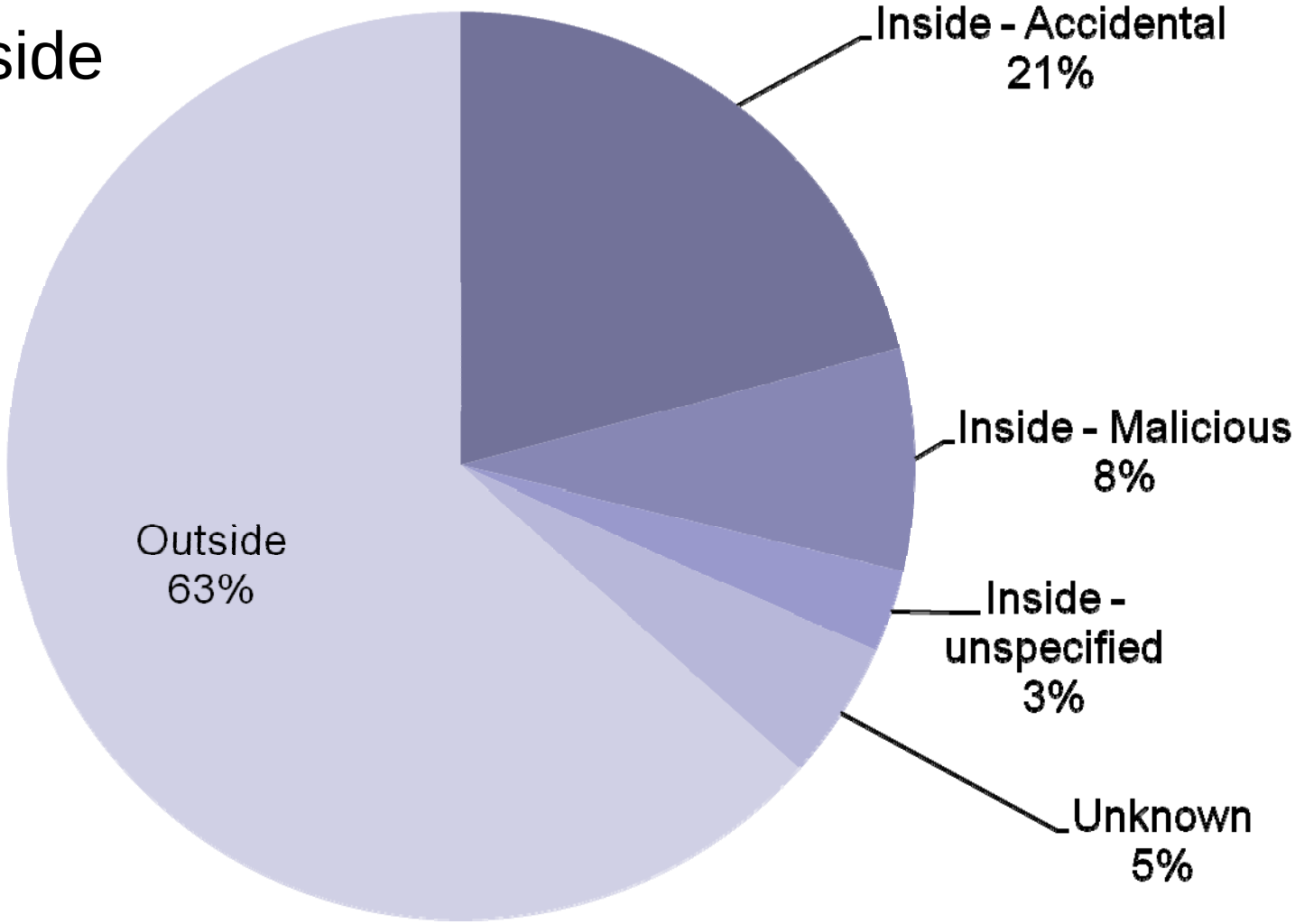
Data Loss Incidents by Type



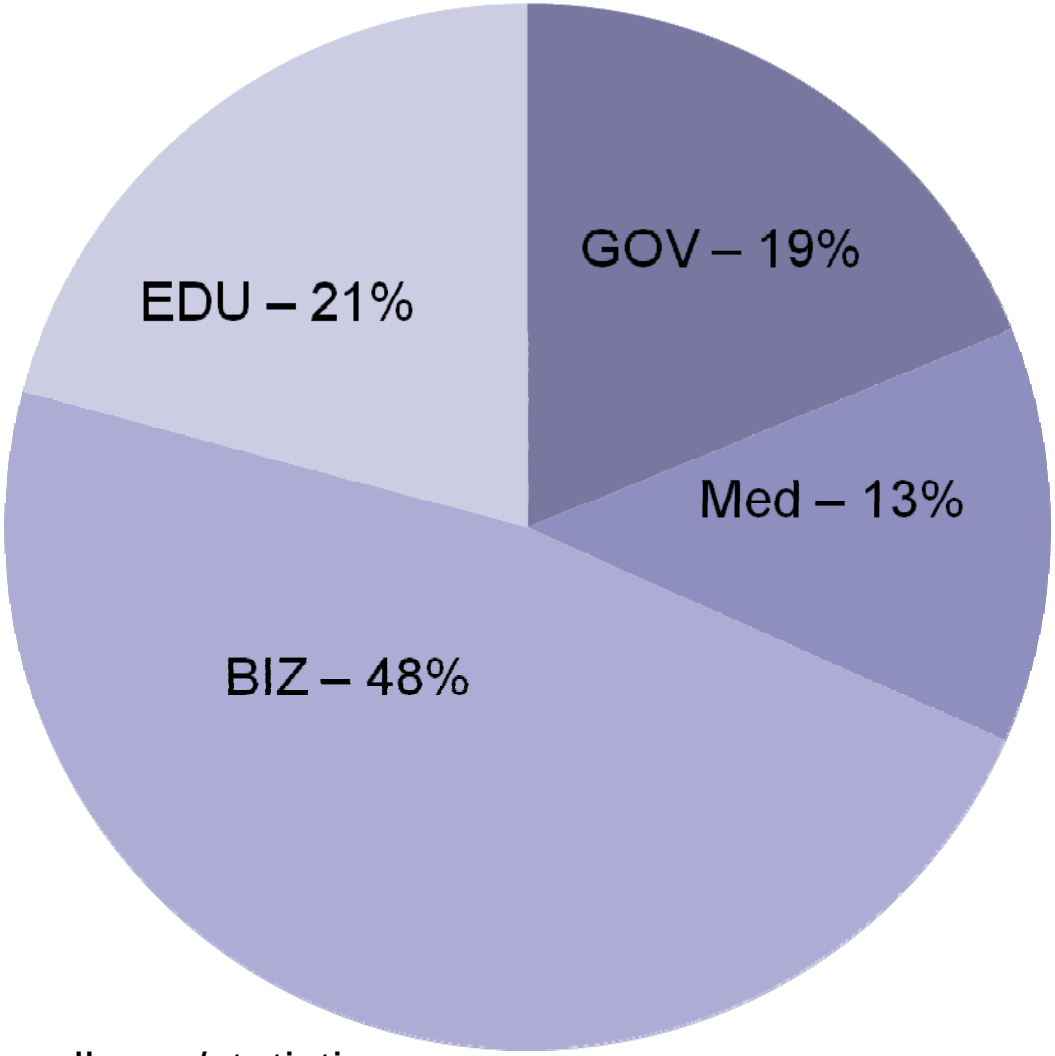
http://www.datalossdb.org/statistics

Data Loss Incidents by Vector

1/3 are inside

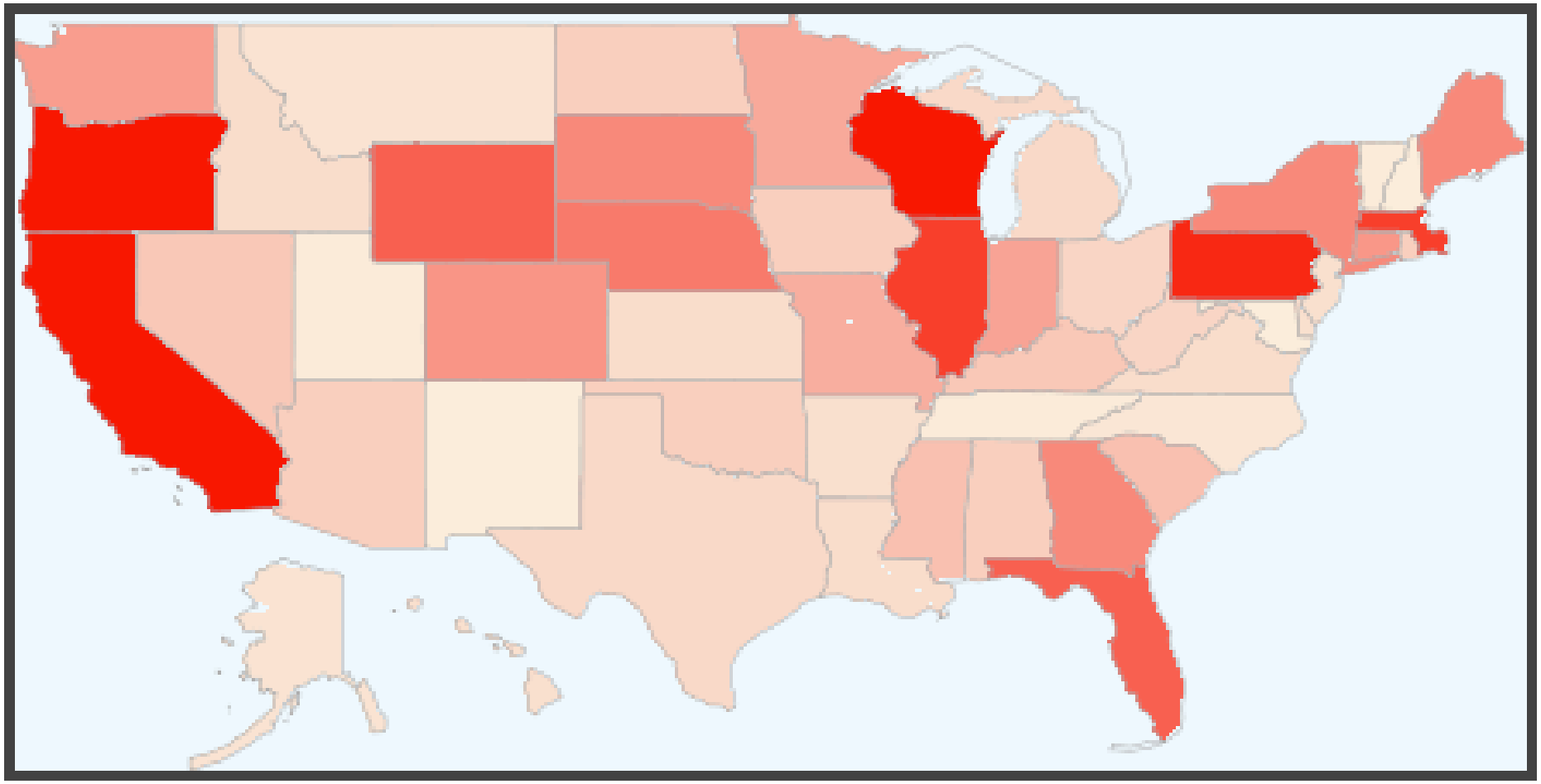


Data Loss by Business Type



http://www.datalossdb.org/statistics

Dataloss by HQ Location



Expanded Very Large Array

LIGO

NCAR

NPACI

TeraGrid

NHMFL

IODP

NNIN

NEES

GEMINI OBSERVATORY

WATERS NETWORK

NATIONAL NANOFABRICATION USERS NETWORK

NRAO

University-National Oceanographic Laboratory System

Open Science Grid

NCSA

incorporated research institutions for seismology

IRIS

neon

NATIONAL ECOLOGICAL OBSERVATORY NETWORK

Information Security: 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.
- For managers, Information Security starts with policy.

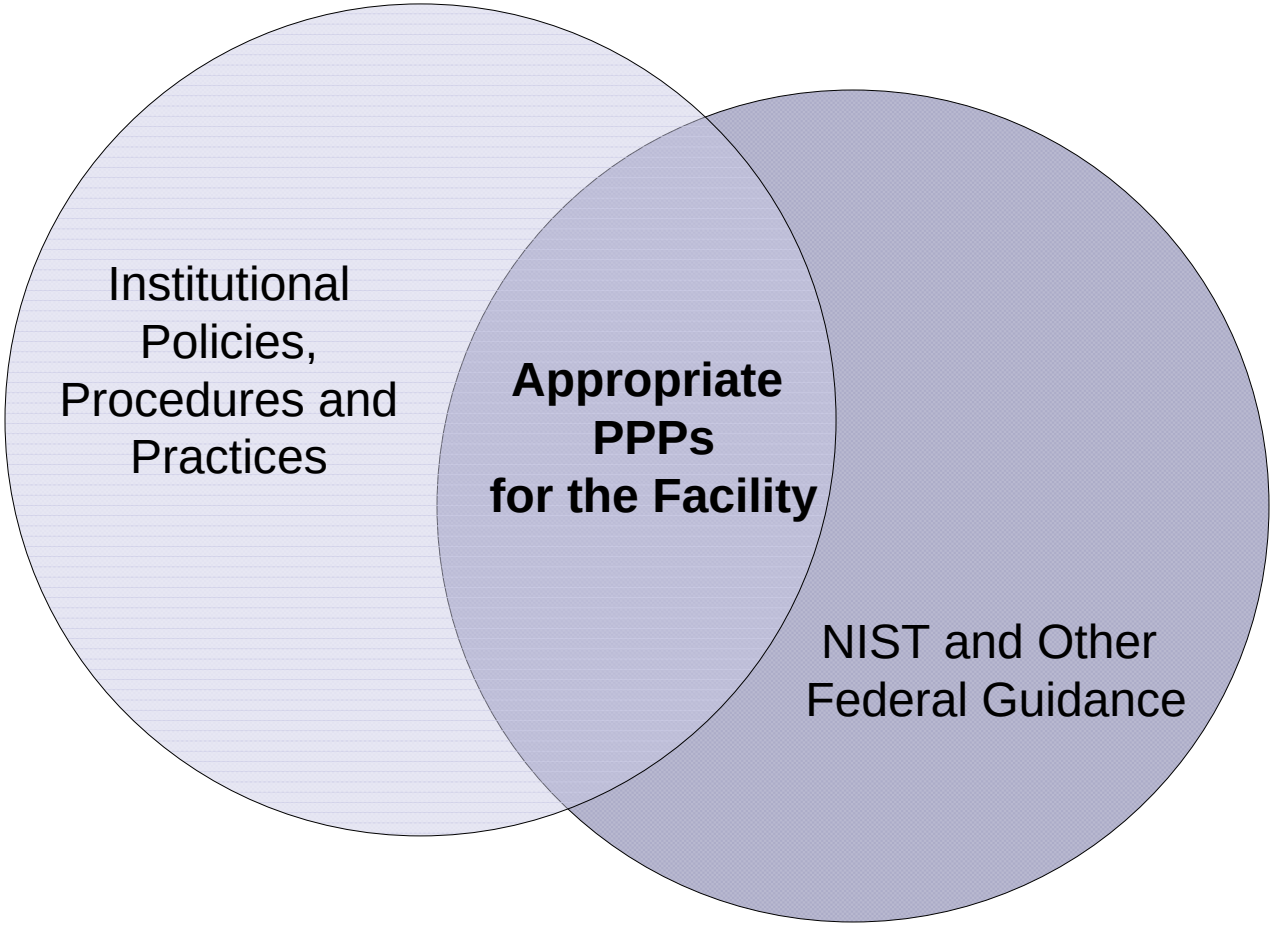
Starting with Policies

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.

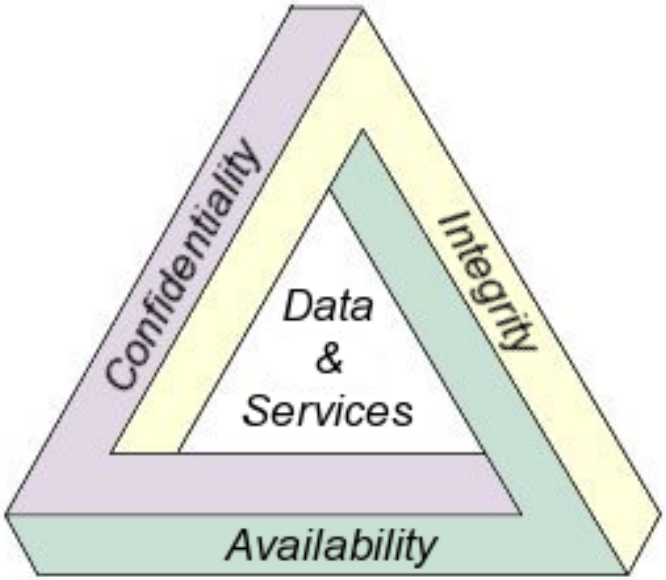
Background

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

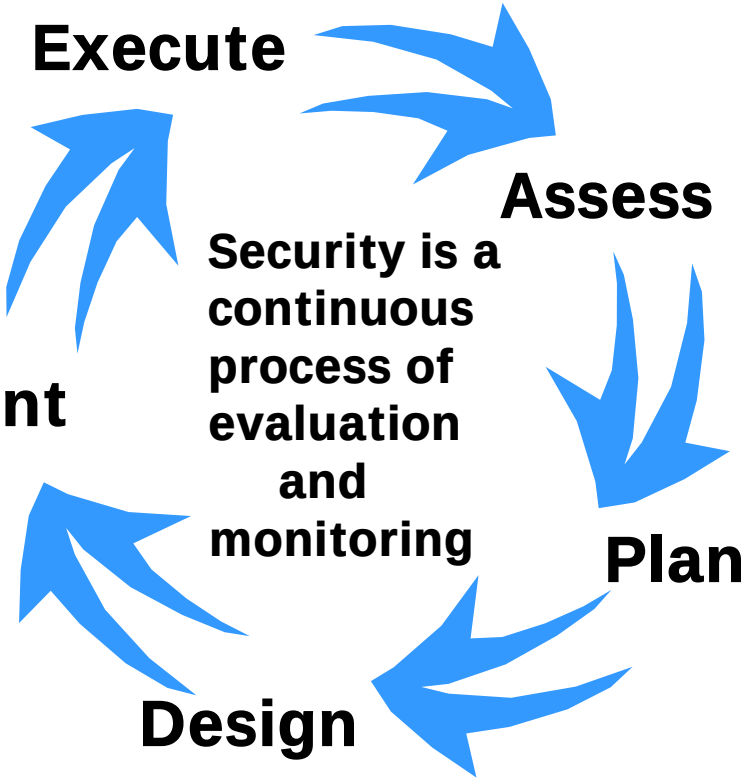


* Confidentiality, Integrity and Availability definitions taken from Wikipedia.
See: http://en.wikipedia.org/wiki/Information_security#Confidentiality.2C_integrity.2C_availability.
Site known good April 2010. Diagram is in the public domain.

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



Execute

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

Assess

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

Plan

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

Design

- Policy
- Standards
- Enterprise Architecture
- Configuration Standards

Implement

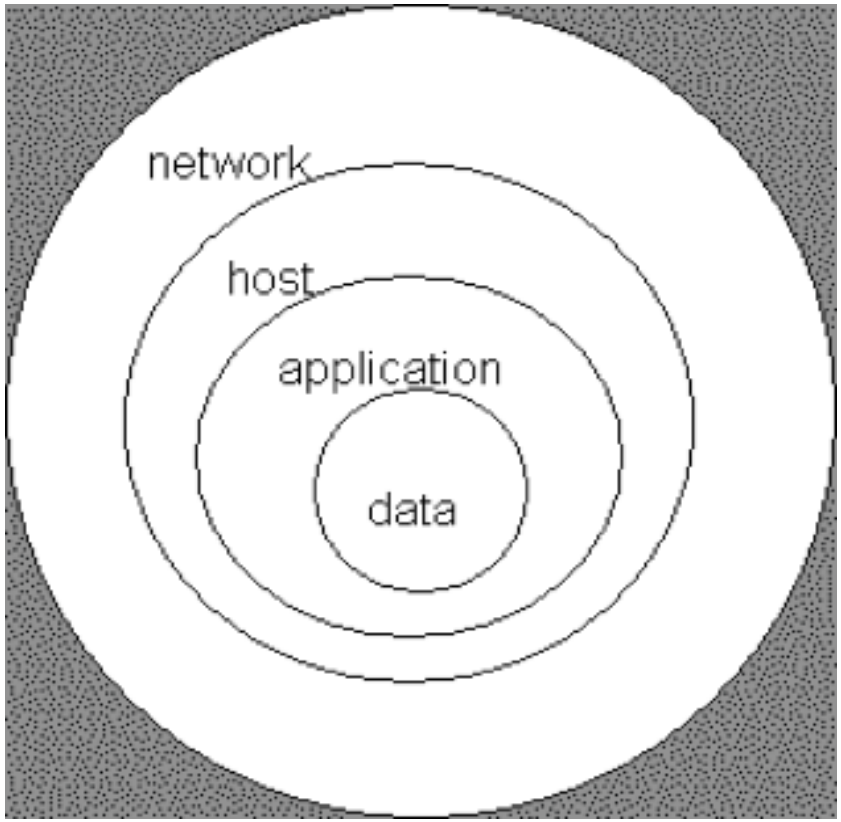
- Product Selection
- Product Implementation
- Top-down Security
- Management

Security Fundamentals

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

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.*

Use the Language of the Cooperative Agreement as a Framework for a Security Plan

NSF Cooperative Agreements Information Security Requirement

- Incorporated in NSF's Supplemental Financial and Administrative Terms and Conditions:
  - CA-FATC – Large Facilities: Article 51
  - CA-FATC – FFRDCs: Article 54
- 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 Cyber-security summits.

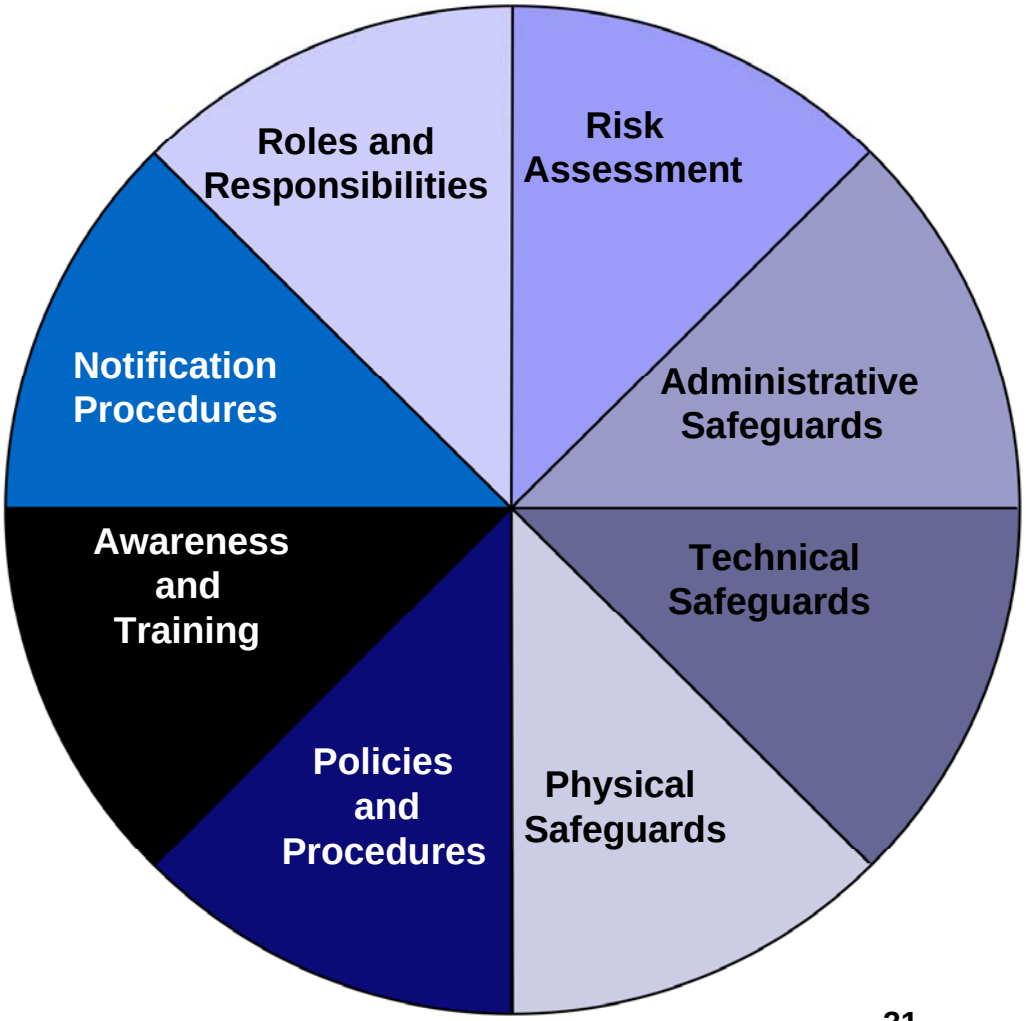
Information Security Responsibilities

- 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.

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



IT Security Program…

Elements of an IT Security Program
•Good planning •Sound operations •Continuous assessment
Good Management or Oversight

…becomes a Security Plan

Best Practices that Might Be Useful to NSF Large Facilities*

- Addresses CA language
- References readily available resources such as NIST,SANS, ISO, EDUCAUSE/Internet2…
- Encourages collaboration and information sharing among facilities
- Describes elements of a security program/plan

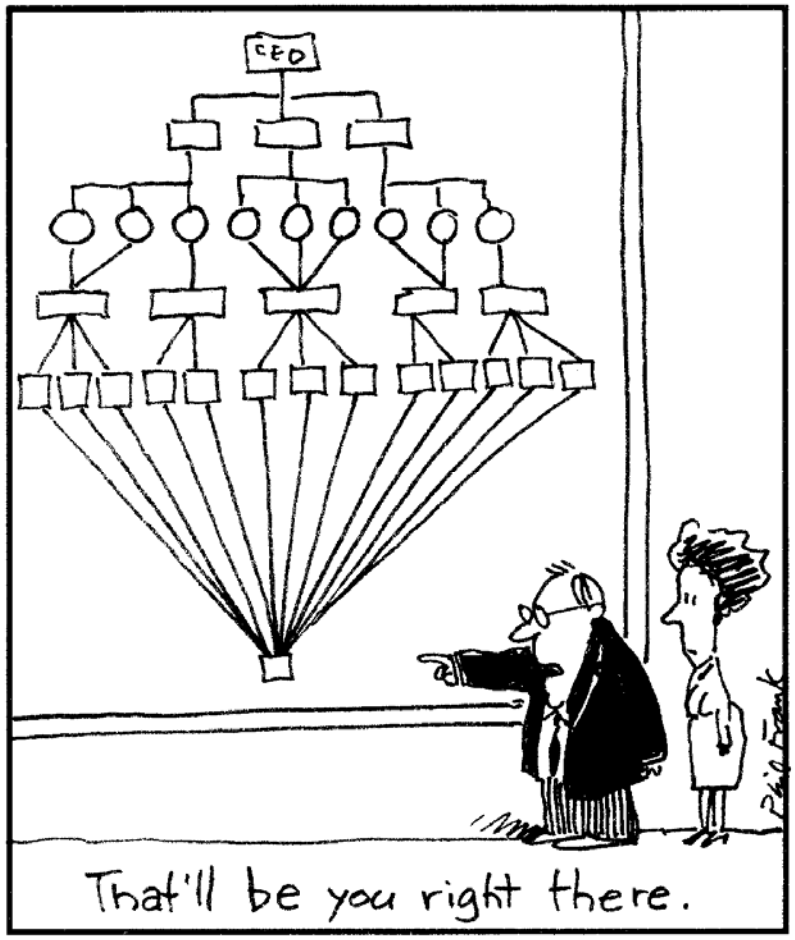
* http://tinyurl.com/yauxcvv

NUGGETS

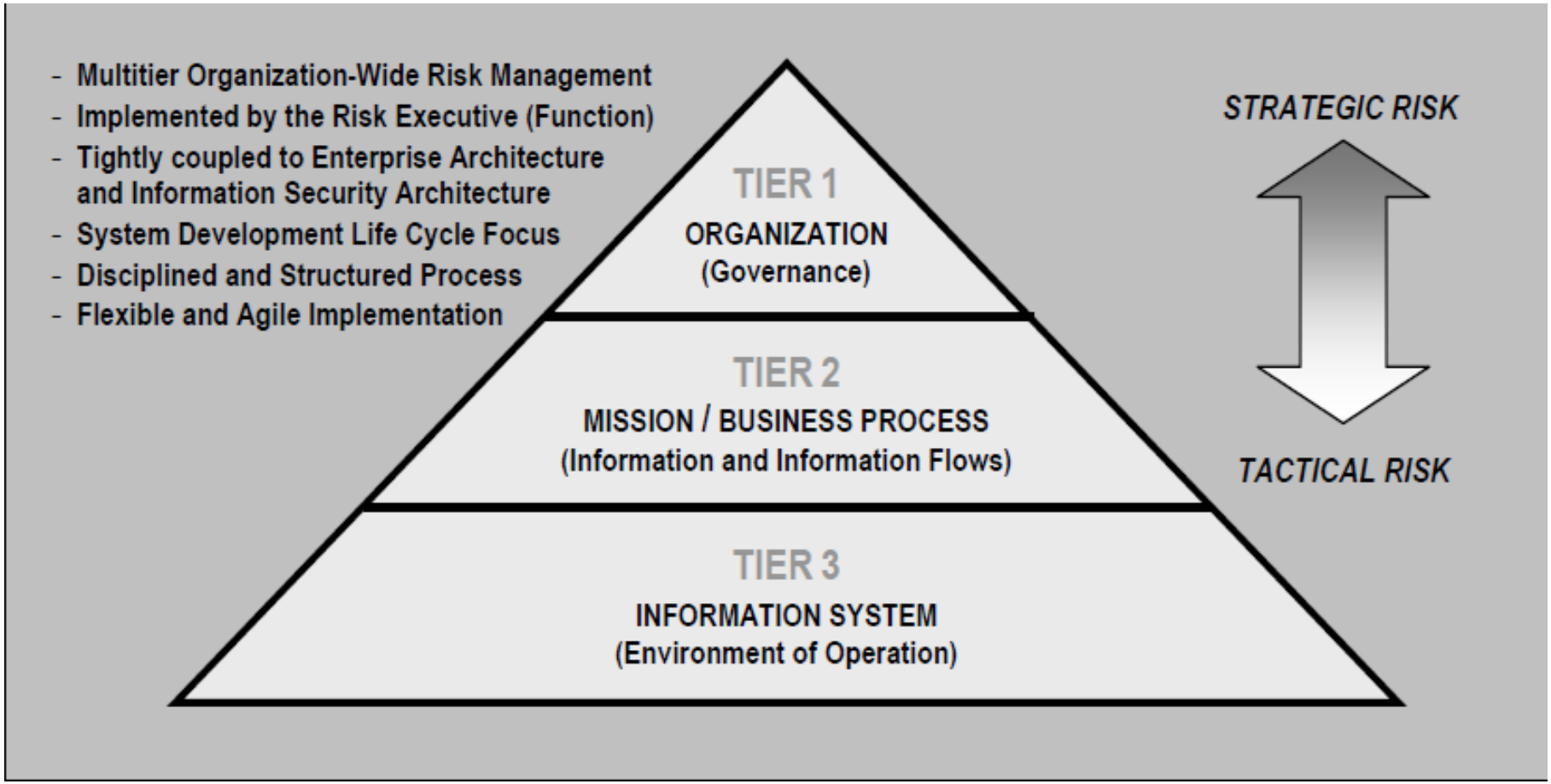
Roles and Responsibilities

Principles

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



Integrated Organization-wide Risk Management



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

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 2008

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

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.***

Security Awareness Training Needs to Focus on Many Levels of the Organization

- 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

Security Awareness Training Needs to Focus on Many Levels of the Organization

- 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

Identity and Access Management

- 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

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

What problems are we trying to solve?

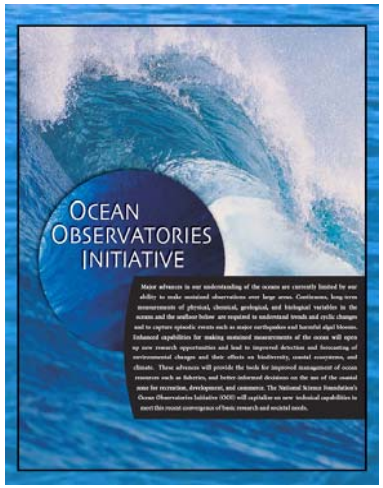
- Reduce the need for multiple usernames and passwords
- Reduce amount of personal data held by third parties
- Reduce the duplication of effort across multiple institutions
- Enable publishers, service and network providers to have a common interface for multiple systems
- Ease the difficulty in sharing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

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

Agency Large Research Facilities are Already Joining InCommon



Ocean Observatories Initiative

Laser Interferometer Gravitational-Wave Observatory

TeraGrid

Argonne National Laboratory

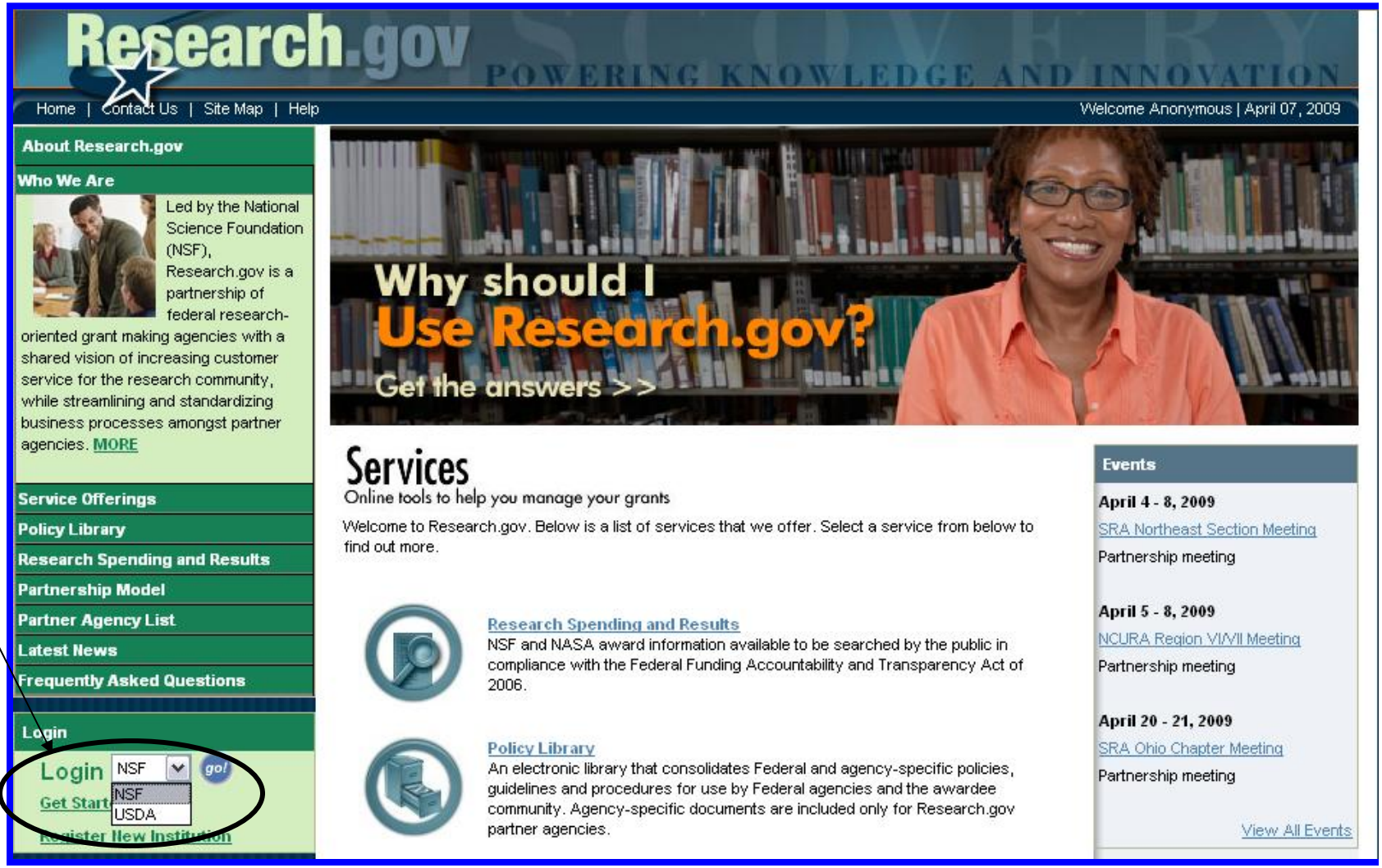
Lawrence Berkeley National Laboratory

Considering InCommon membership:

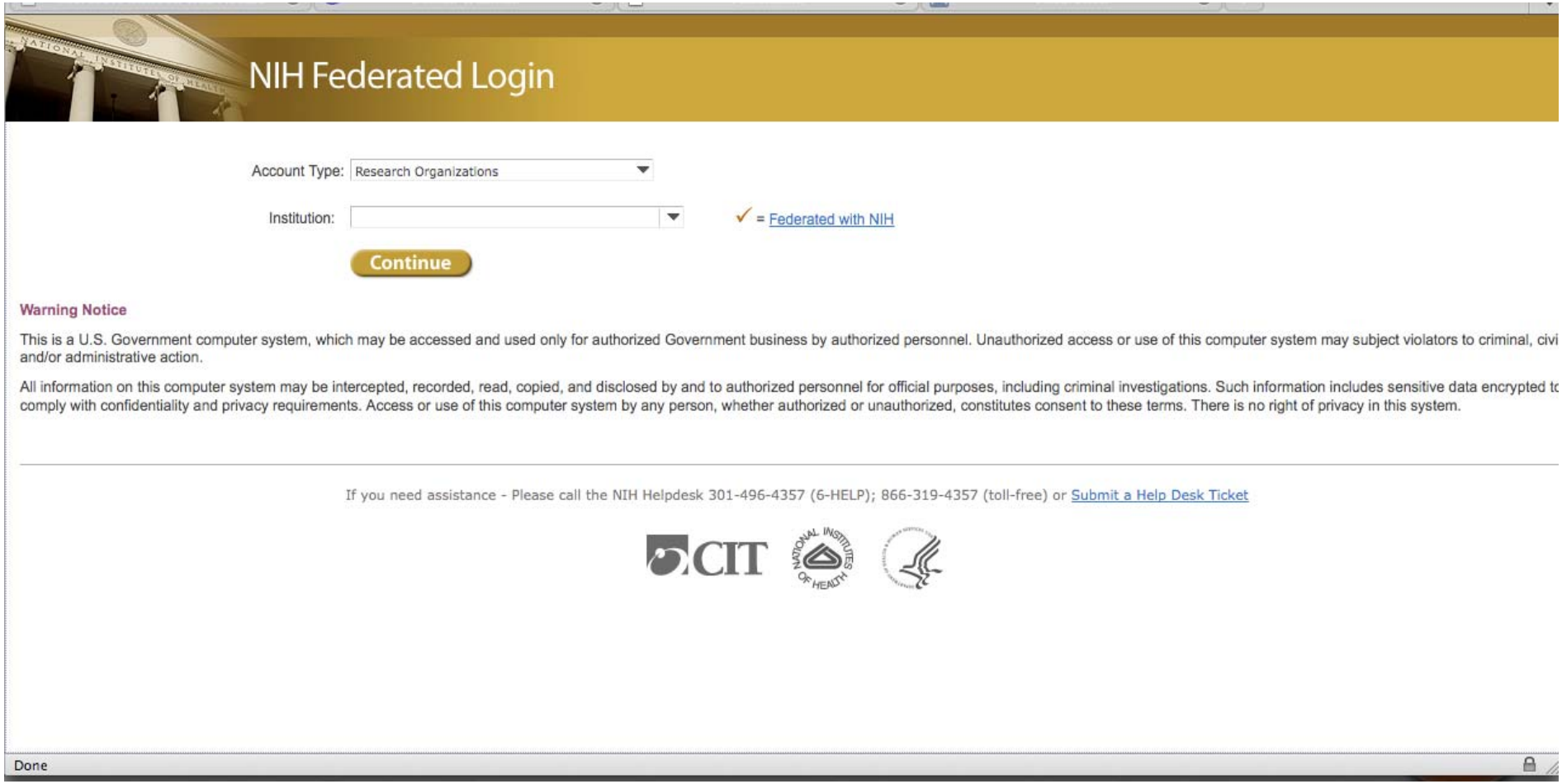
- Laser Interferometer Gravitational Wave Observatory (LIGO)
- Long Term Ecological Research (LTER)
- National Ecological Observatory Network (NEON)
- Open Science Grid (OSG)

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

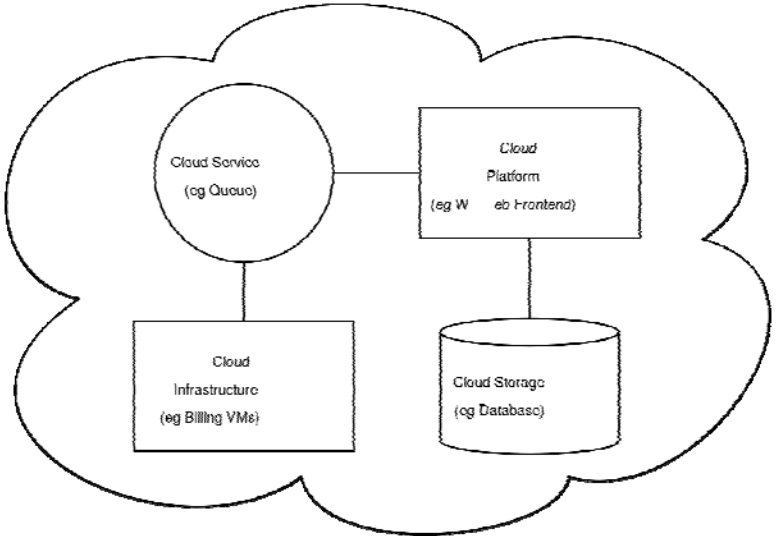
User selects login path



National Institutes of Health



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?

NOTIFYING NSF

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

When to report to NSF…

If…

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

Or, if there is

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

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

In summary…

- Information Security is the awardee's responsibility
- Cybersecurity is not an entity unto itself but integral to complex enterprises

In summary…

- 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 plans and programs of other Large Facilities
  - Community best practices
    - EDUCAUSE, Internet2, universities
  - Published standards 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.

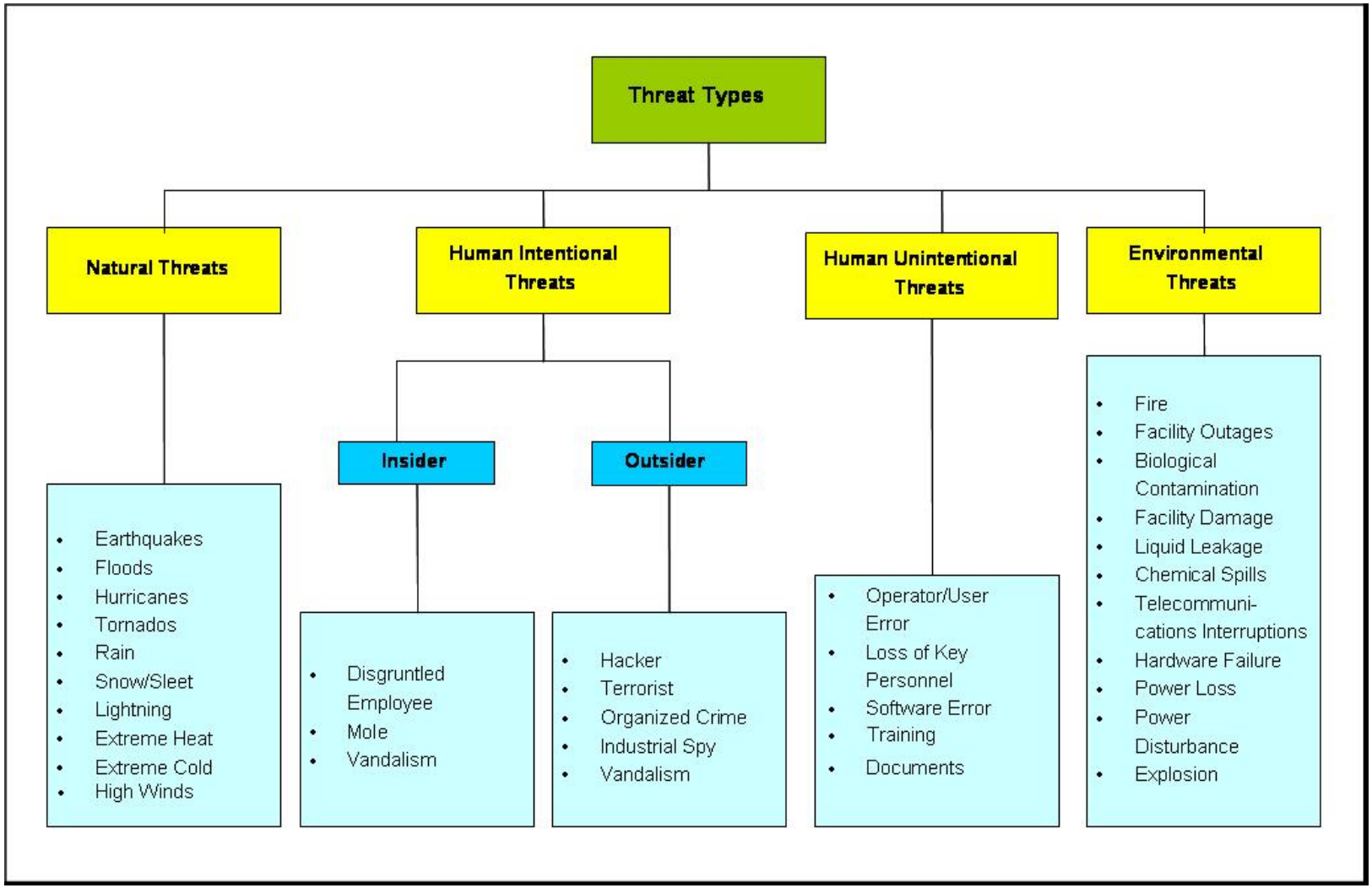
Questions?

Ardoth Hassler
Senior IT Advisor, NSF
ahassler@nsf.gov

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

Resources/Supporting Materials

Examples of Threat Types

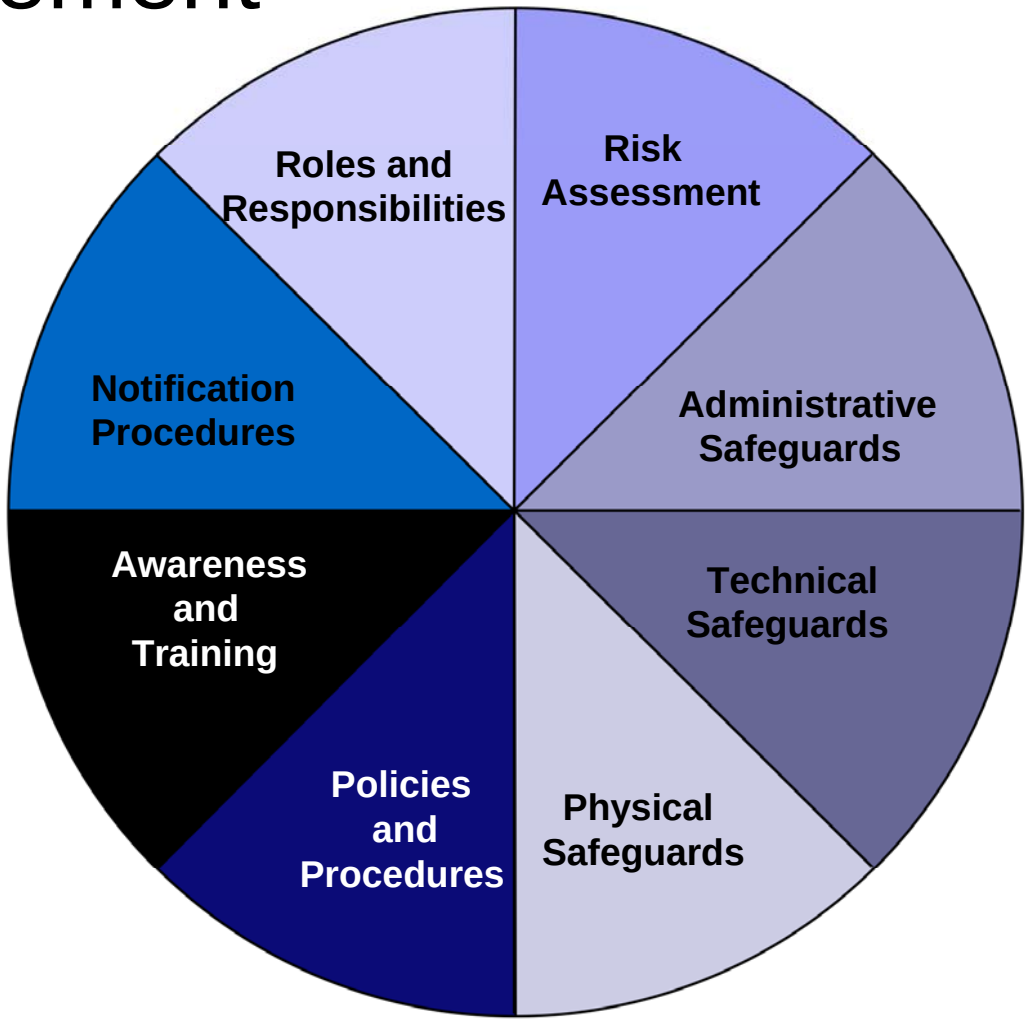


Ref: NIST 800-30 *Risk Guide for Information Technology Systems*

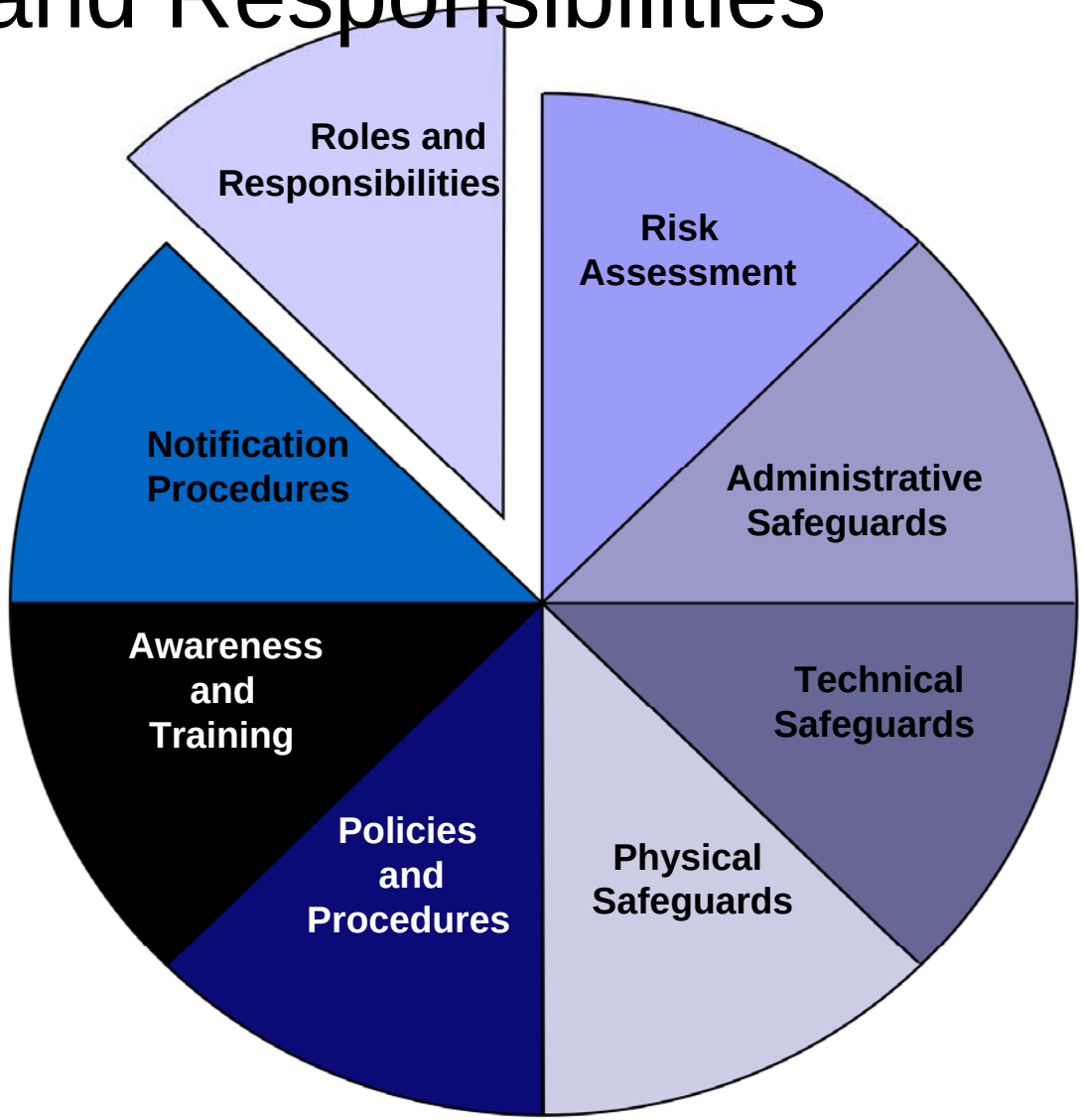
Awardee Responsibilities under the Cooperative Agreement

Summary of IT Security Program

- roles and responsibilities
- risk assessment
- technical safeguards
- administrative safeguards
- physical safeguards
- policies and procedures
- awareness and training
- notification procedures



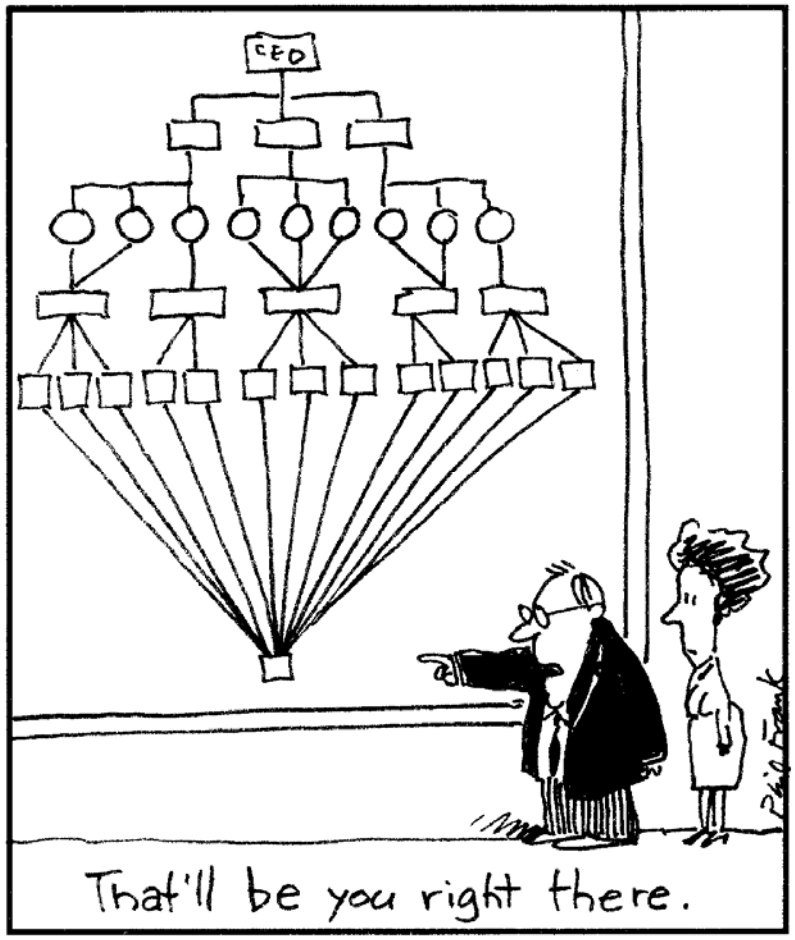
Roles and Responsibilities



Roles and Responsibilities

Principles

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

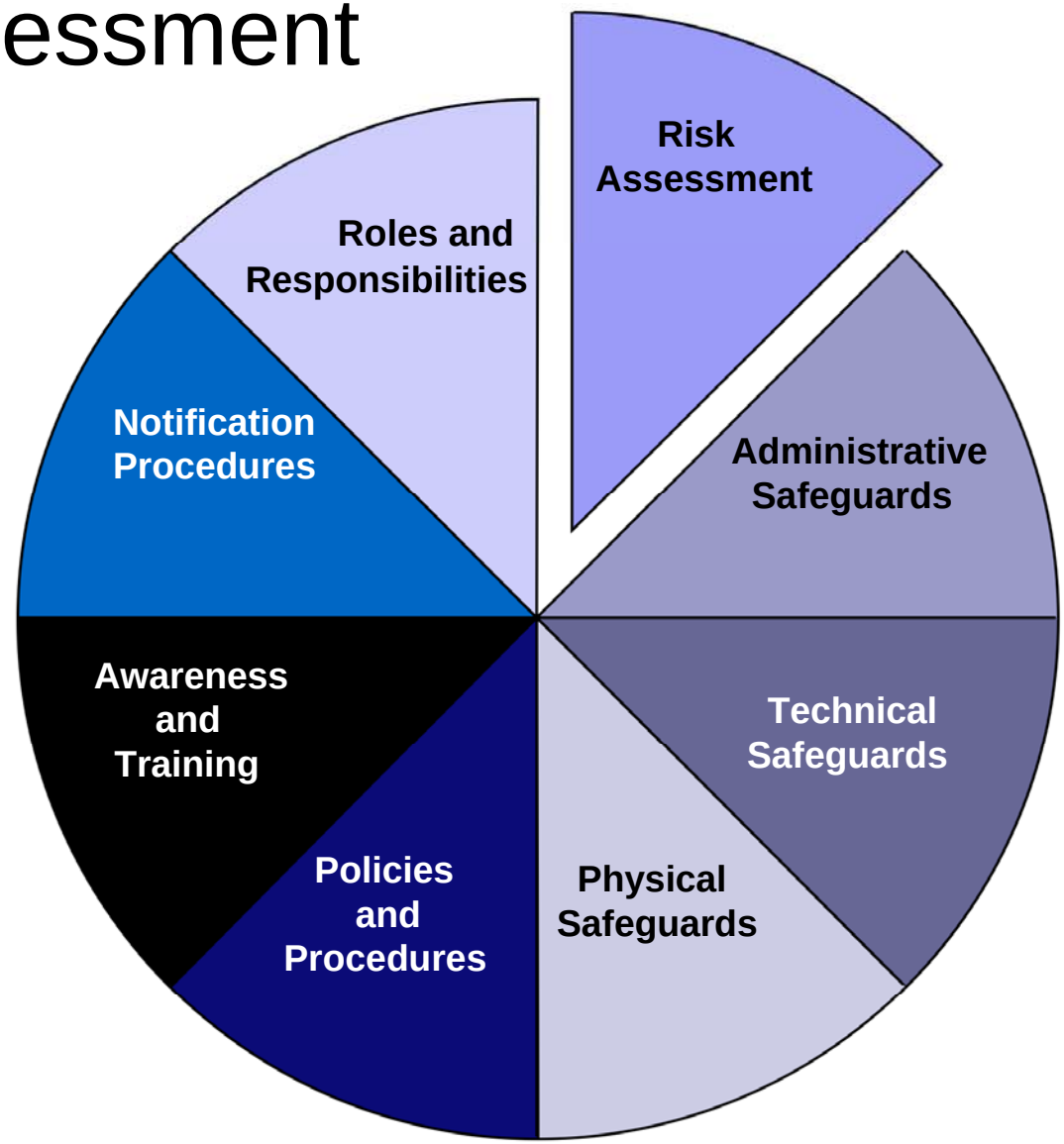


Roles and Responsibilities

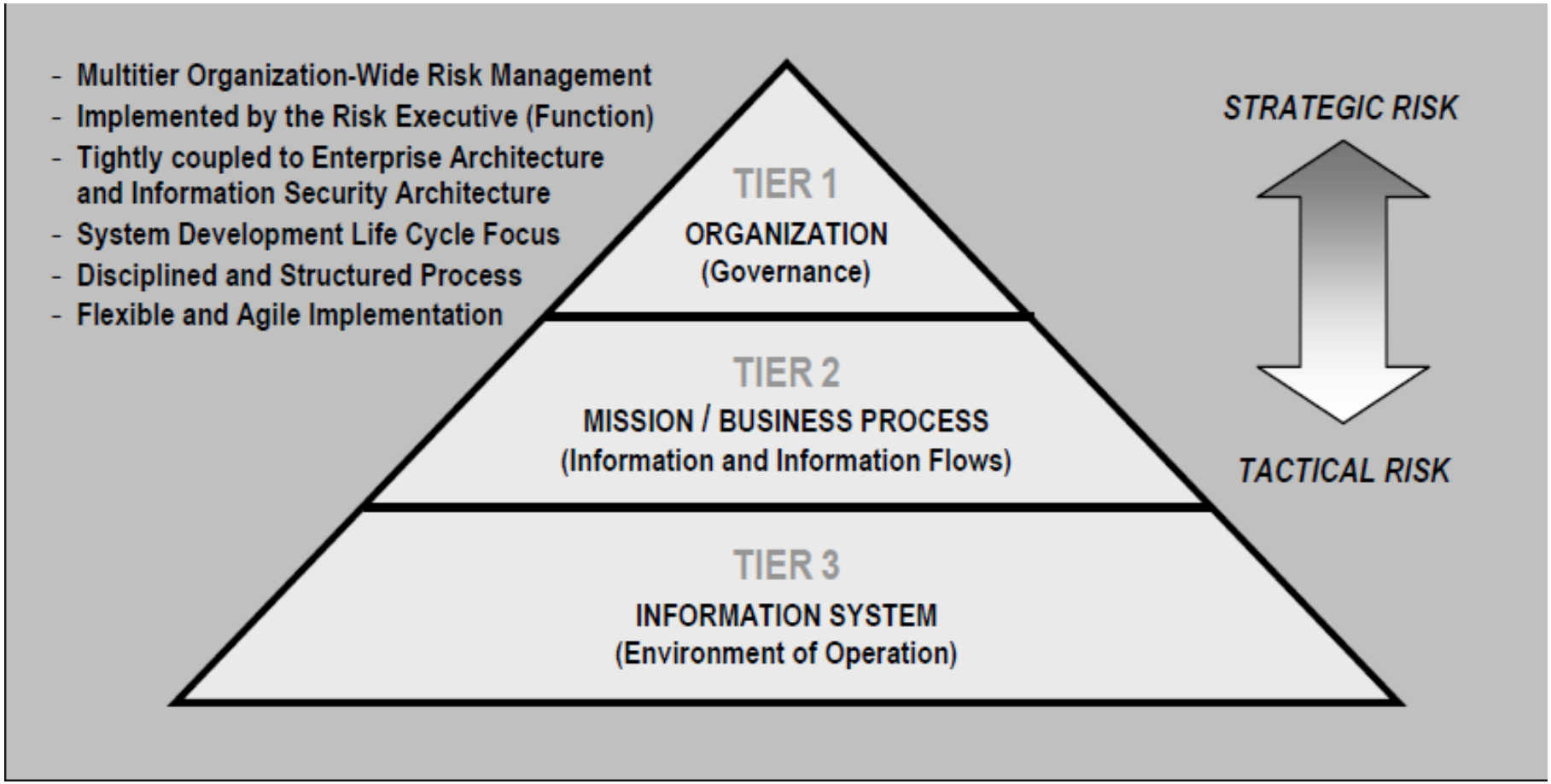
Examples of identified roles include:

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

Risk Assessment

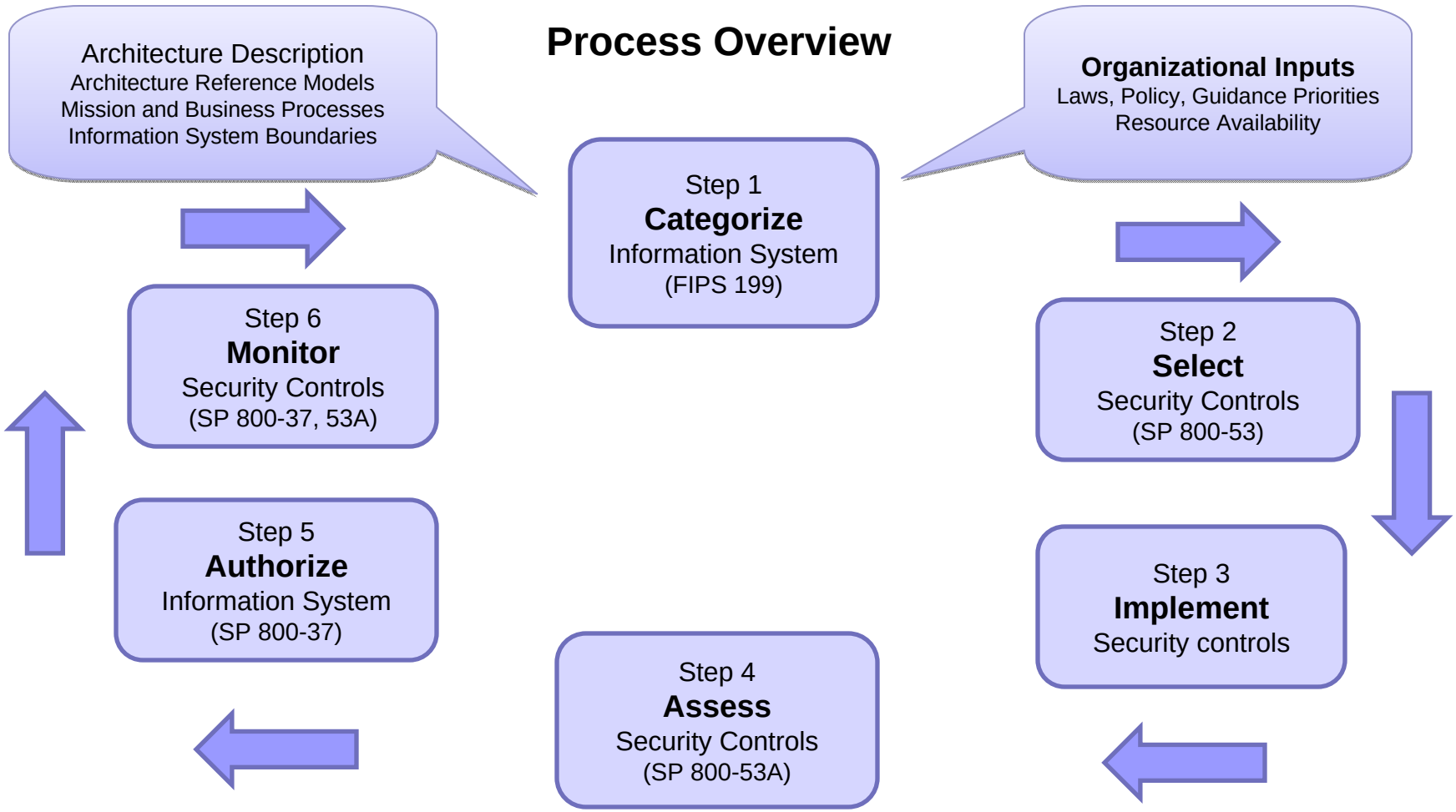


Integrated Organization-wide Risk Management



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

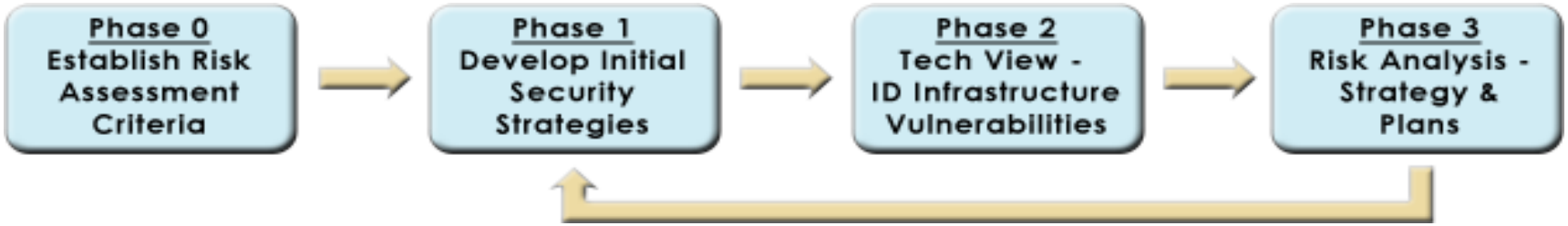
FISMA Risk Management Framework



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

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

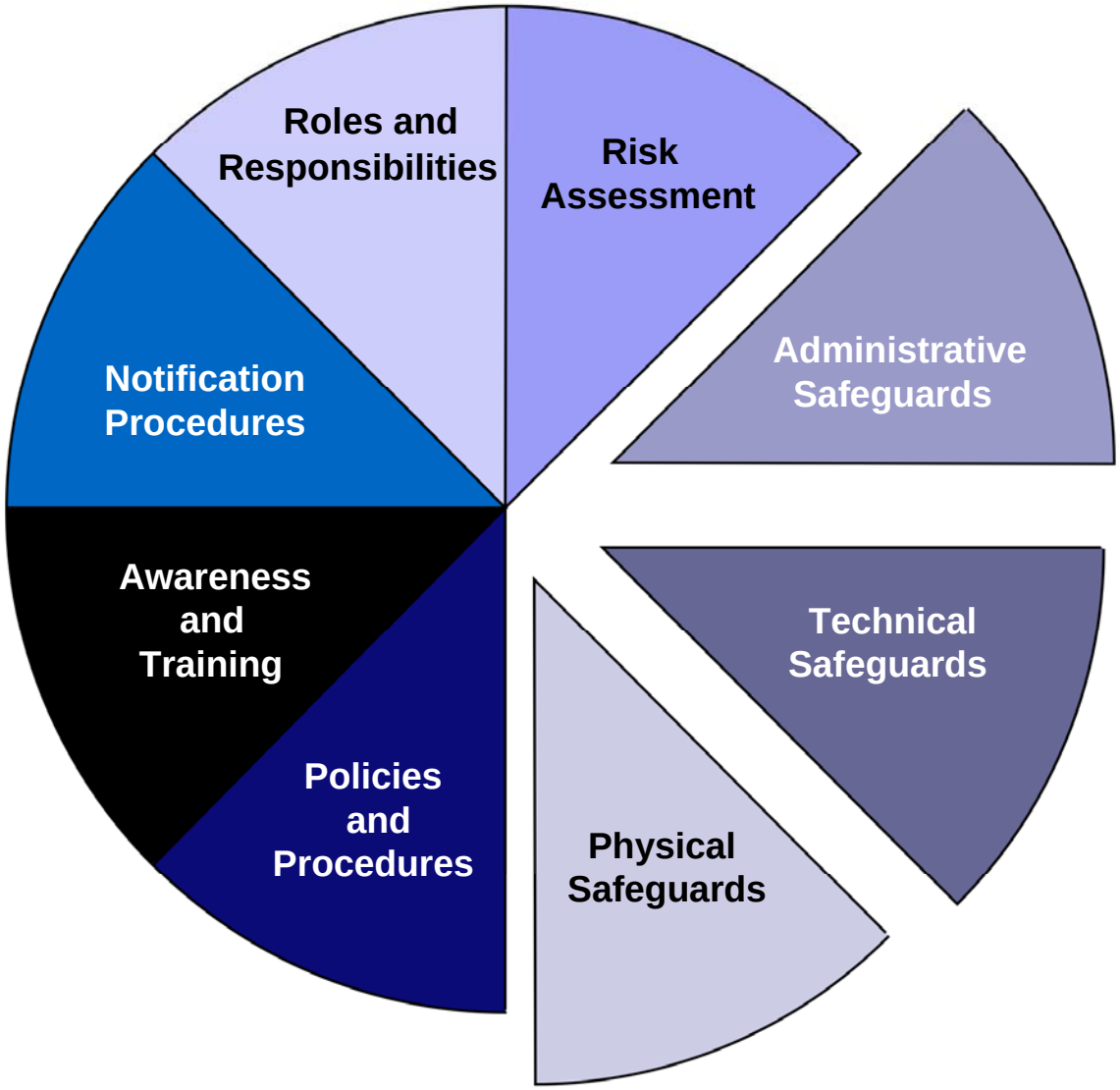
EDUCAUSE/Internet2 Higher Education Security Council



- 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: EDUCUASE/Internet2 Higher Education Information Security Council: Risk Assessment Framework.
Site known good April 2010.

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

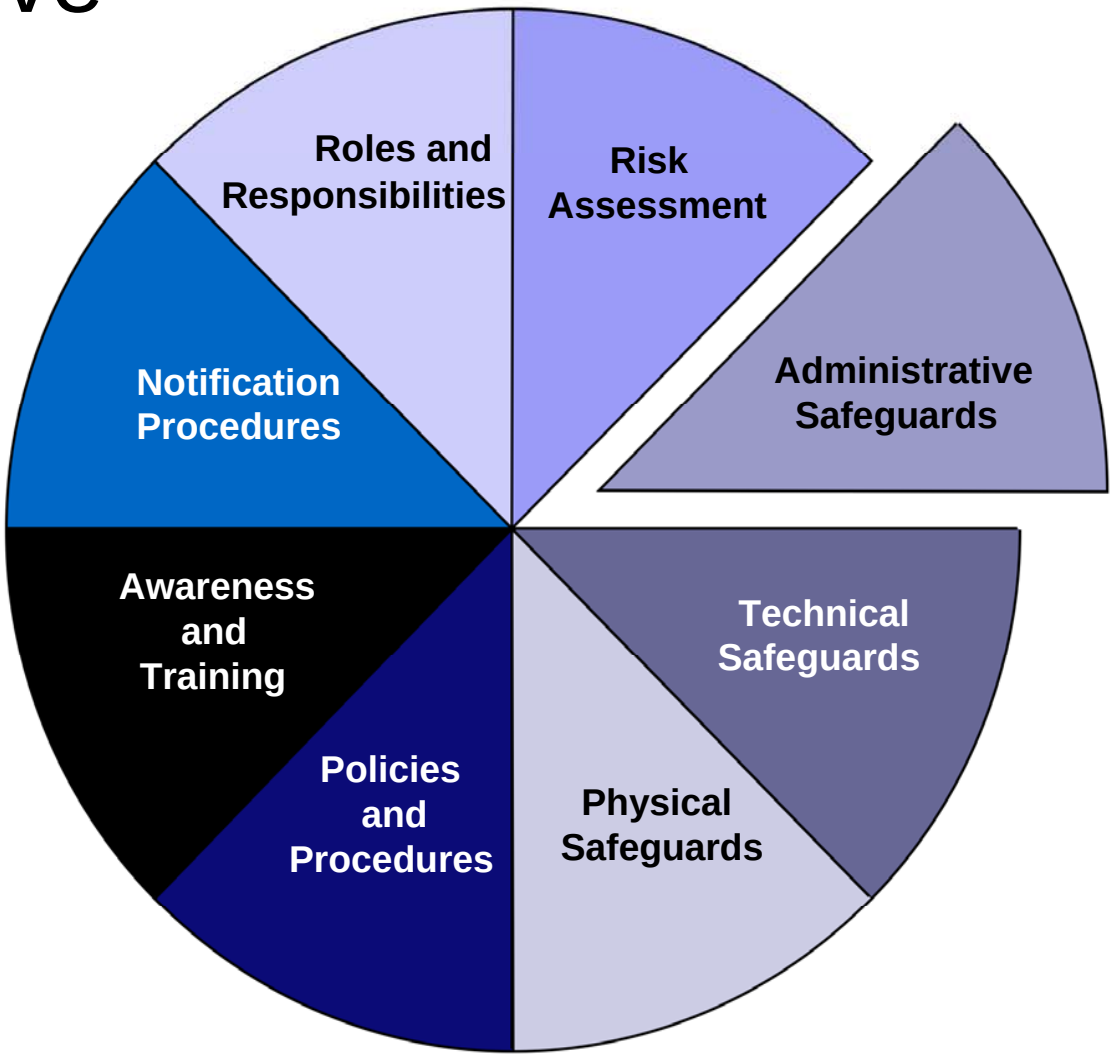
Adapted from a presentation by David C. Smith, UISO, Georgetown University 2008

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

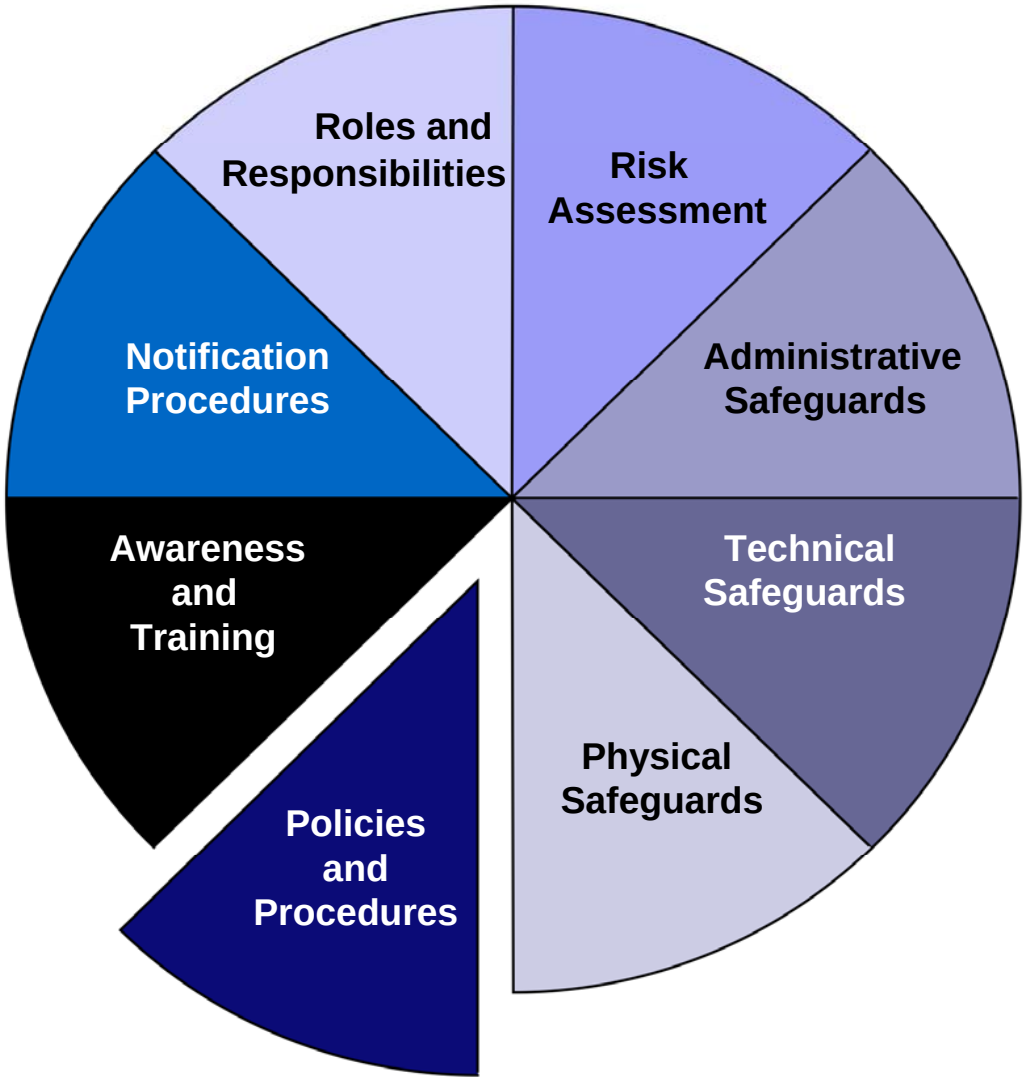
- Compliance and Legal Issues
- ***Policies and Procedures***
- ***Awareness and Training***
- ***Risk Assessment and Management*** *(previous section)*
- Continuity of operations (discussed later)

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.

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.

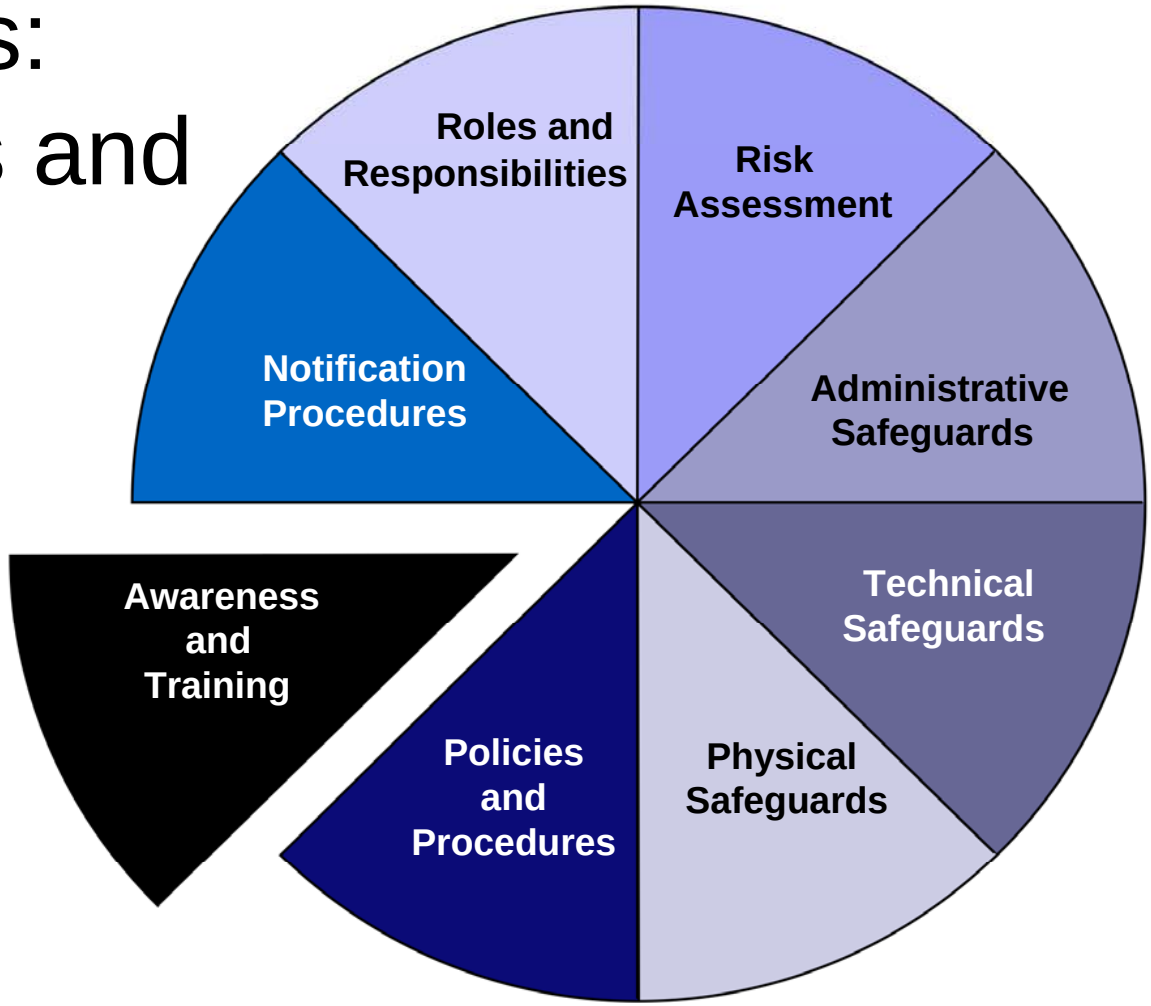
More Example Policies

- 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)

Remember: this is facility information, not agency information.

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

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

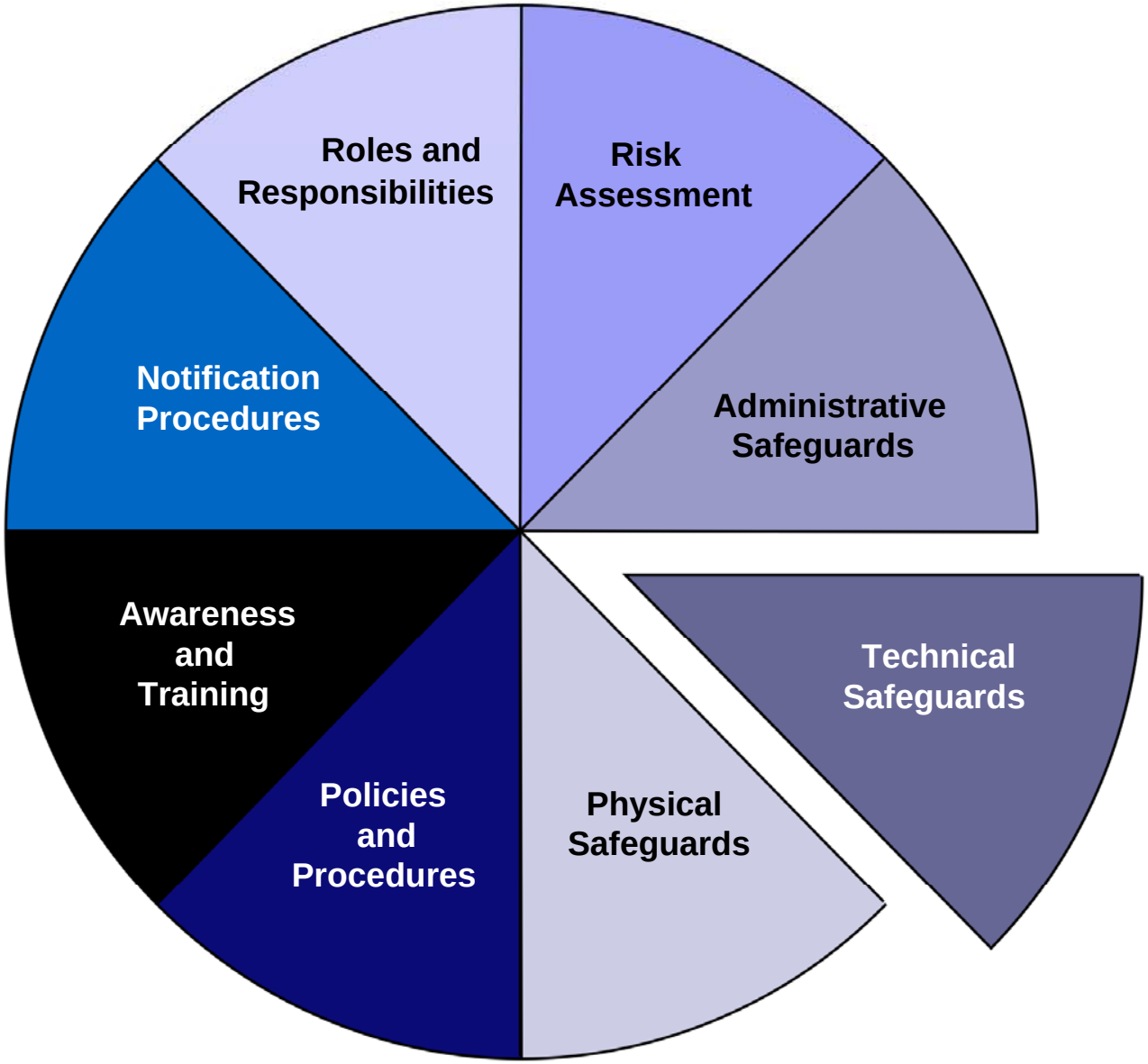
- All IT professionals have a professional responsibility to keep *themselves* current on cybersecurity

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 106,000+ hits on security training!

Technical Safeguards



Technical Safeguards
Examples

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

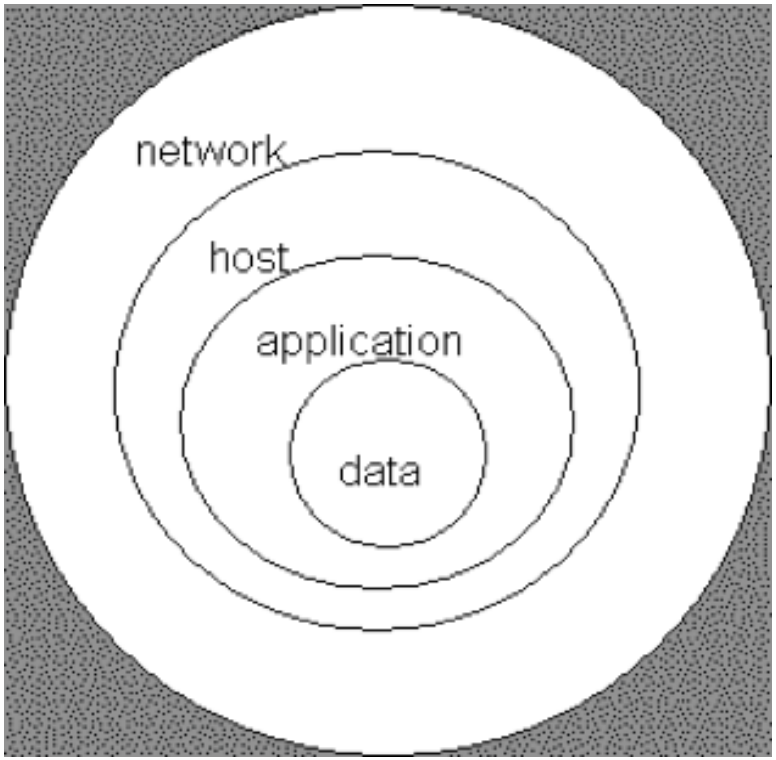
Technical Safeguards
Access Management and Oversight

- 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

Technical Safeguards

Security Architecture & Telecom and Network Security

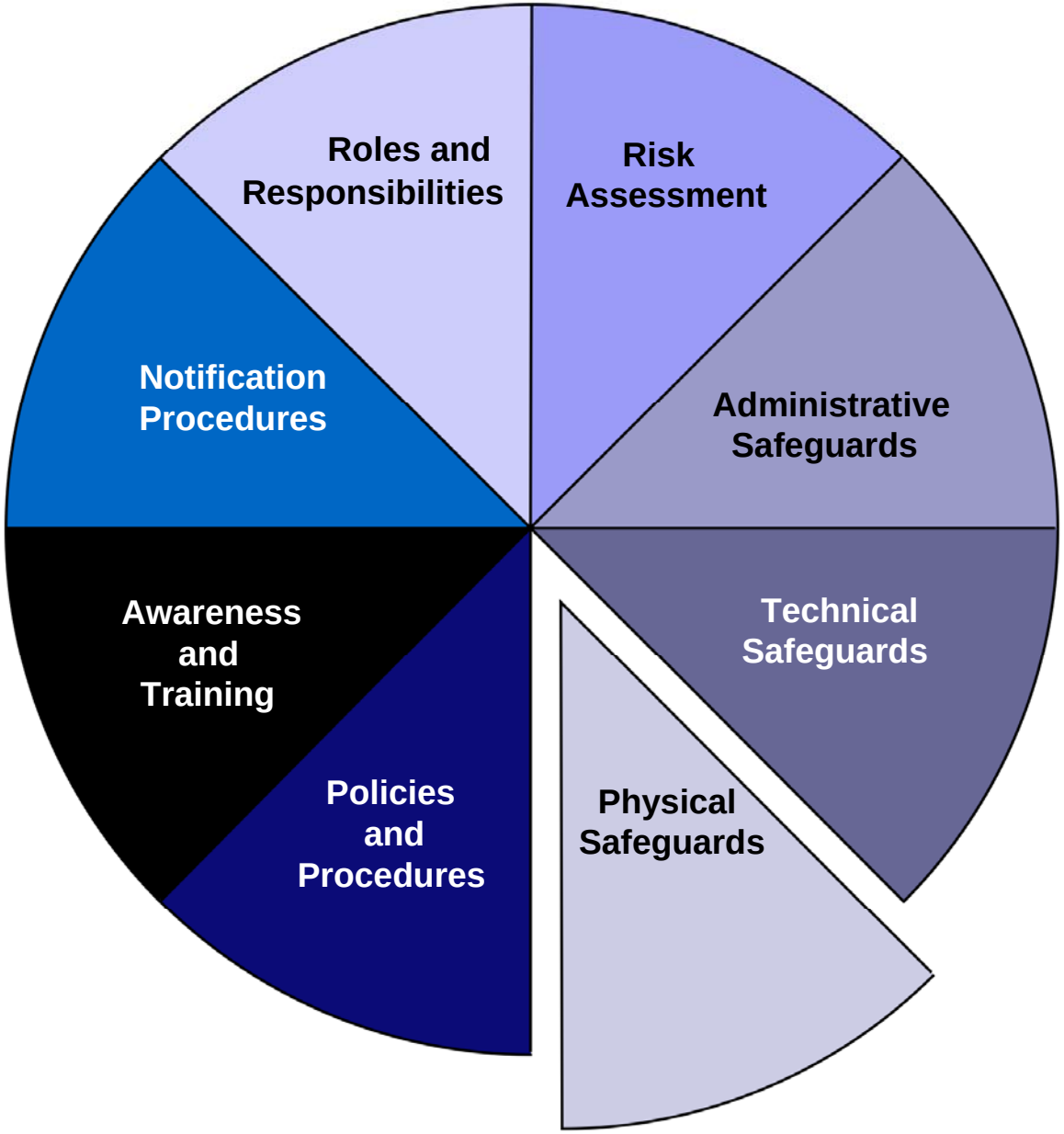
- **Principle of Defense in Depth:** There are multiple safeguards in place so that if one fails, another will continue to provide protection.



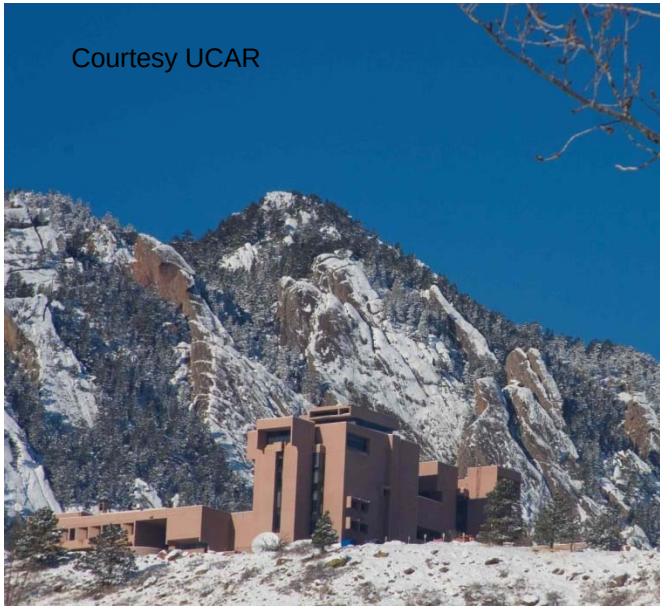
Simple DiD Model*

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

Physical Safeguards



Physical Safeguards: Facilities Vary



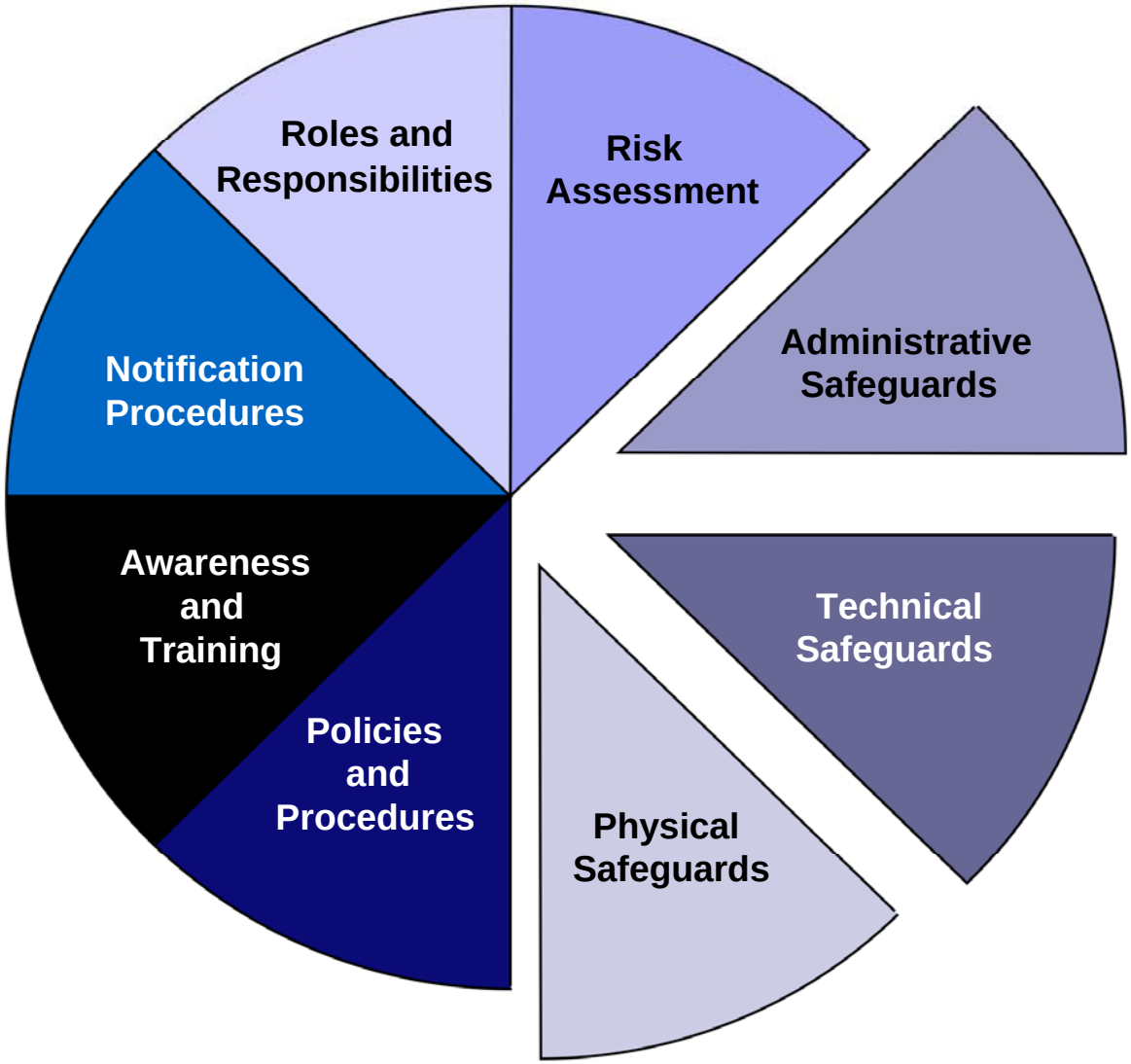
ALMA
ATACAMA LARGE MILLIMETER ARRAY

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

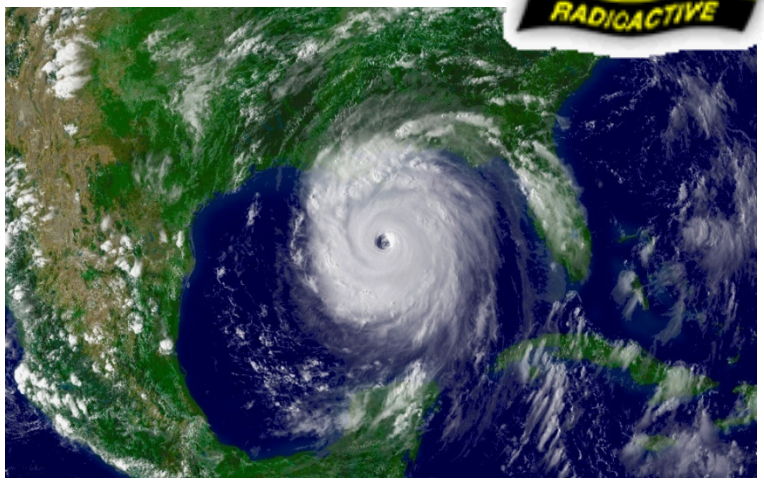
It's all about risk mitigation that is appropriate for the facility.

Administrative, Technical and Physical Safeguards (revisited)

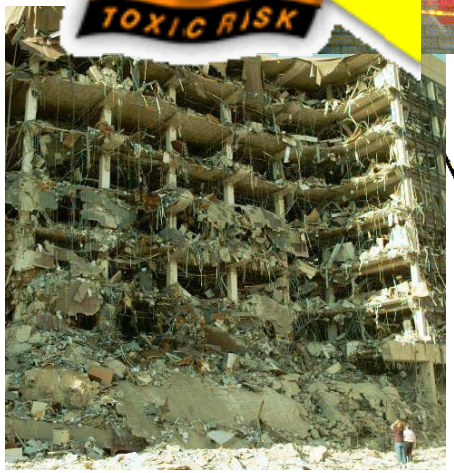


Administrative, Technical and Physical

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



Hurricane Katrina 2005



Oklahoma City 1995

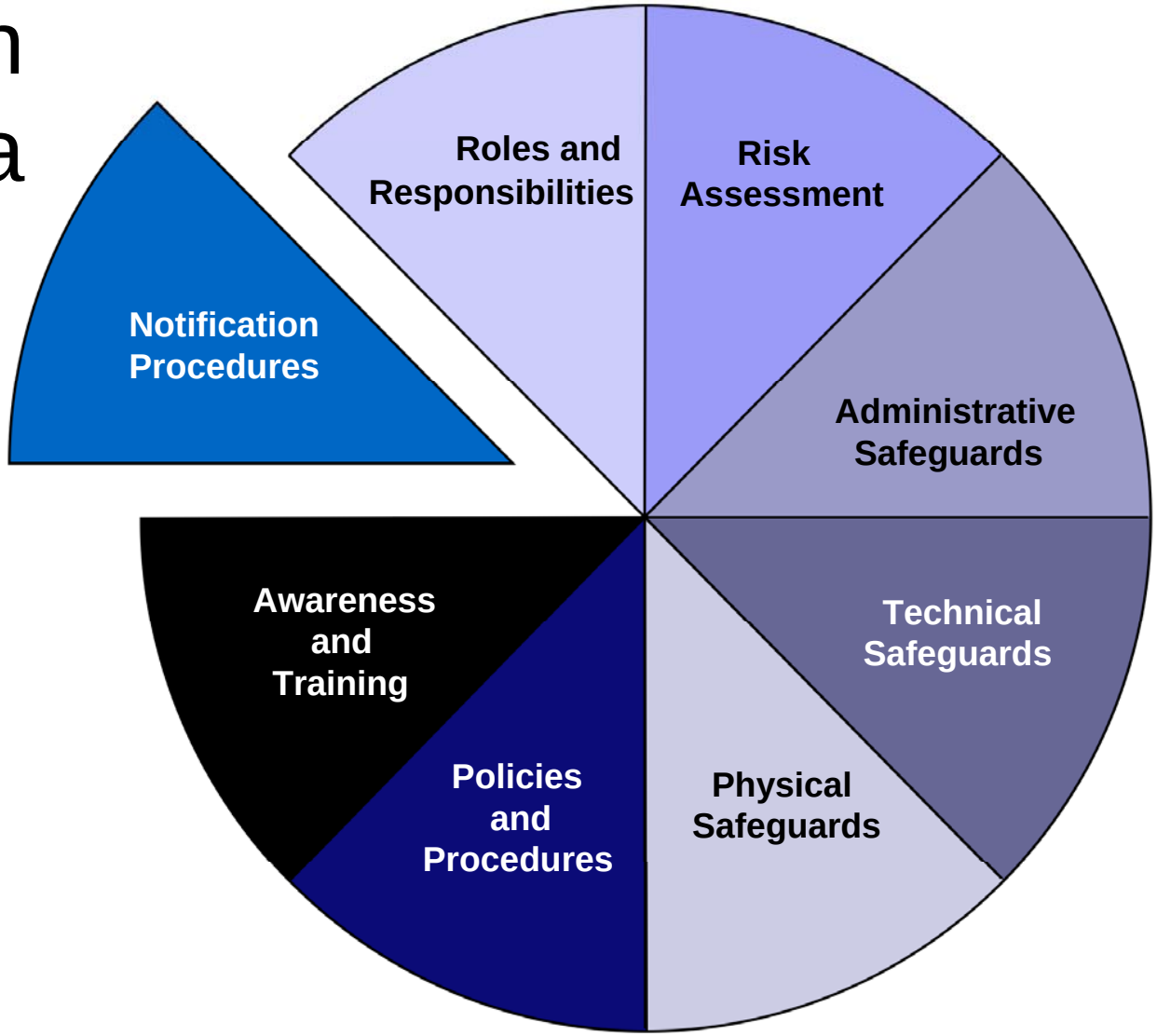
Technical, Administrative and Physical

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/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

When to report to NSF…

If…

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

Or, if there is

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

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

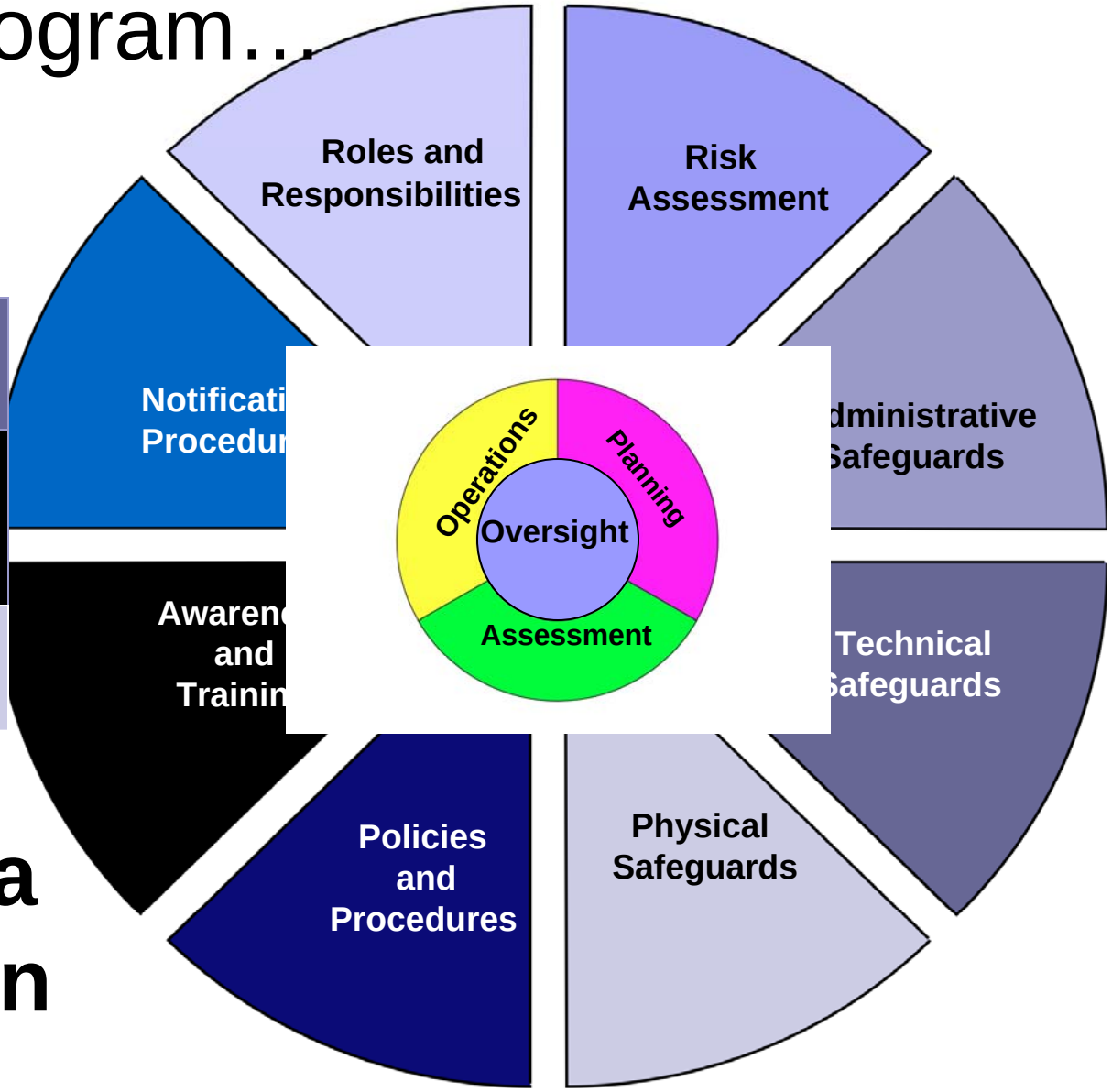
- Some will want to hear from the PI
- Others may want to hear from the cyber-security officer

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

Access Management and Oversight Initiatives

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

References

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

References

- "Best Practices in Cybersecurity That Might be Useful for to NSF Large Facilities"
  - TeraGrid knowledge base. See:
    - https://portal.teragrid.org/kb?p_p_id=knowledgebase_WAR_knowledgebaseportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_knowledgebase_WAR_knowledgebaseportlet_docid=aypt#tabletop
    - http://tinyurl.com/yauxcvv
  - EDUCAUSE/Internet2. See:
    - https://wiki.internet2.edu/confluence/display/itsg2/Home

“Cyber Espionage Efforts By Well Resourced Organizations Looking To Extract Large Amounts Of Data - Particularly Using Targeted Phishing”

One of the biggest security stories of 2007 was disclosure in Congressional hearings and by senior DoD officials of ***massive penetration of federal agencies and defense contractors and theft of terabytes of data by the Chinese and other nation states.*** In 2008, despite intense scrutiny, these nation-state attacks will expand; more targets and increased sophistication will mean many successes for attackers. Economic espionage will be increasingly common as nation-states use cyber theft of data to gain economic advantage in multinational deals. The attack of choice involves targeted spear phishing with attachments, using well-researched social engineering methods to make the victim believe that an attachment comes from a trusted source, and using [then] newly discovered Microsoft Office vulnerabilities and hiding techniques to circumvent virus checking.

Top Ten Cyber Security Menaces for 2008,
SANS Institute. http://www.sans.org/2008menaces/

Photos and Graphics Courtesy:

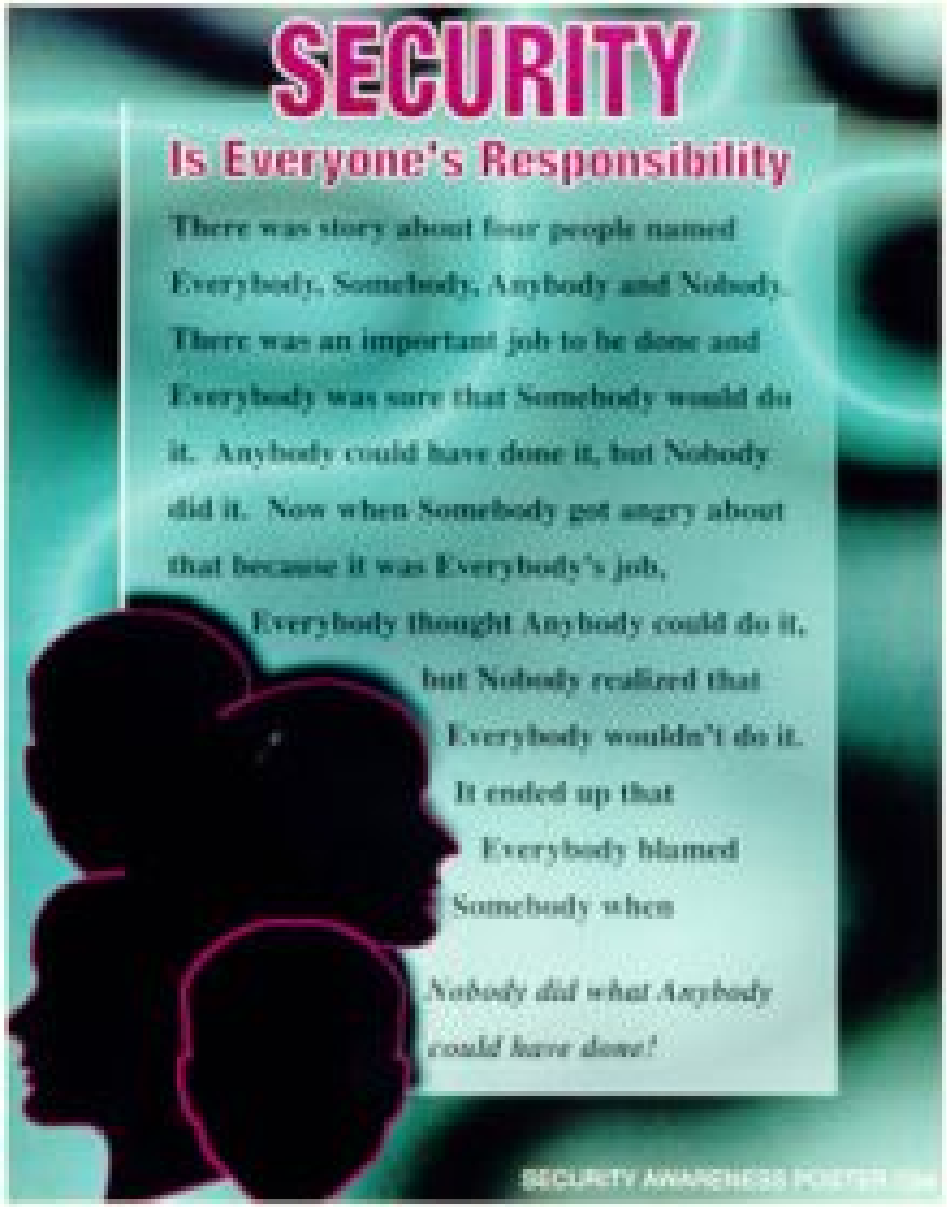
- EDUCAUSE and Internet2
- NSF and the Large Facilities
- Wikipedia (public domain or permission to use)
- Oklahoma City: oklahomacitybombing.com
- US Department of Commerce

A word about Wikipedia…

CNET says about Wikipedia*:

- "The good: Wikipedia is free and easy to access; full of arcane information; evolving constantly; multiple languages; enormous collection of articles and media; works in any browser.
- "The bad: Vulnerable to vandalism; some Wikipedia sections still under construction; lack of kids' resources; uninspiring interface; demands Web access for most 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 their 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 March 25, 2009



* 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