

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

Ardoth Hassler
Senior IT Advisor
National Science Foundation

Large Facilities Workshop
Boulder, Colorado
April 7, 2008

Introduction

- Community has asked for guidance on cybersecurity
- NSF-sponsored the first CyberSecurity Summit after a major incident affected multiple large facilities
 - Opportunity to gather PIs and security professionals with program directors
 - 4th Summit meeting is May 7-8 in Arlington, VA
- Reports from the Summits have resulted in
 - Closer workings within the community
 - NSF developing language about cybersecurity for the Cooperative Agreements
- This is a work in progress.
- Your feedback is most welcome.

Examples of NSF Large Facilities



A Work in Progress

What's at stake...

- Lost productivity
 - TeraGrid supports around \$271M in research annually*
- Expensive incident response and notification
 - Laptop stolen from public west-coast research university 2005:
 - \$750K out of pocket
 - Research server breach at private east-coast research university 2006:
 - \$200K out of pocket
 - Cost of TeraGrid's Stakkato Incident in 2003-2004: not calculated
- 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?

* Information provided by John Towns, NCSA

First Principles

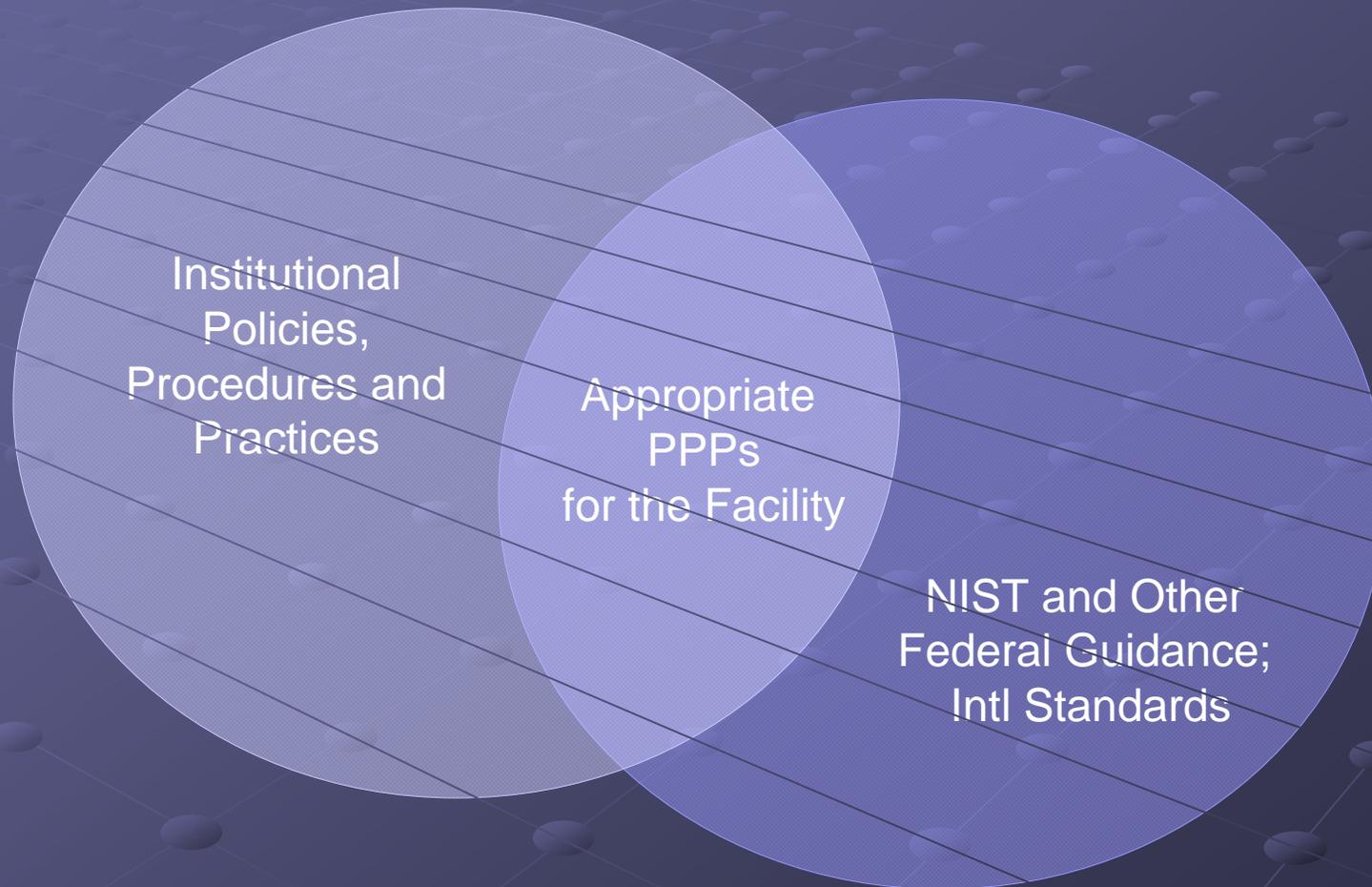
- Information security is a journey not a destination.
 - The challenges keep coming. Security programs evolve and improve.
- Security budgets are limited
 - Priorities must be established; tradeoffs must be made.
- Good IT practices foster good security
 - Good IT security reflects good IT practices.
- 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



A Work in Progress

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.

A Work in Progress

Sources for Reference

(Links at end of presentation)

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

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 28, 2008

Background

A Work in Progress

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

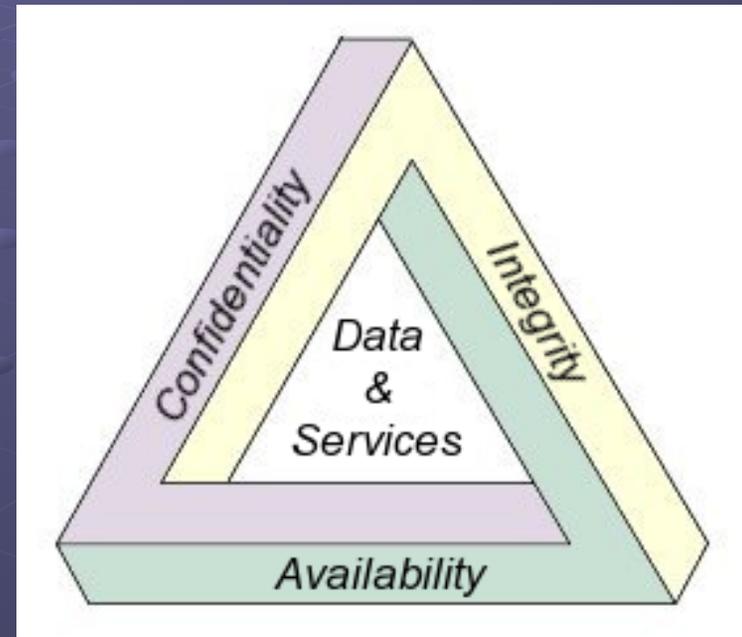
- Security for all IT systems under the award, including equipment and information, is the Awardee's responsibility.
- The Awardee is required to provide a summary of its IT Security program:
 - Include roles and responsibilities, risk assessment, technical safeguards, administrative safeguards; physical safeguards; policies and procedures; awareness and training; notification procedures.
 - Include 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.

Security Fundamentals

- Fundamental Principles of Security are:
 - Confidentiality
 - Integrity
 - Availability
- 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

Principles of Information Security

The three main principles of a security program to ensure access and use of data and services are *confidentiality*, *integrity* and *availability*. These are known as the “CIA Triad” (or sometimes the “AIC Triad” for availability, integrity or confidentiality). The level of security required for a facility to achieve these principles may vary as security goals and requirements may 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 March 18, 2008. Diagram is in the public domain.

Information Security is a Continuous Process

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

Execute

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

Assess

**Security is a
continuous
process of
evaluation
and
monitoring**

Implement

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

Plan

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

Design

- Policy
- Standards
- Enterprise Architecture
- Configuration Standards

A Work in Progress



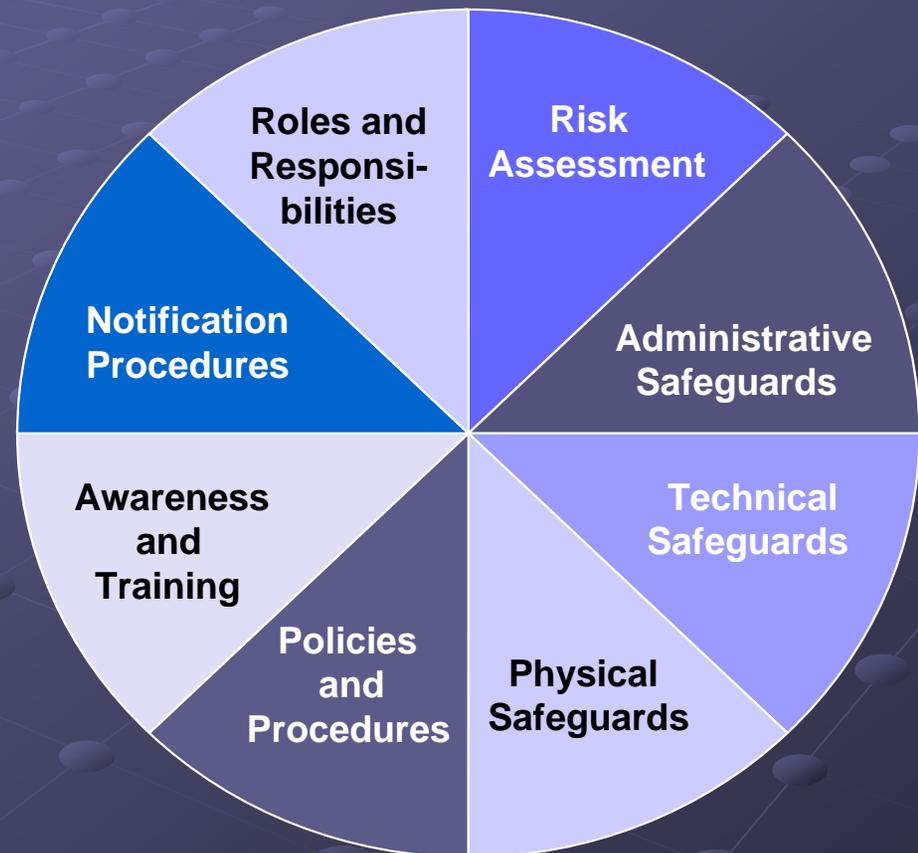
Cyberinfrastructure
Best Practices
that
Large Facilities May Find
Useful

A Work in Progress

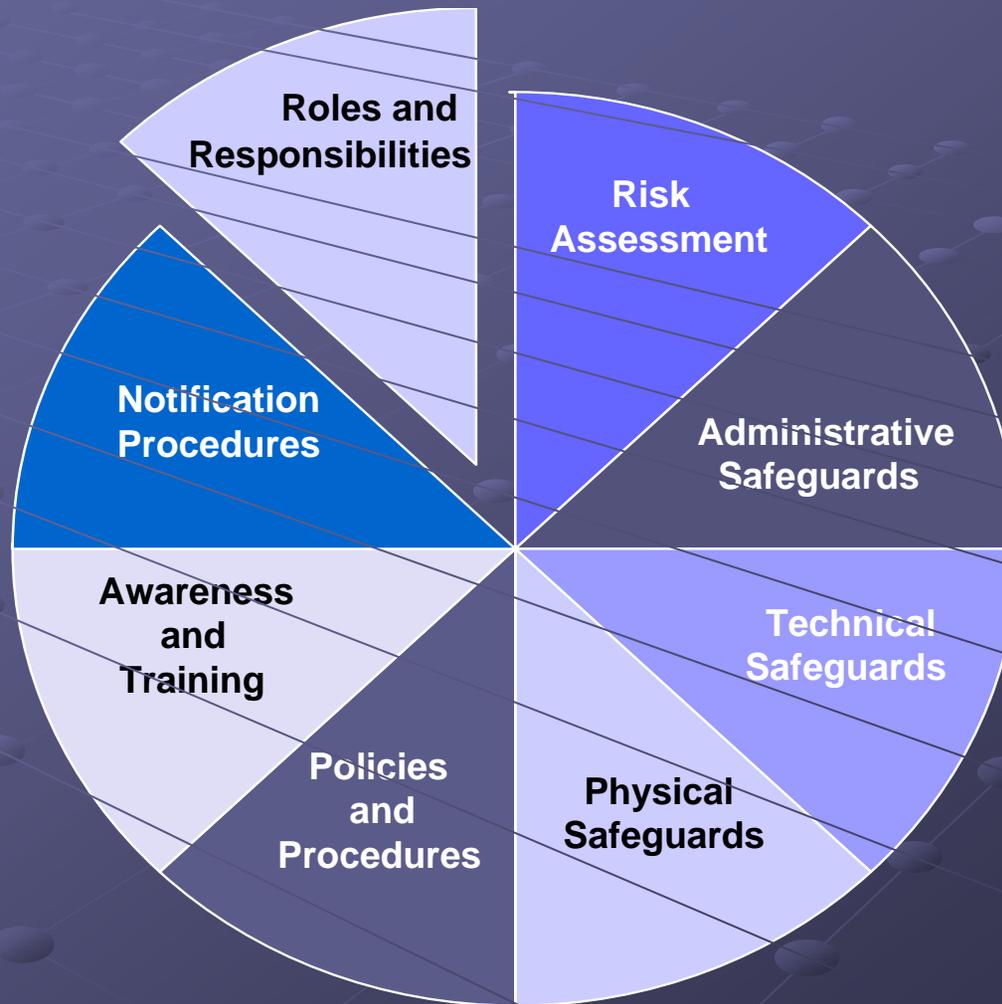
Awardee Responsibilities under the Cooperative Agreement

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



A Work in Progress

Roles and Responsibilities Principles

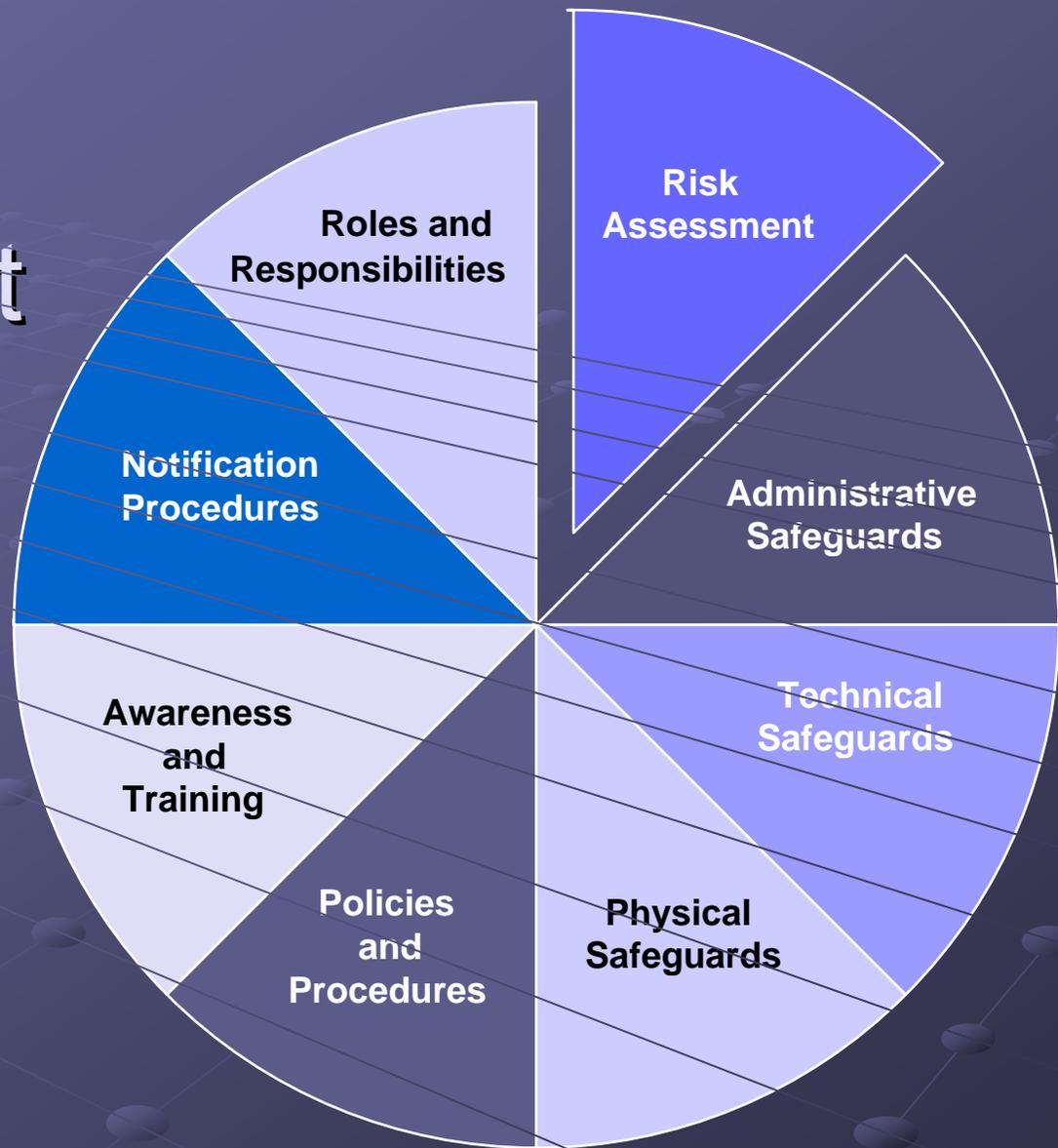
- Cybersecurity is not just a technical or “computer geek” responsibility
- Everyone in the facility has a responsibility for cybersecurity

Roles and Responsibilities

Examples of identified roles include:

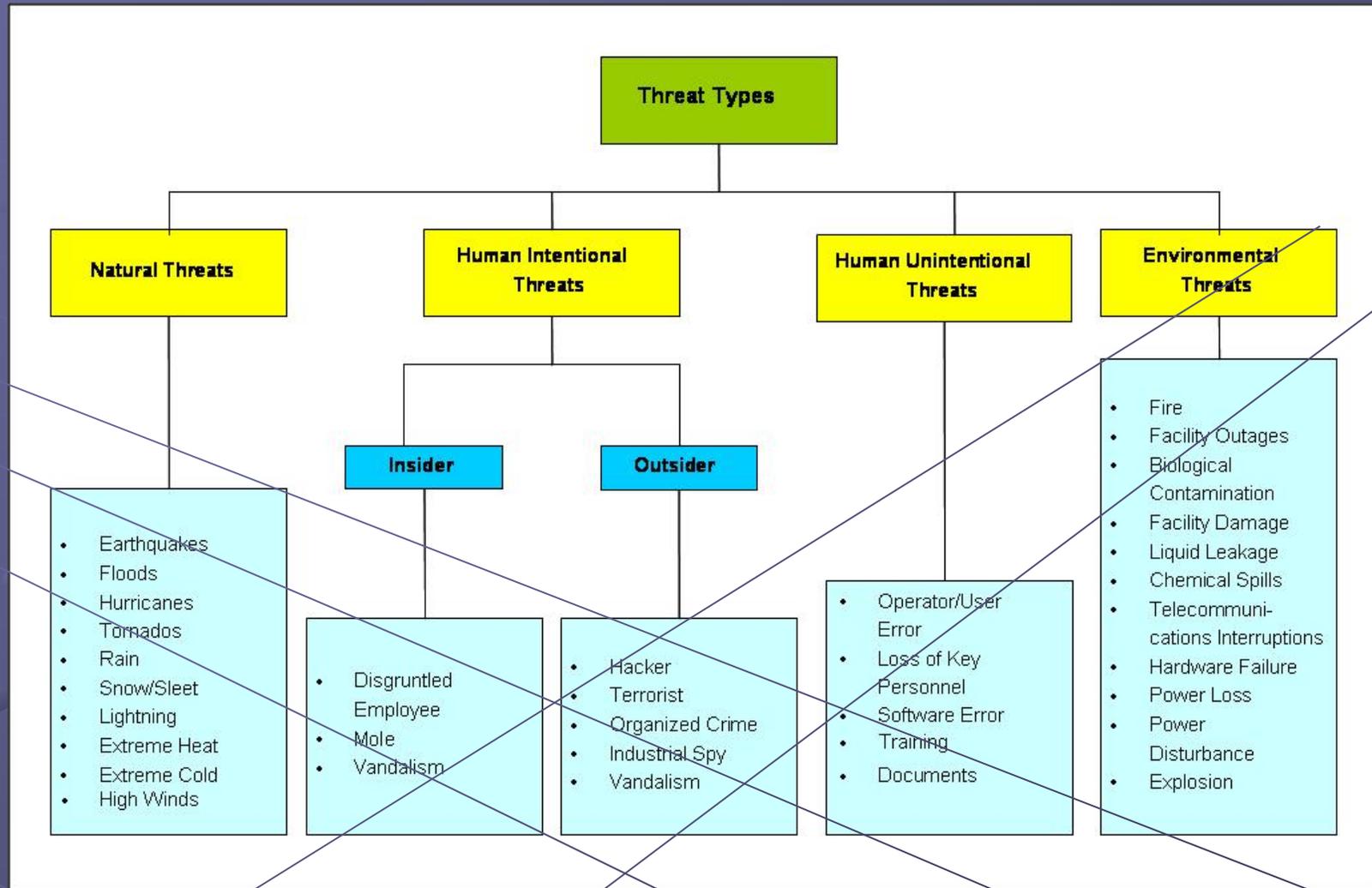
- Upper Management
- System and Network Administrators
- Information Security Support Staff
- Users
 - Internal
 - External

Risk Assessment



A Work in Progress

Examples of Threat Types

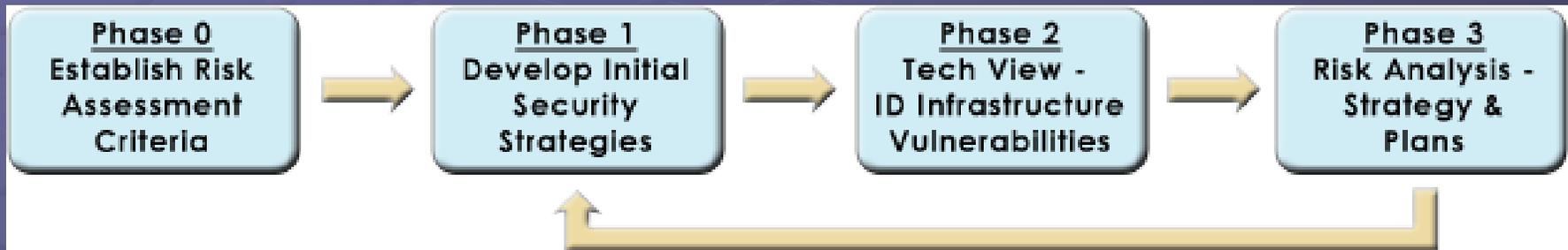


Ref: NIST 800-30 *Risk Guide for Information Technology Systems*

A Work in Progress

A Model for *Risk Assessment* #1:

EDUCAUSE/Internet2 Security Task Force

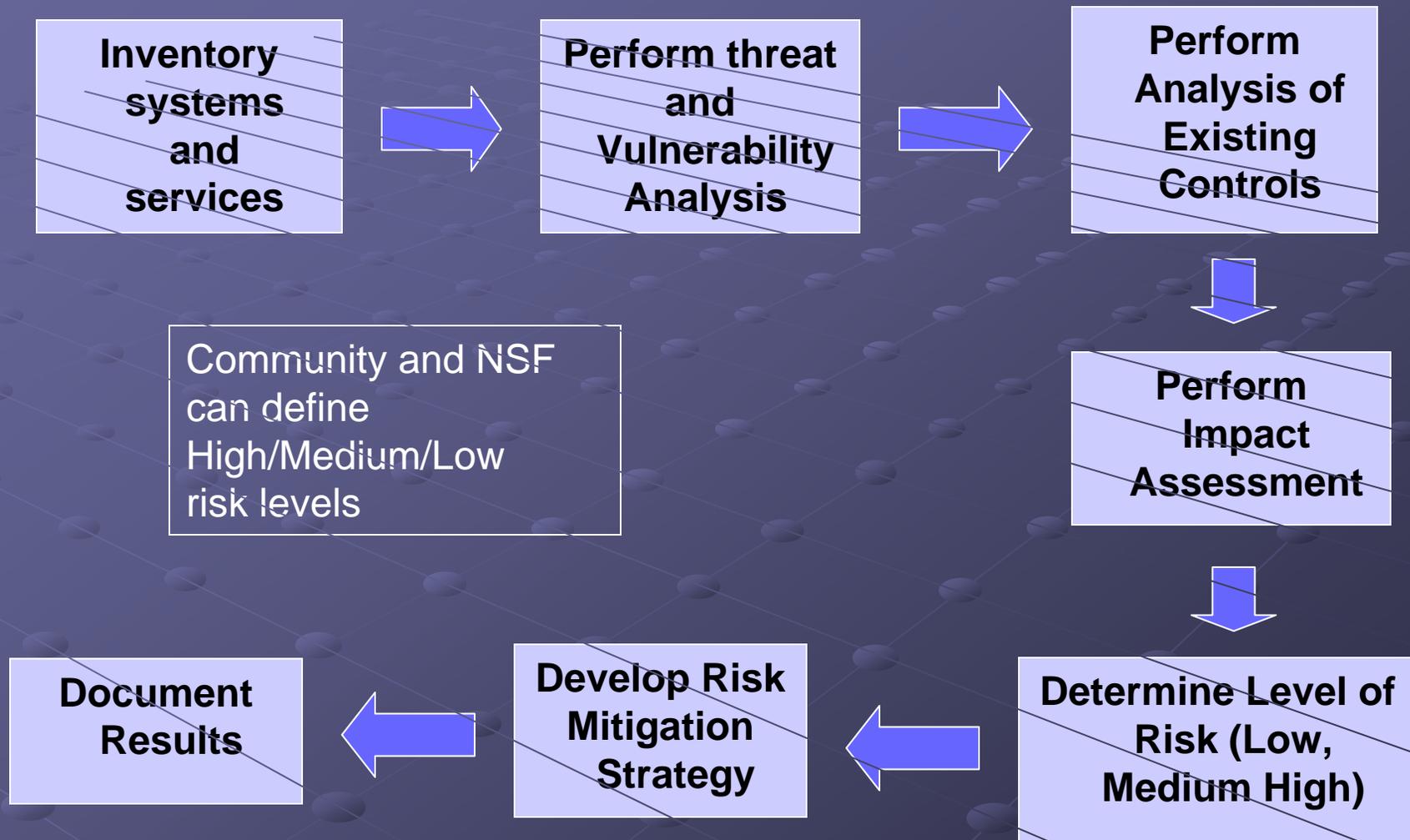


- Phase 0: Establish Risk Assessment Criteria for the Identification and Prioritization of Critical Assets - Asset Classification
- Phase 1: Develop Initial Security Strategies
- Phase 2: Technological View - Identify Infrastructure Vulnerabilities
- Phase 3: Risk Analysis - Develop Security Strategy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

Source: [EDUCAUSE/Internet2 Security Task Force Tools: Risk Assessment Framework](#).
known good 3/18/2008

A Model for *Risk Assessment* #2:

Methodology Adapted from NIST 800-30



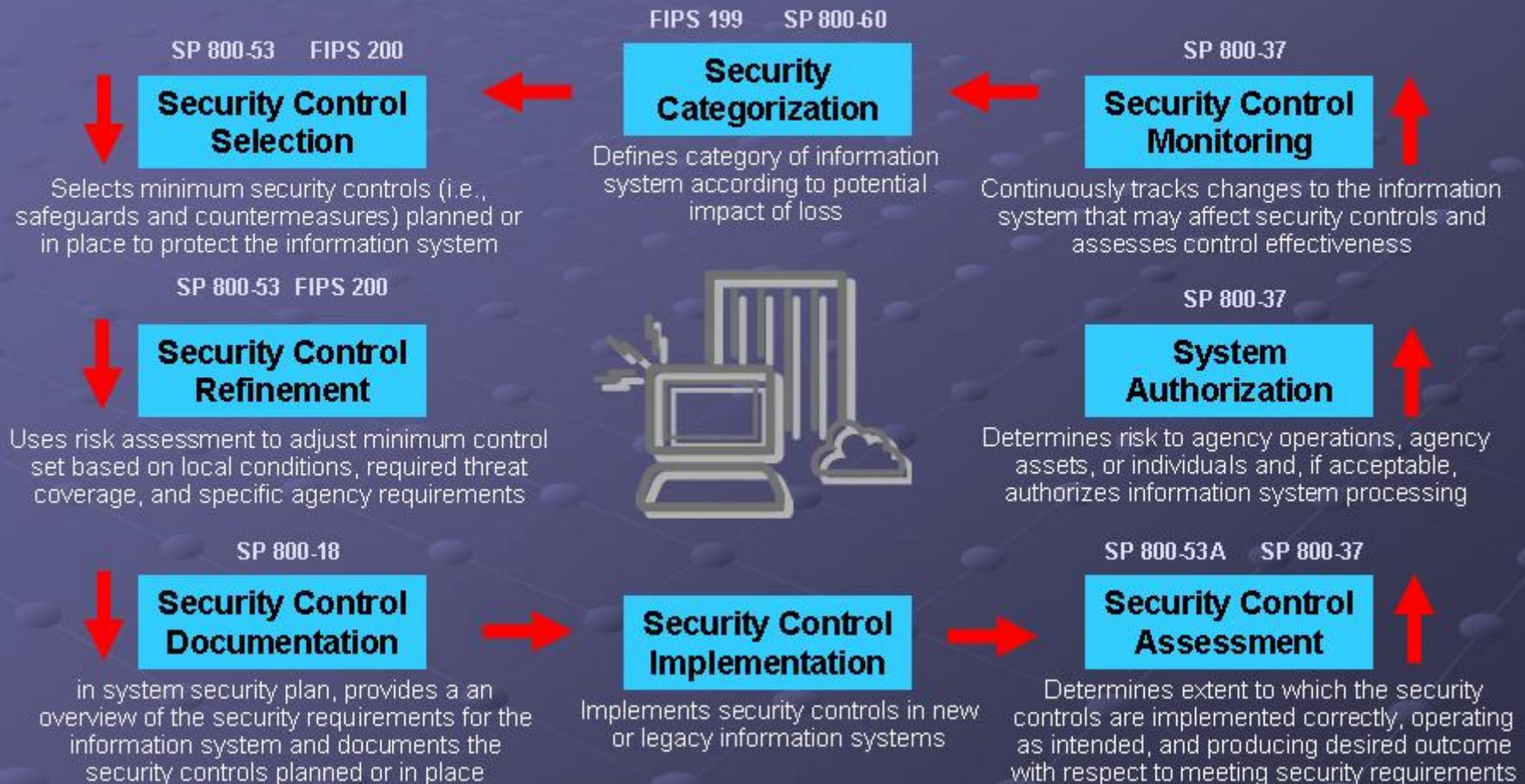
Adapted from NIST 800-30 *Risk Guide for Information Technology Systems*

A Work in Progress

A Model for *Risk Assessment*. #3

FISMA *Risk* Management Framework

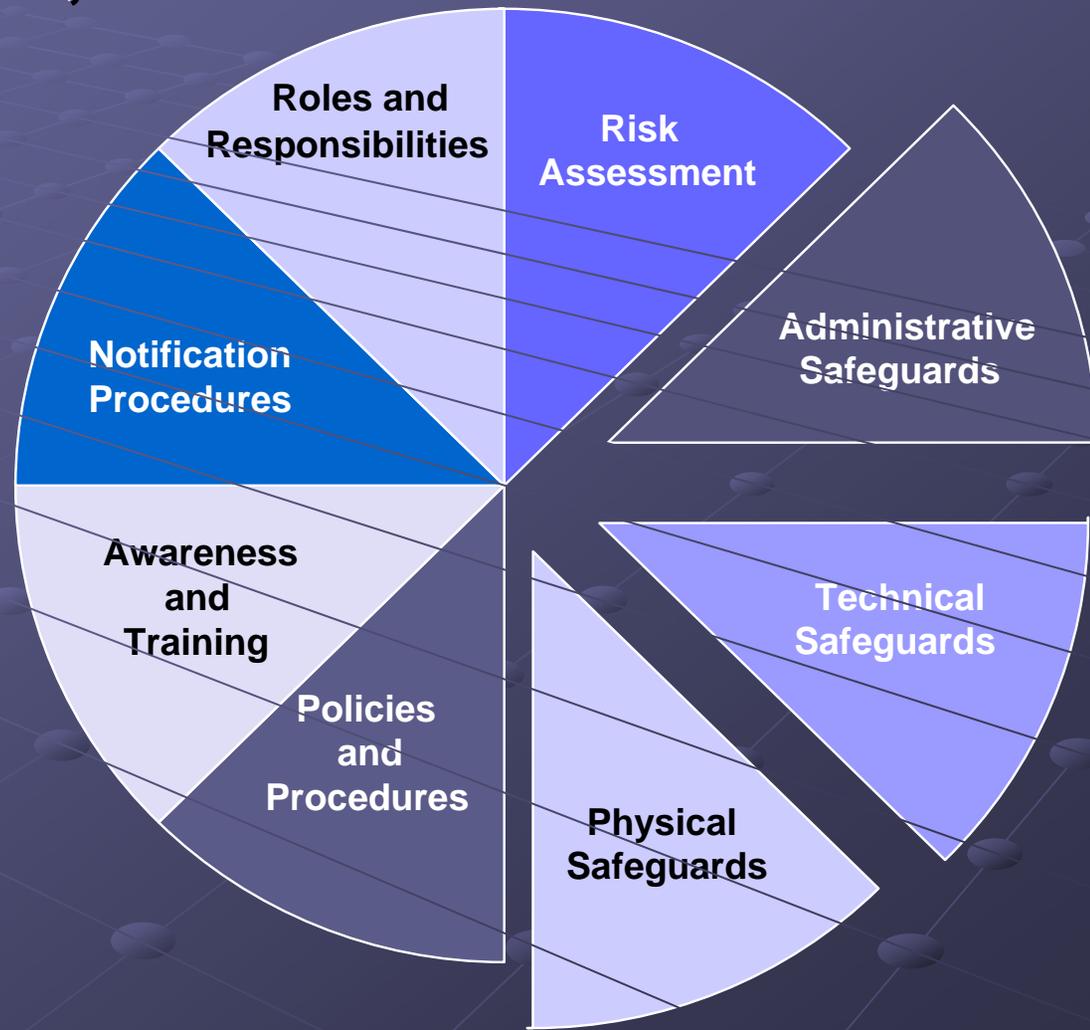
Special Pubs and FIPS are Available for *Guidance*



FIPS – Federal Information Processing Standards Publication
 NIST – National Institute of Standards and Technology
 SP – Special Publication

A work in progress.

Administrative, Technical AND Physical

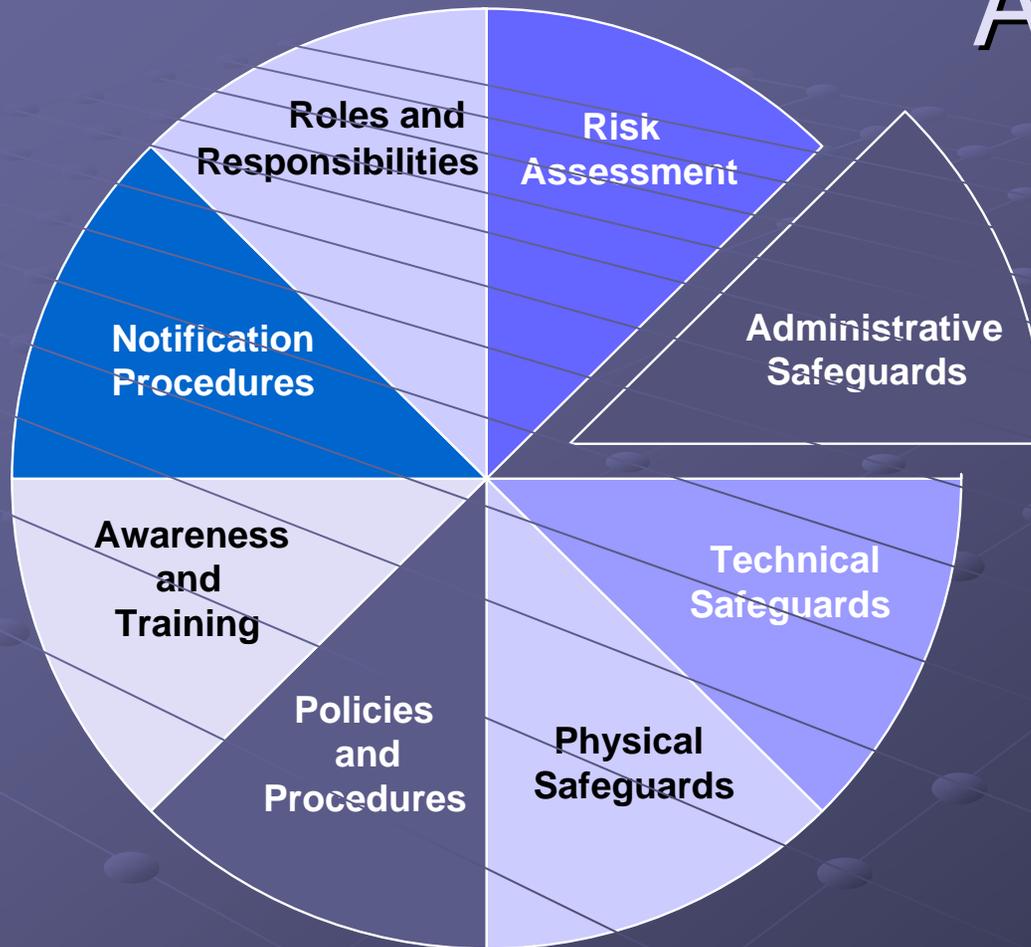


A Work in Progress

Administrative, Technical and Physical Responsibilities: 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



A Work in Progress

Administrative Safeguards

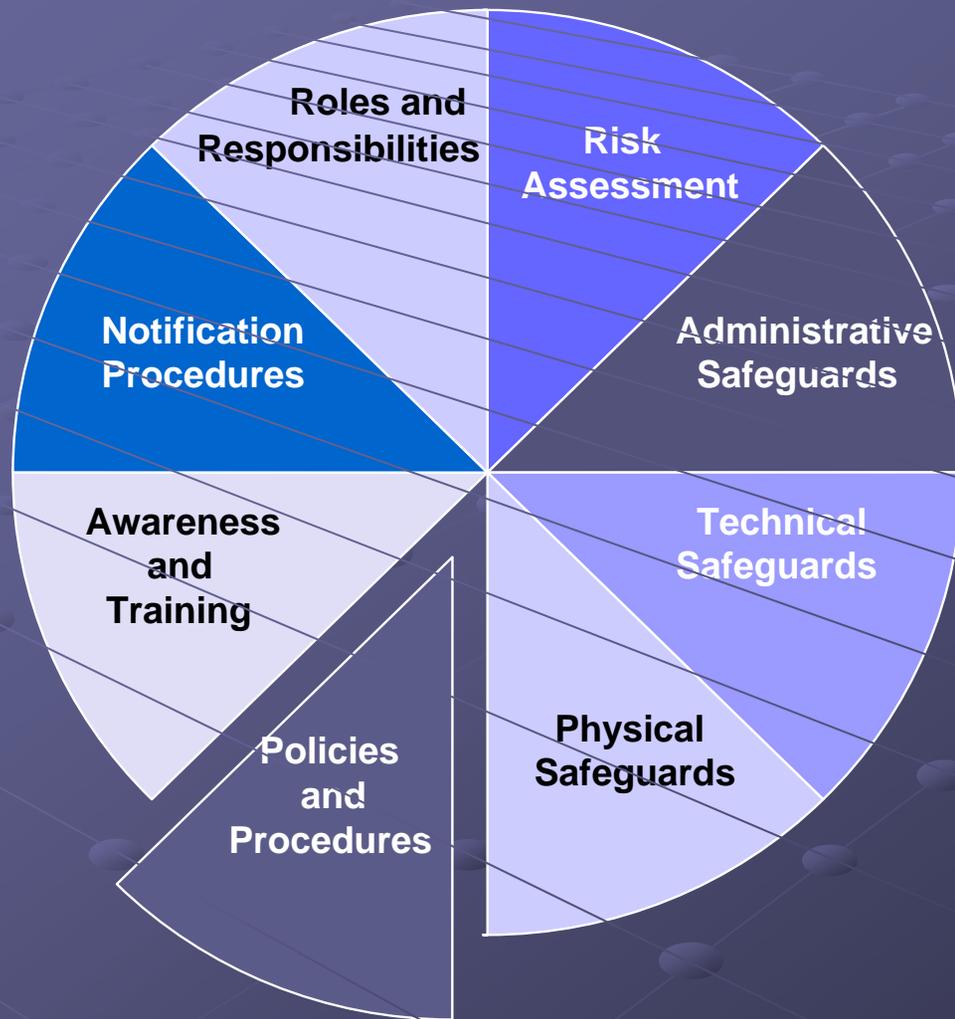
Examples

- 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
 - 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 and don't keep it.

Administrative Safeguards: Written Policies and Procedures



A Work in Progress

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

*Outline taken from EDUCAUSE/Internet2 Security Guide “Security Policies and Procedures”

A Work in Progress

More Example Policies

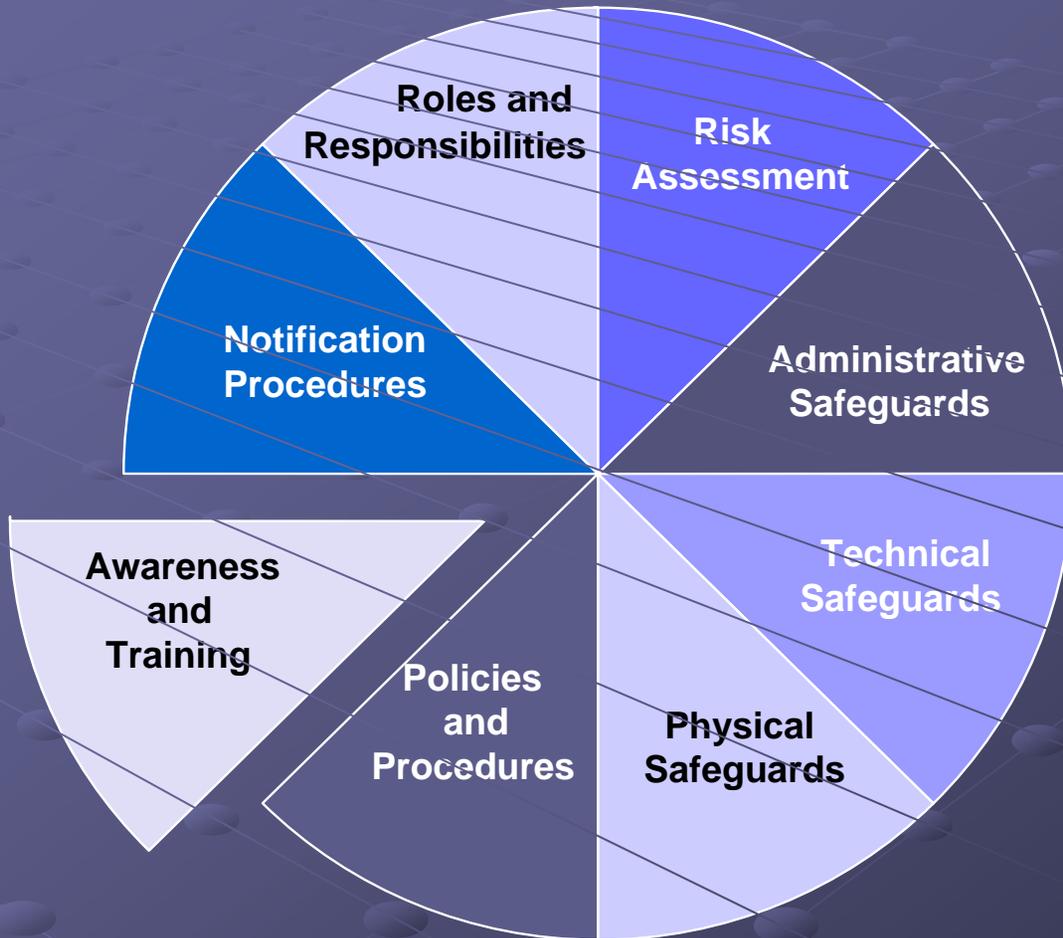
- Responsible/Acceptable Use Policy. AUPs typically define what uses are permitted and what are not. (No personal commercial gain, no illegal behavior, follow export control mandates, etc.)
- “Agreement of Use” or “Rules of Behavior.” Facilities need to make sure that:
 - only authorized users are using resources and know how they are using them;
 - users are accountable for the actions of others they may designate as users; and,
 - 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

A Work in Progress

Administrative Safeguards: Awareness and Training



A Work in Progress

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

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

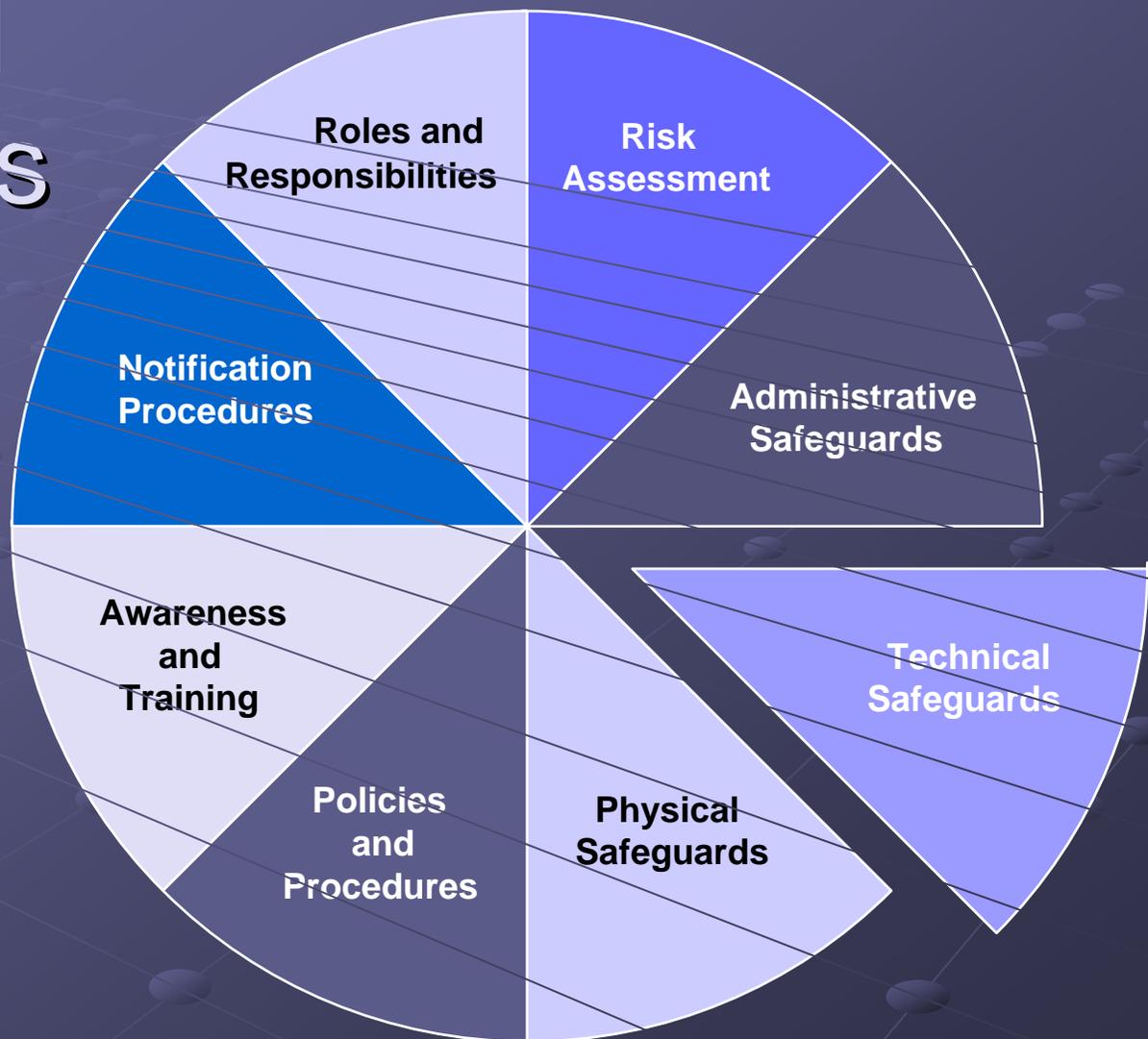
Security Awareness Training Resources

● 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 121,000+ hits on security training!

Technical Safeguards



A Work in Progress

Technical Responsibilities

Examples

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

Technical Responsibilities

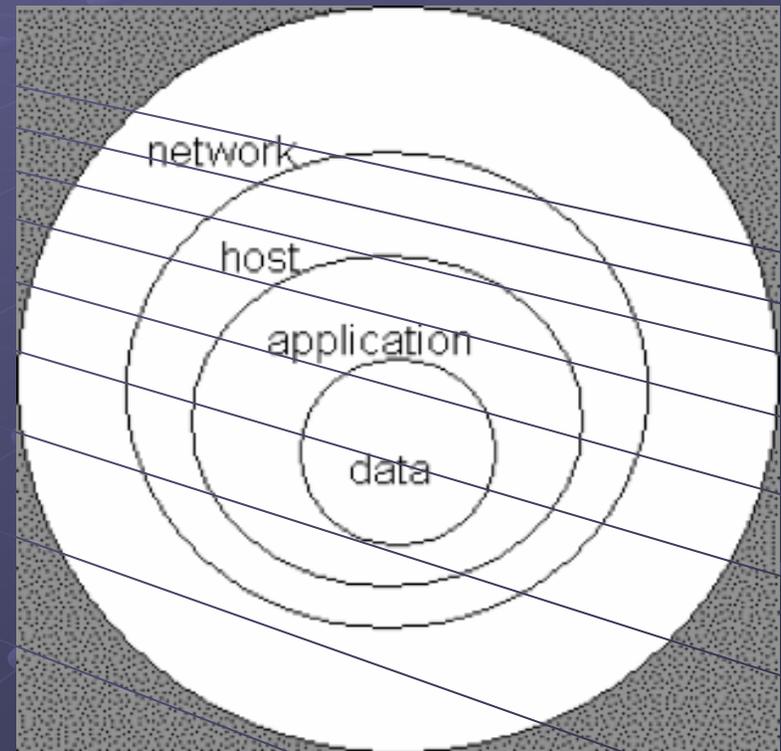
Access Management and Oversight

- 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 and Telecommunications 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

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 (Tripwire, 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

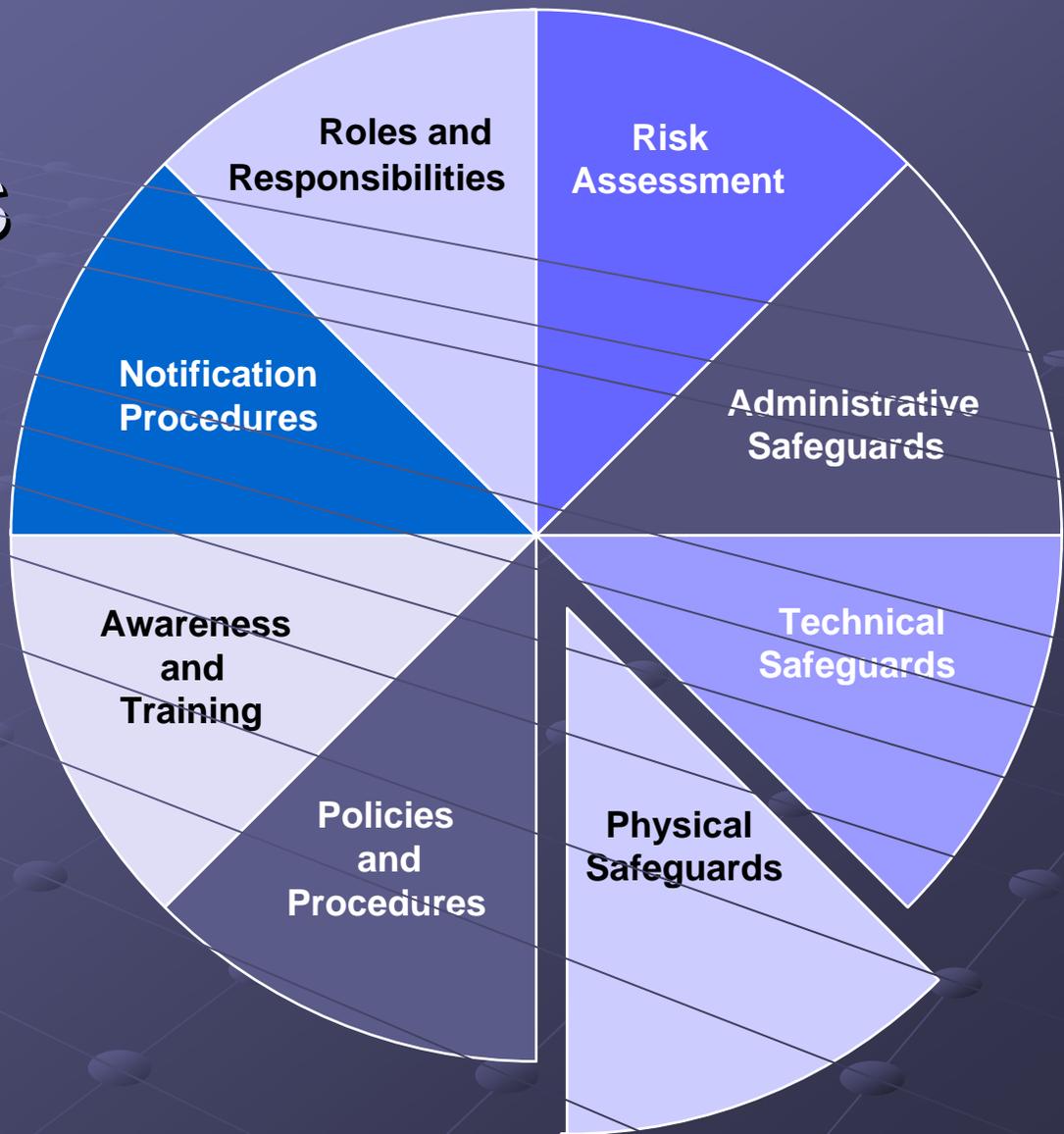
National Center for Supercomputing Applications



Slide provided by John Towns, NSCA

A Work in Progress

Physical Safeguards

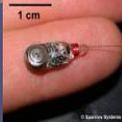


A Work in Progress

Physical Safeguards: Facilities Vary



Peromyscus maniculatus
Deer mouse



A Work in Progress

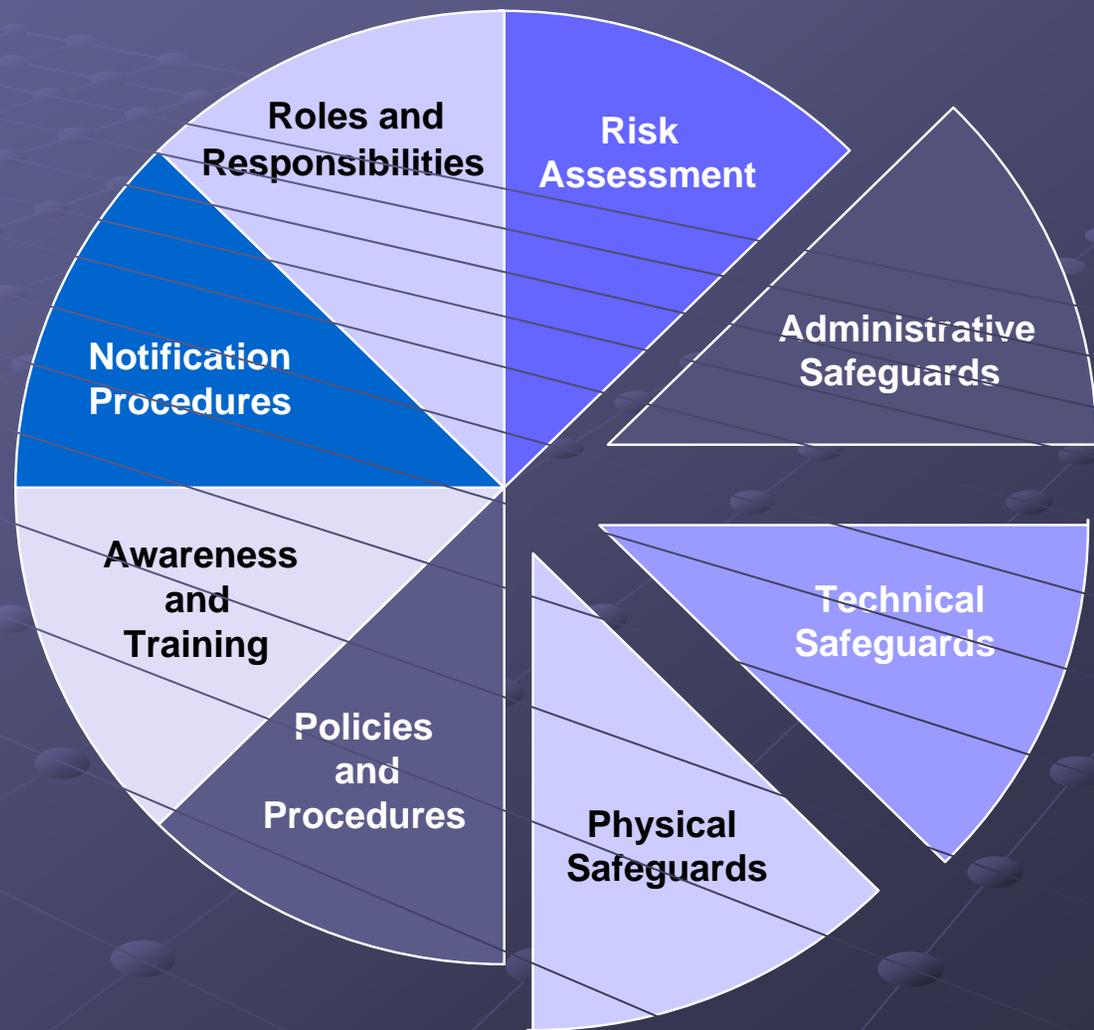
Elements of Physical Safeguards

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.

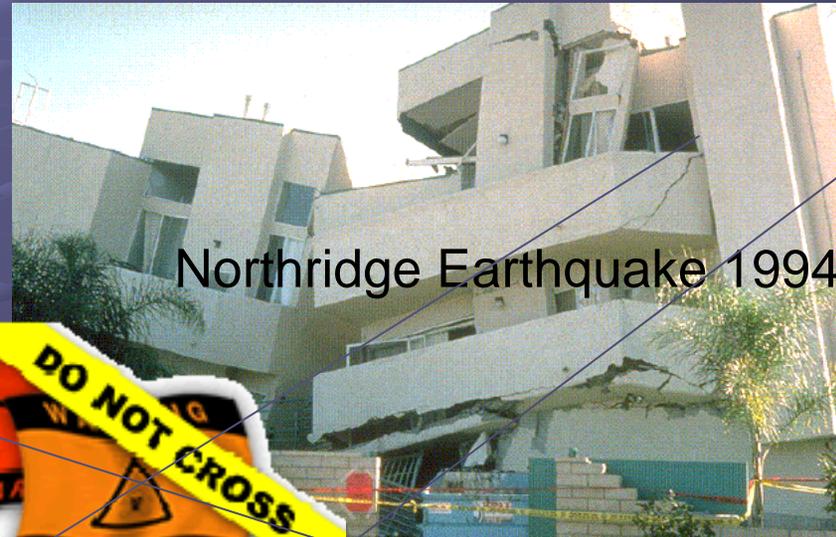
Administrative, Technical AND Physical (revisited)



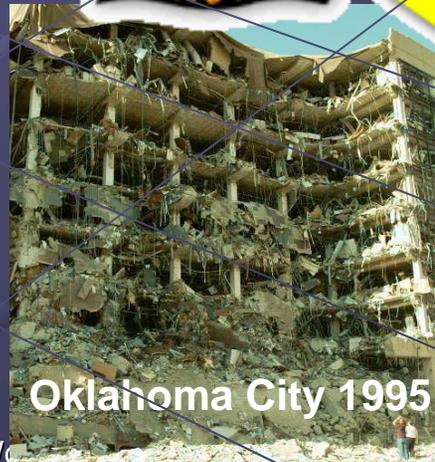
A Work in Progress

Administrative, Technical and Physical

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



Northridge Earthquake 1994



Oklahoma City 1995



A W

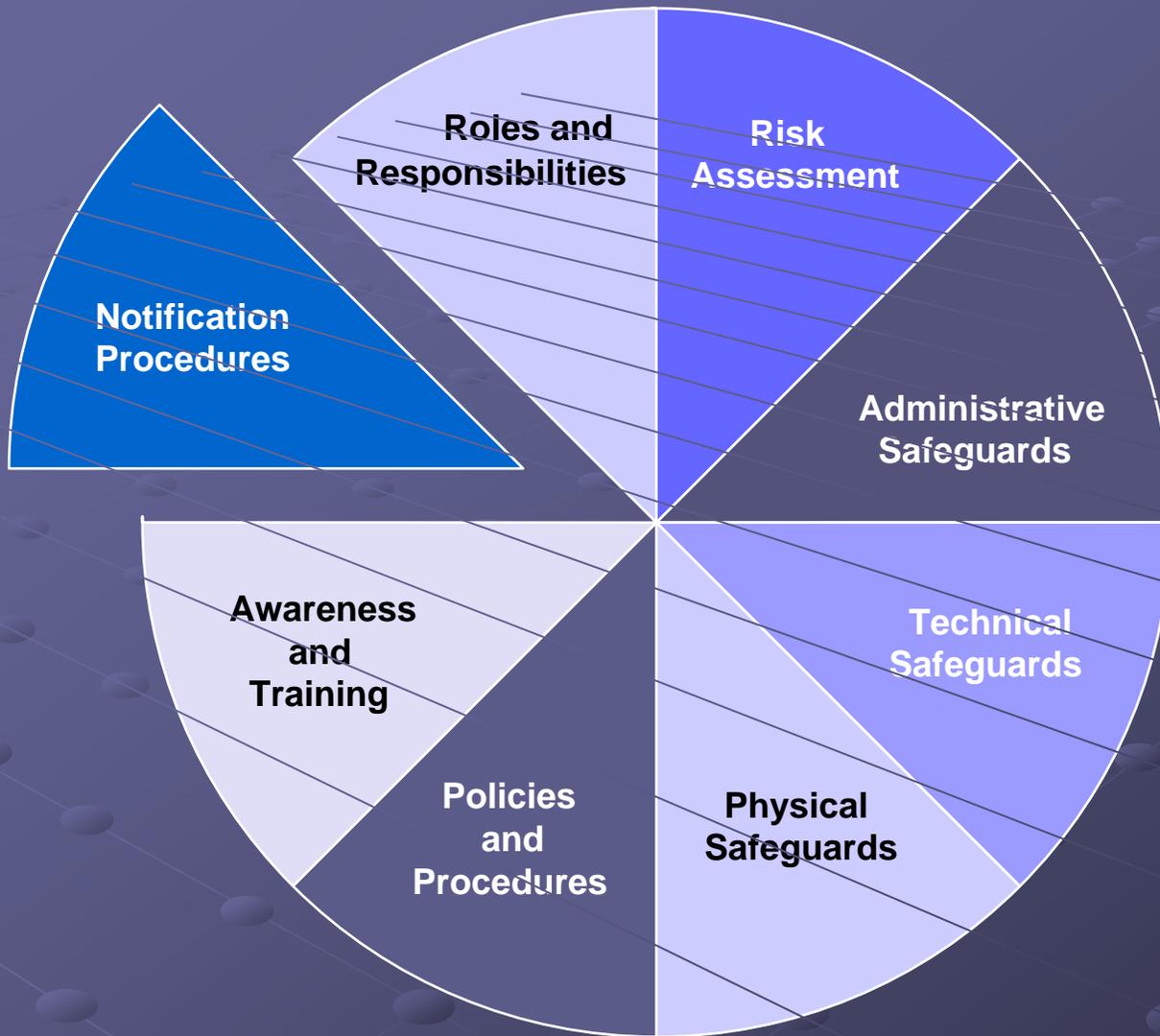
Technical, Administrative and Physical

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



A Work in Progress

Notification Procedures

- Understand the impact of an incident
- Define the roles
- Develop procedures for notifying:
 - 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 described on their website 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
 - 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 is compromised, don't send email from it! (Duh!)
 - Use encrypted email
 - Telephone
 - FAX

IT Security Program

Elements of an IT Security Program
<ul style="list-style-type: none">• 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 wheels...

- 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 from NIST and other organizations

Remember...

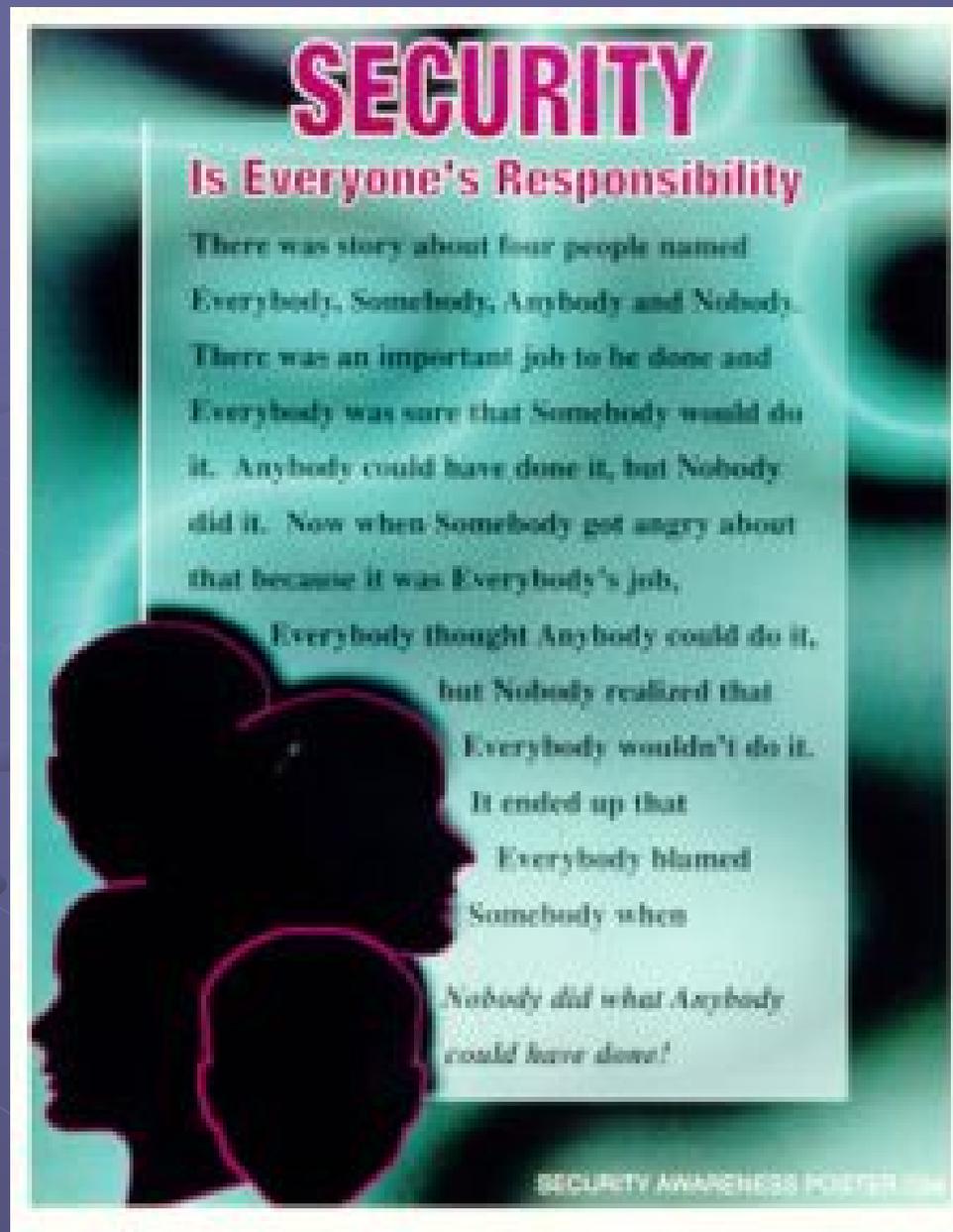
- It's about risk mitigation
- Information Security programs and plans will improve over time
- Information Security is a journey not a destination

Good IT practices foster
good security.

Good IT security reflects good
IT practices.

Invitation: 4th Cybersecurity Summit

- May 7-8, 2008
- Arlington, Virginia
- Invitation only; no registration fee
- Early registration ends April 11
- Hotel need to be reserved by April 11 to get the conference rate
- See your Program Director to arrange an invitation



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

A Work in Progress

Questions?

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

In real life:
Associate Vice President,
University Information Services
Georgetown University

A Work in Progress

Sources of Best Practices

● Consortia

- NEES [Cyberinfrastructure Security Plan](#)

● Security Policies

- EDUCAUSE Resource Center
- EDUCAUSE/Internet2 Wiki
- Other similar institutions

● Incident Handling and Response

- TeraGrid [model](#)
- Yale University

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 15 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](#)