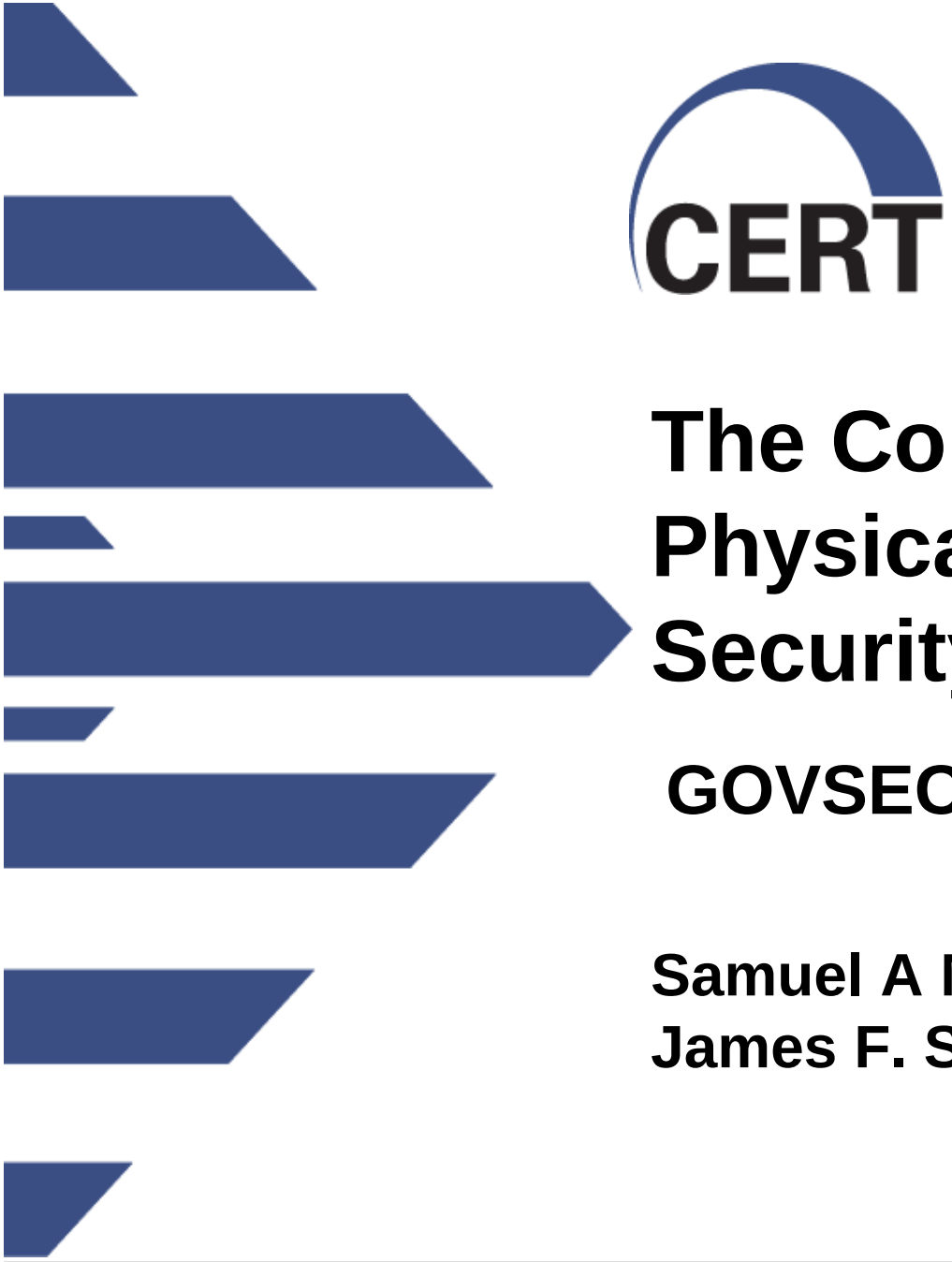


The Confluence of Physical and Cyber Security Management

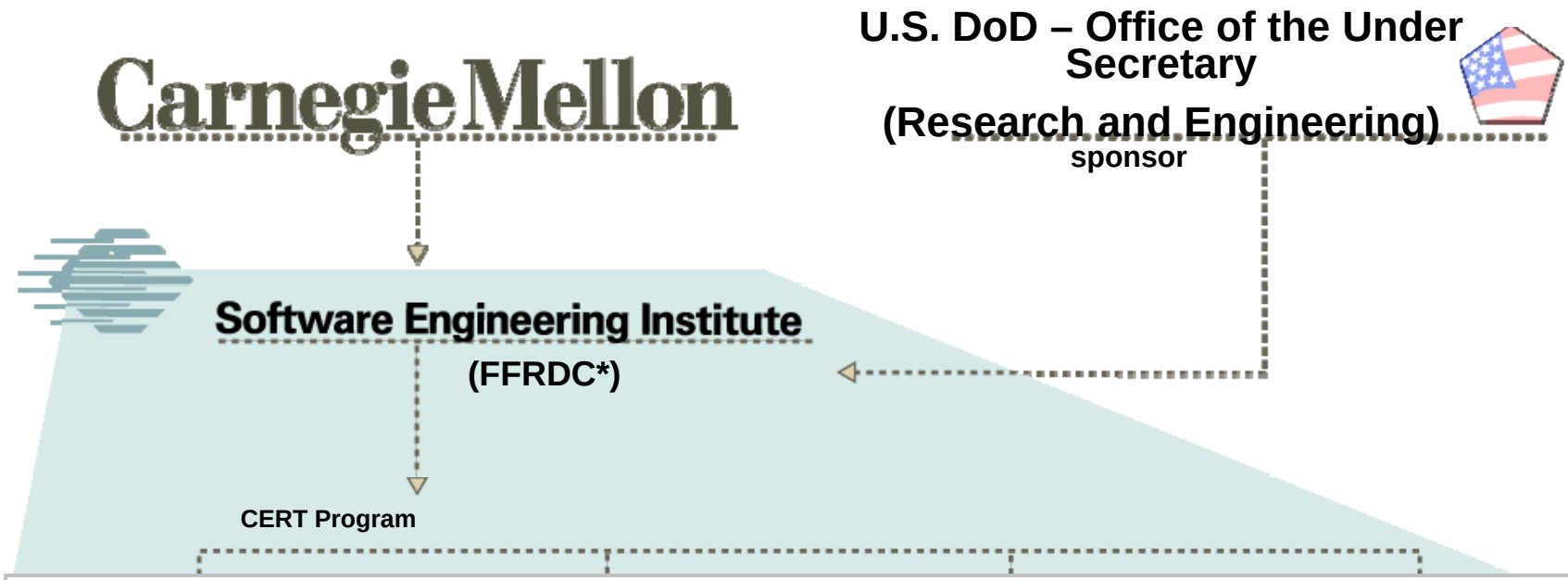
GOVSEC 2009

Samuel A Merrell, CISSP
James F. Stevens, CISSP

Today's Agenda:

- Introduction
- Risk Management Concepts
- Confluence of Physical and Cyber Security
- Adopting a Service View
- A Service View for Critical Infrastructure
- Next steps

Software Engineering Institute



- Cyber Threat and Vulnerability Analysis
- Enterprise and Workforce Development
- Secure Software and Systems
- Digital Forensics

CERT Capabilities

Resiliency Engineering and Management

Resiliency Engineering and Management (REM) develops, deploys, and institutionalizes tools, techniques, methods, and training that advance organizational capabilities for governing and managing operational resiliency and risk for critical assets (such as information and infrastructure) and services

REM Research Focus

REM work aligned along four focus areas:

- Resiliency Engineering
- Information Resiliency
- Critical Infrastructure Resiliency
- Governance, Risk & Compliance

Today's Agenda:

- Introduction
- Risk Management Concepts
- Confluence of Physical and Cyber Security
- Adopting a Service View
- A Service View for Critical Infrastructure
- Next steps

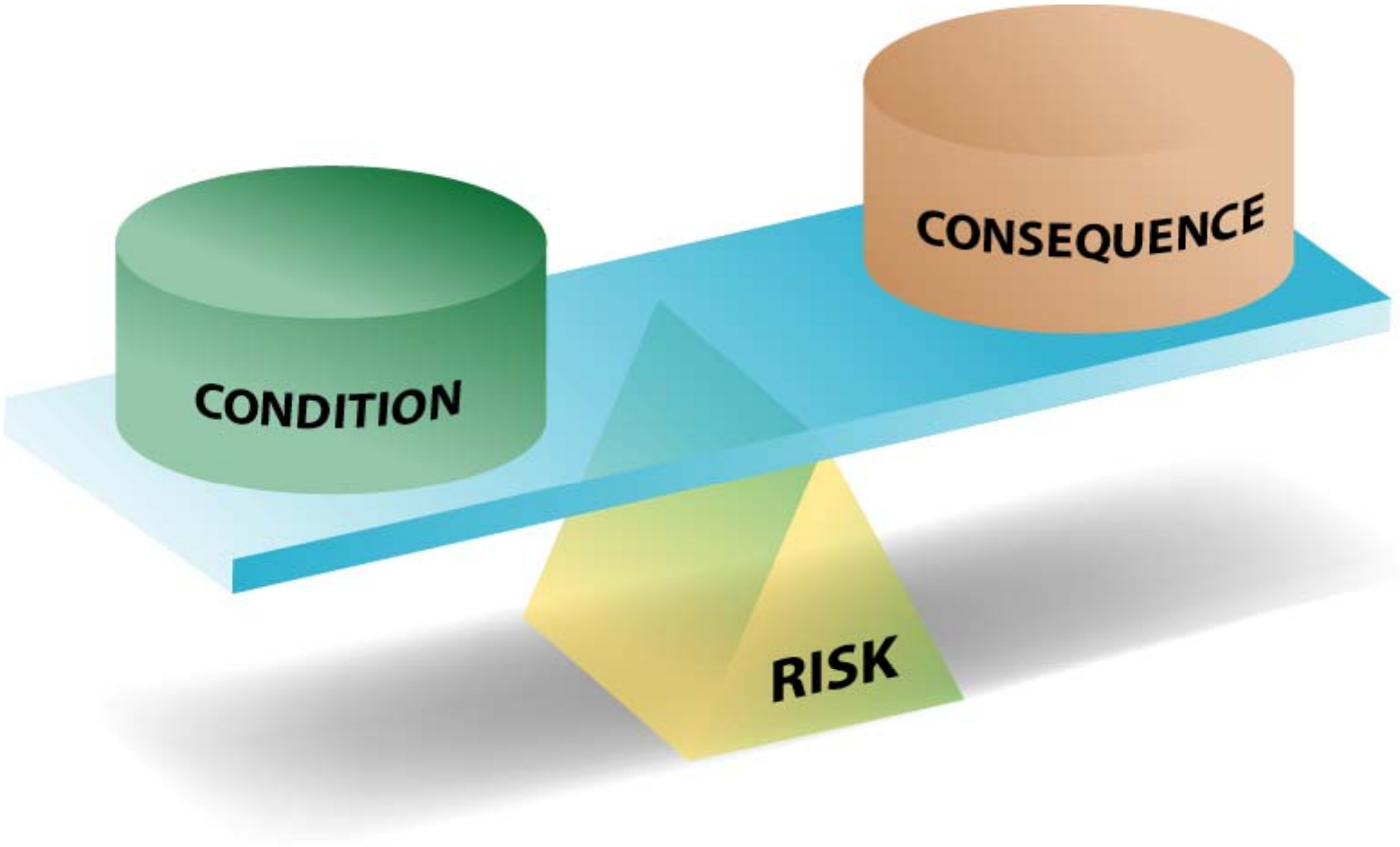
Risk

A risk is the possibility of incurring a loss or harm

For risk to exist in any circumstance, the following three conditions must be satisfied

- There must be a loss associated with the situation
- There must be some uncertainty with respect to the eventual outcome
- Some choice or decision is required

The Basic Risk Equation



Risk Mitigation Options

Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level

Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence

Risk Limitation. To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability

Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls

Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability

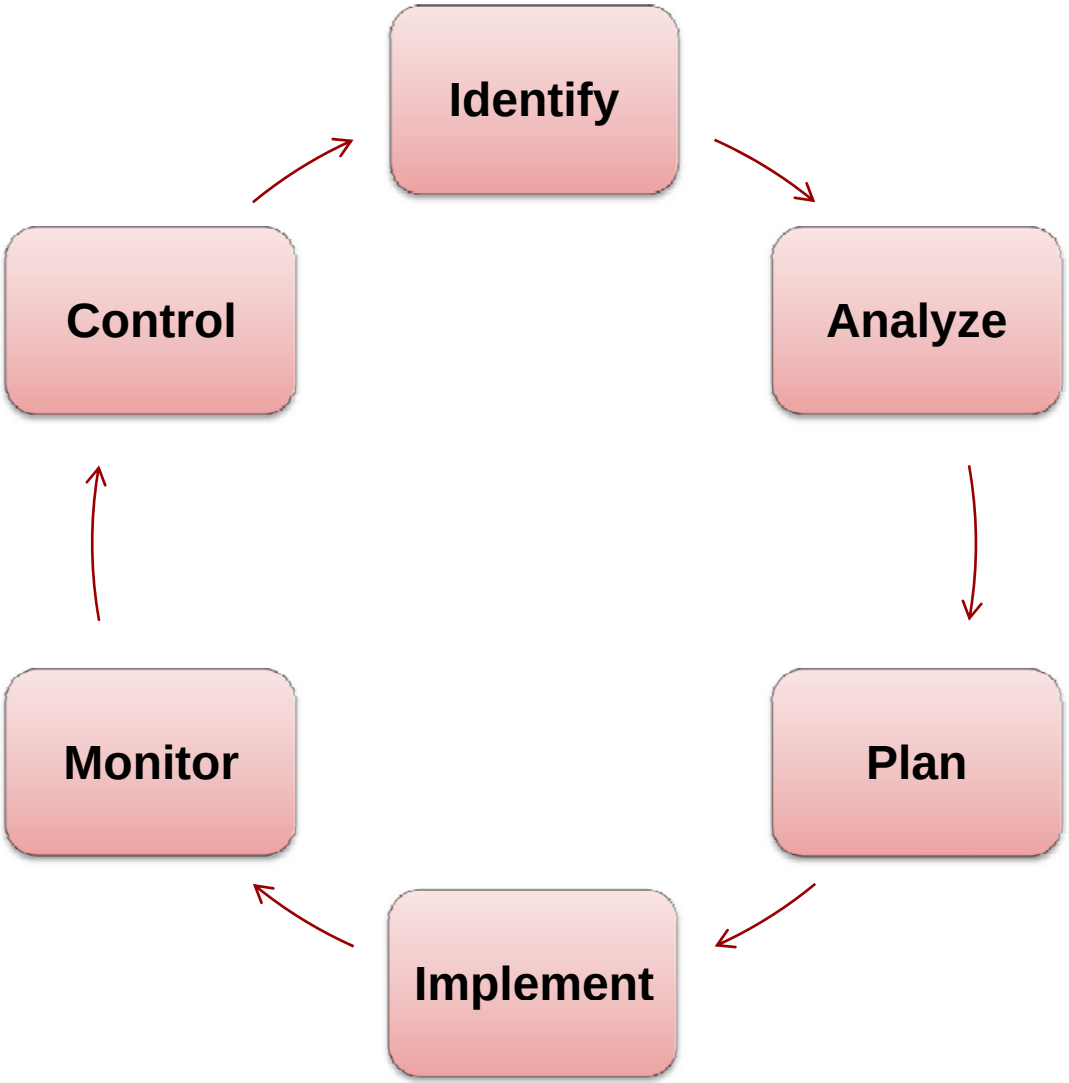
Risk Transference. To transfer the risk by using other options to compensate for the loss

Residual and Acceptable Risk

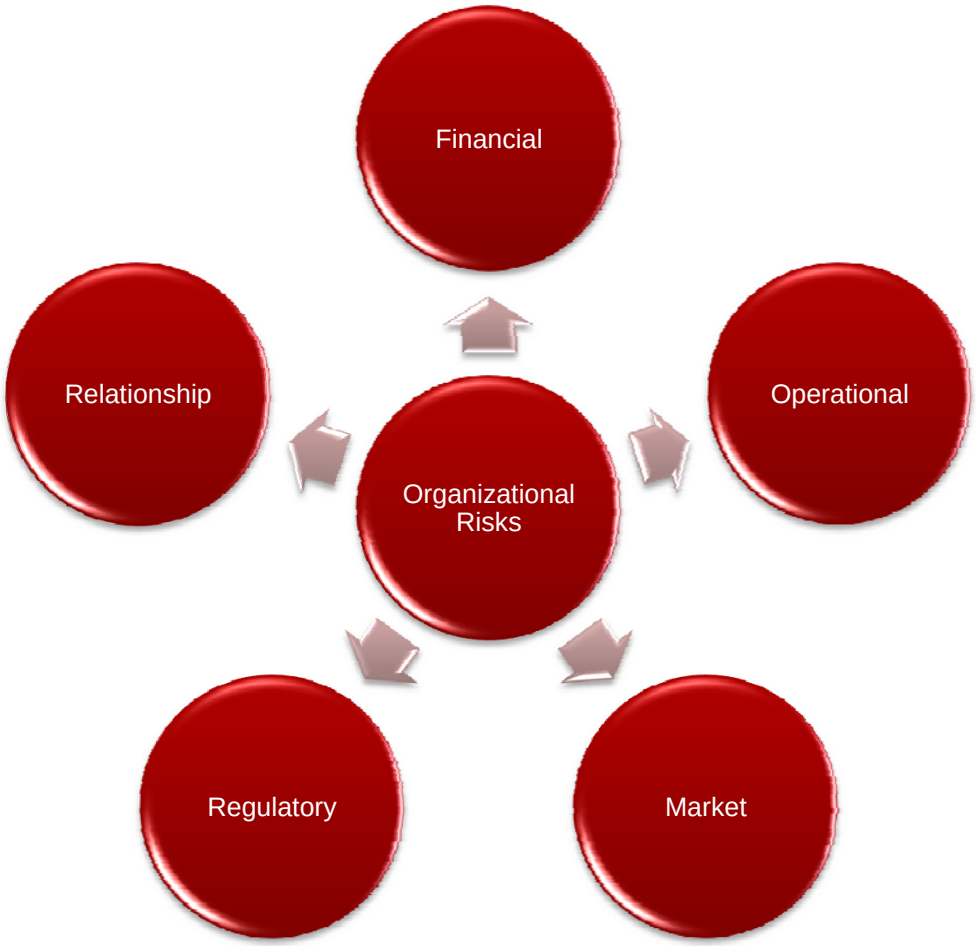
Residual risk is the potential for the occurrence of an adverse event after adjusting for the effectiveness and impact of all implemented security measures (controls)

Acceptable risk is the level of residual risk that has been determined to be a reasonable level of potential loss/disruption to a system or organization

A Risk Management Process

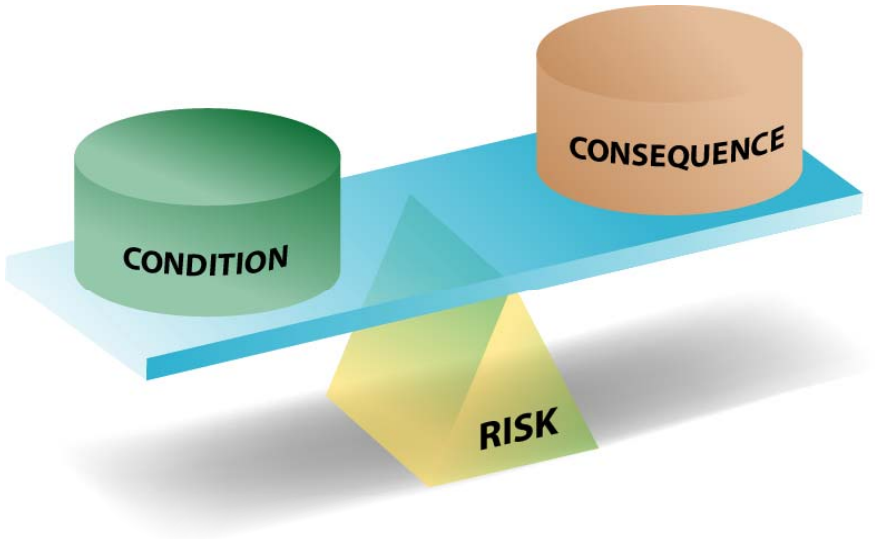


Diverse Risks To Be Managed



Security and Operational Risk

- Managing firewall rule-sets
- Installing fences around facilities
- Limiting access to intellectual property or confidential information
- Developing business continuity and disaster recovery plans



The aim of these "security" activities, both physical and cyber, is ultimately to manage operational risk

Focus on Operational Risk

A form of hazard risk affecting day-to-day business operations

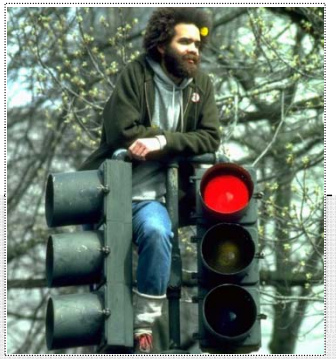
The potential failure to achieve mission objectives

"Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events."

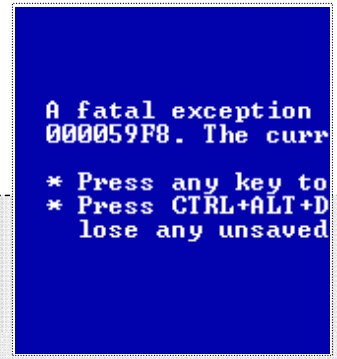
--Basel II Capital Accords

Scope of Operational Risk is *Vast*

Actions of people



Systems & technology failures



Failed internal processes

External events

Tech reliance

Global economy

Open boundaries

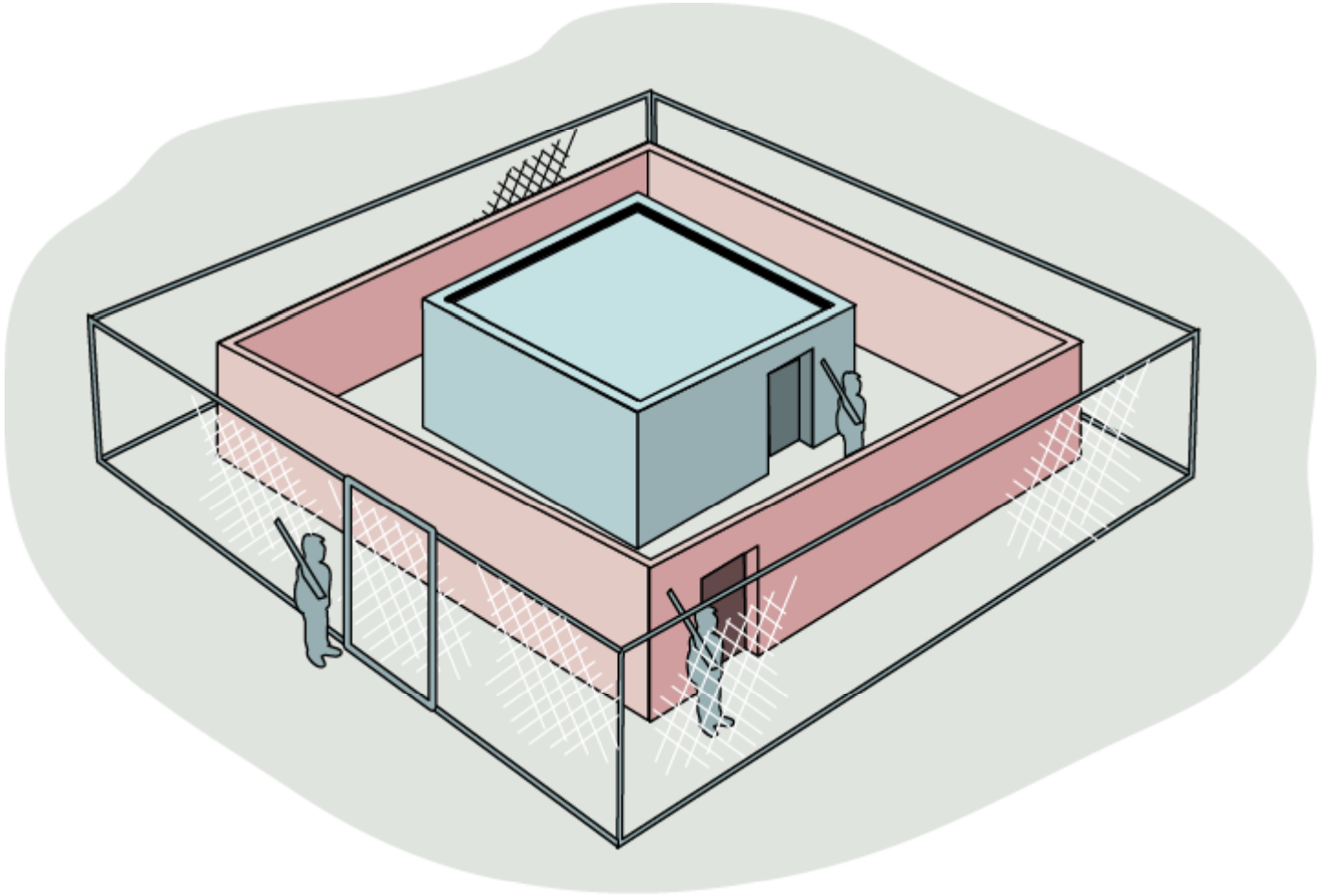
Complexity

Cultural shifts

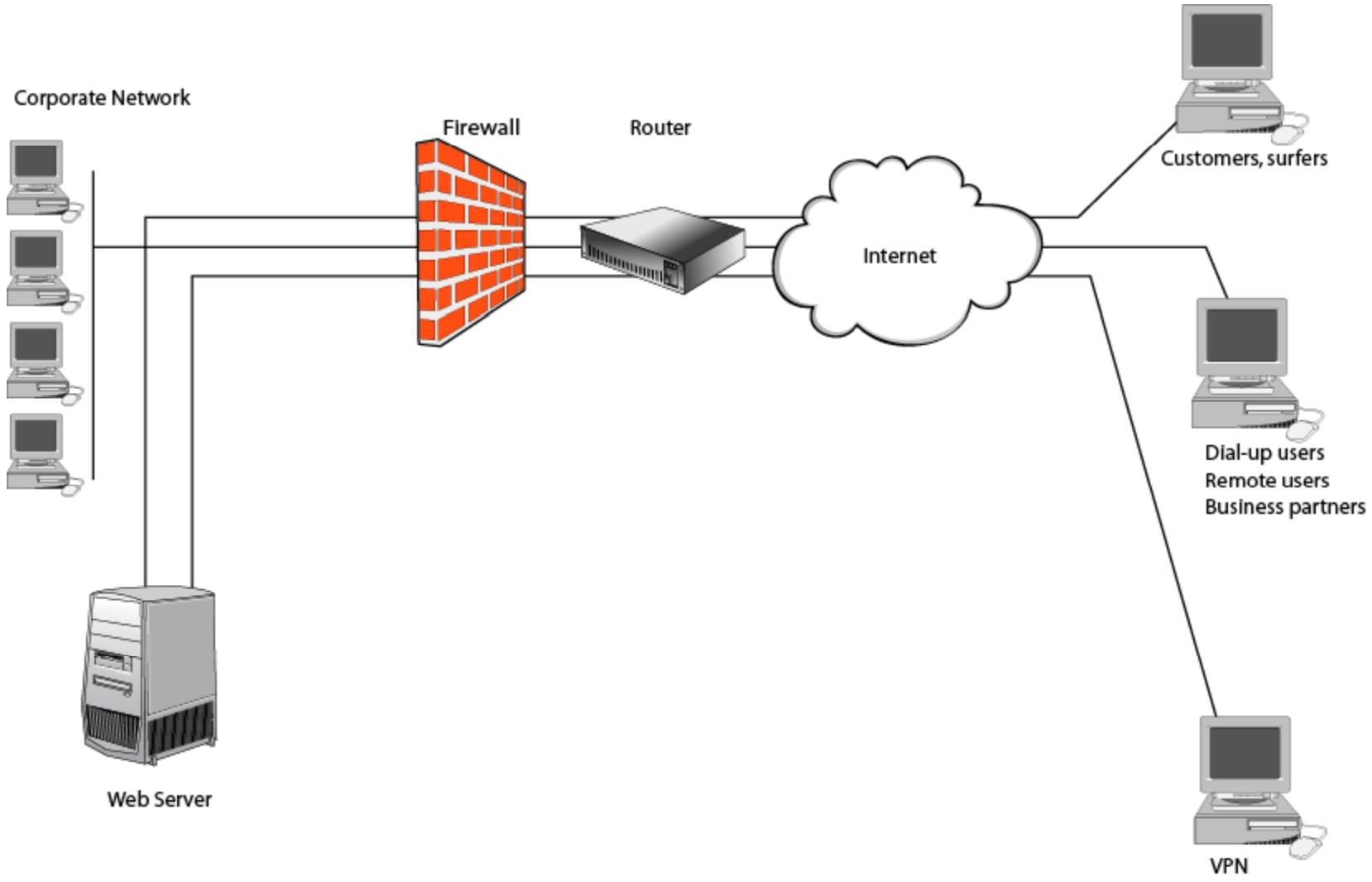
Today's Agenda:

- Introduction
- Risk Management Concepts
- Confluence of Physical and Cyber Security
- Adopting a Service View
- A Service View for Critical Infrastructure
- Conclusion

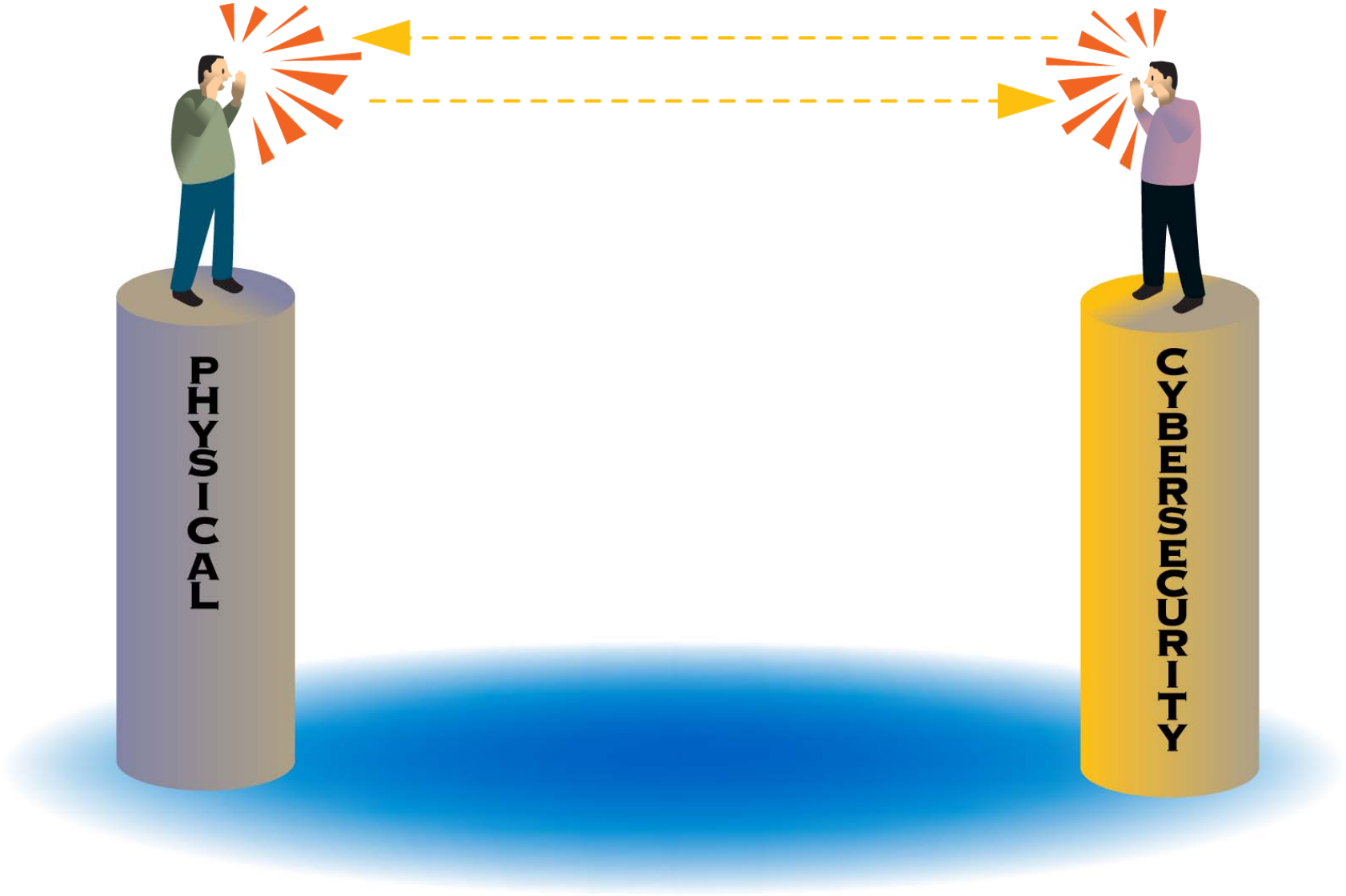
Physical Security - Yesterday



Cyber Security - Yesterday



Silos of Responsibility



Today - Confluence

The Risk Management Challenge

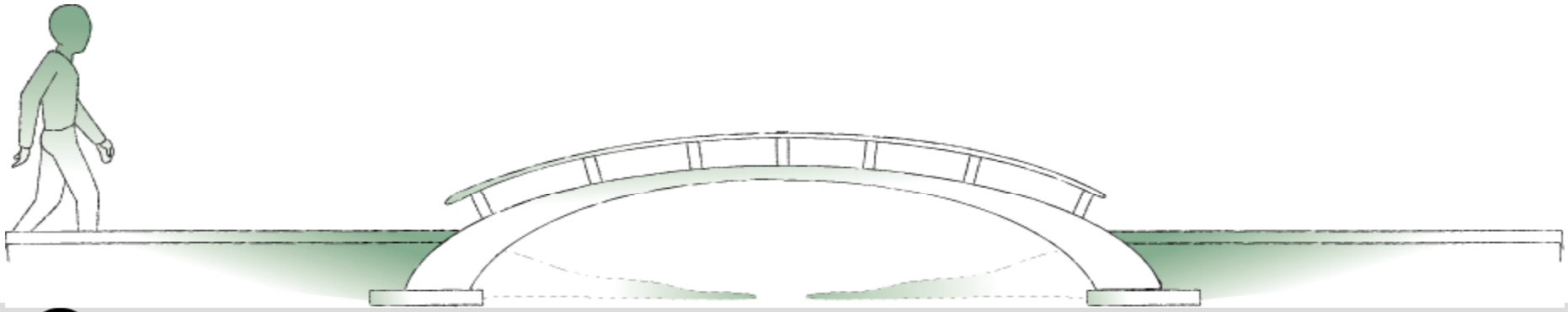
- The convergence of physical and cyber security has rapidly expanded the threat environment that must be managed
- Limited organizational resources are available for security activities
- Ensure that those limited resources are effectively and efficiently deployed

“Human sacrifice, dogs and cats living together... mass hysteria!” – Dr. P. Venkman

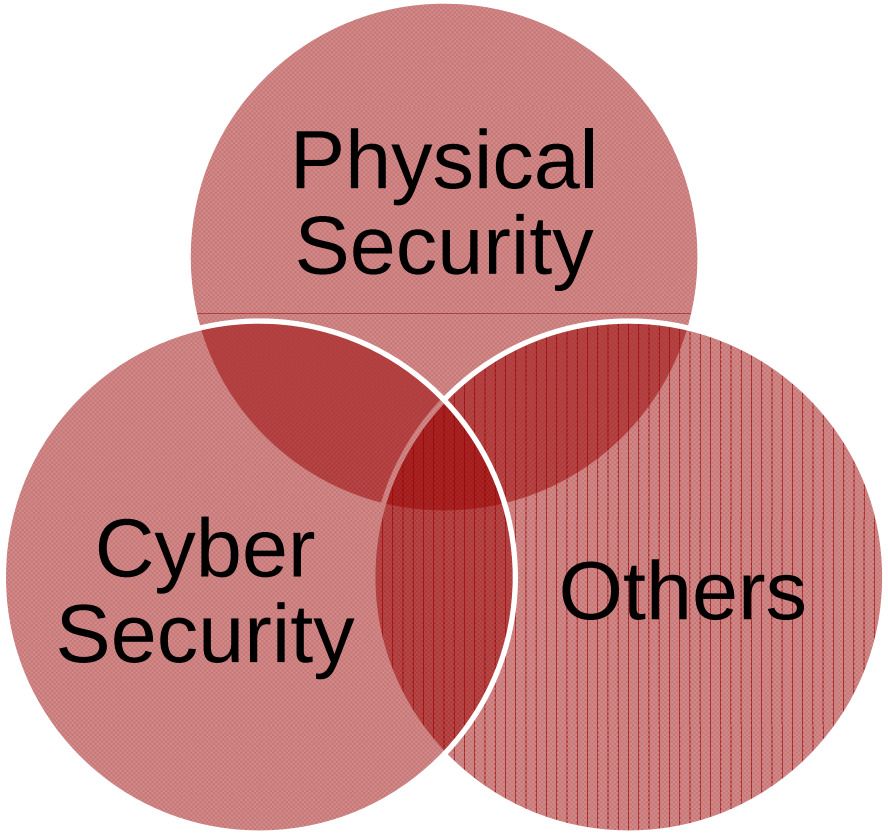
A Structured Approach

Shifting Security Paradigms

	Yesterday	***Today***
Scope:	**Security**	***Operational***
Ownership:	**IT and Physical**	***Enterprise***
Focus:	**Discrete**	***Continuous***
Driver:	**External**	***Internal***
Execution:	**Platform/practice**	***Process***
Goal:	**IT and Physical security**	***Enterprise resilience***



An Integrated View of Security



A Fresh Look at Security Management

Operational risks must be managed within a program that can adapt to a dynamic environment – this requires active mitigation of all identified risks, regardless of their nature (e.g., cyber or physical)

http://en.wikipedia.org/wiki/File:Pittsburgh_view-from-incline_sm.jpg

Today's Agenda:

- Introduction
- Risk Management Concepts
- Confluence of Physical and Cyber Security
- Adopting a Service View
- A Service View for Critical Infrastructure
- Conclusion

Current Approaches to Security Management

Security by **compliance**

- FISMA
- HIPAA
- PCI

Security by adoption of **best practices**

- ISO 17799
- DISA STIGs
- Vendor guides

Result:

Uneven use of limited resources

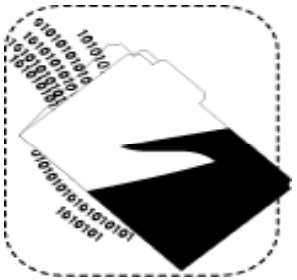
Enterprise Perspective

An enterprise view of risk

- Enables risk mitigation decisions that effectively deploy limited resources
- Integrates with enterprise architecture approaches to security management
- NIST SP 800-39's "Risk Executive"
- Incorporates physical and cyber security management

Assets of an Organization

people



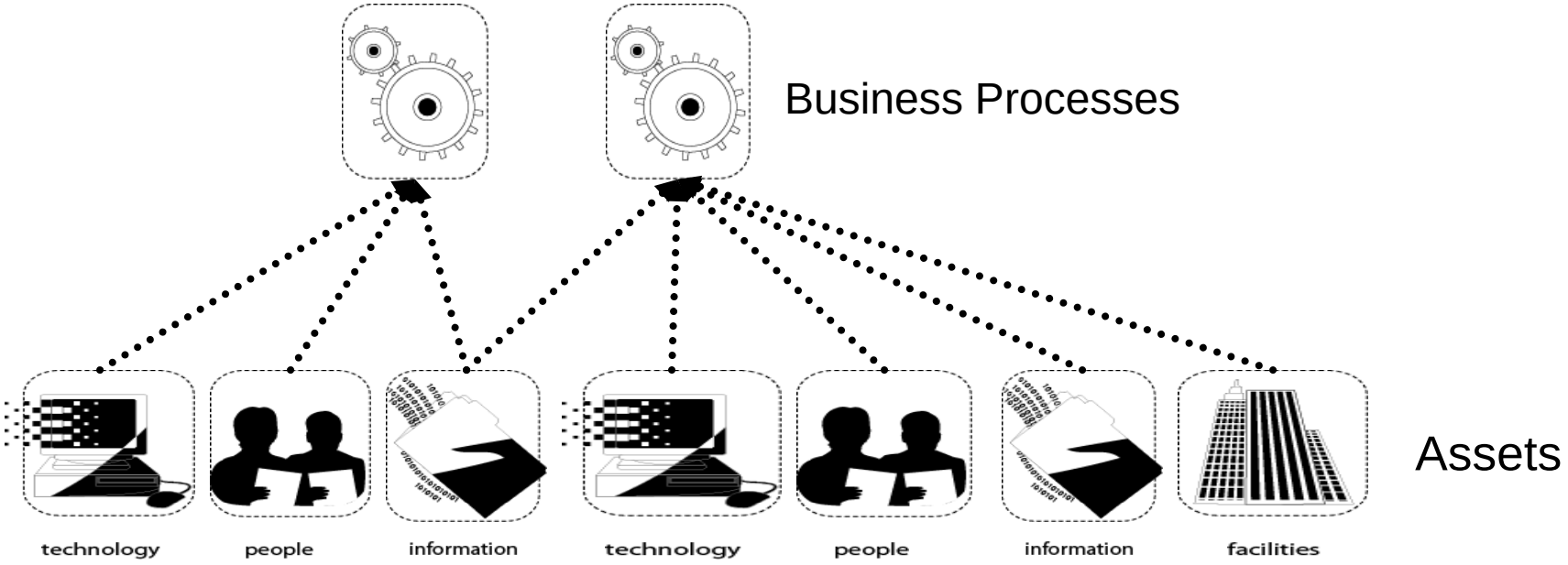
information

technology

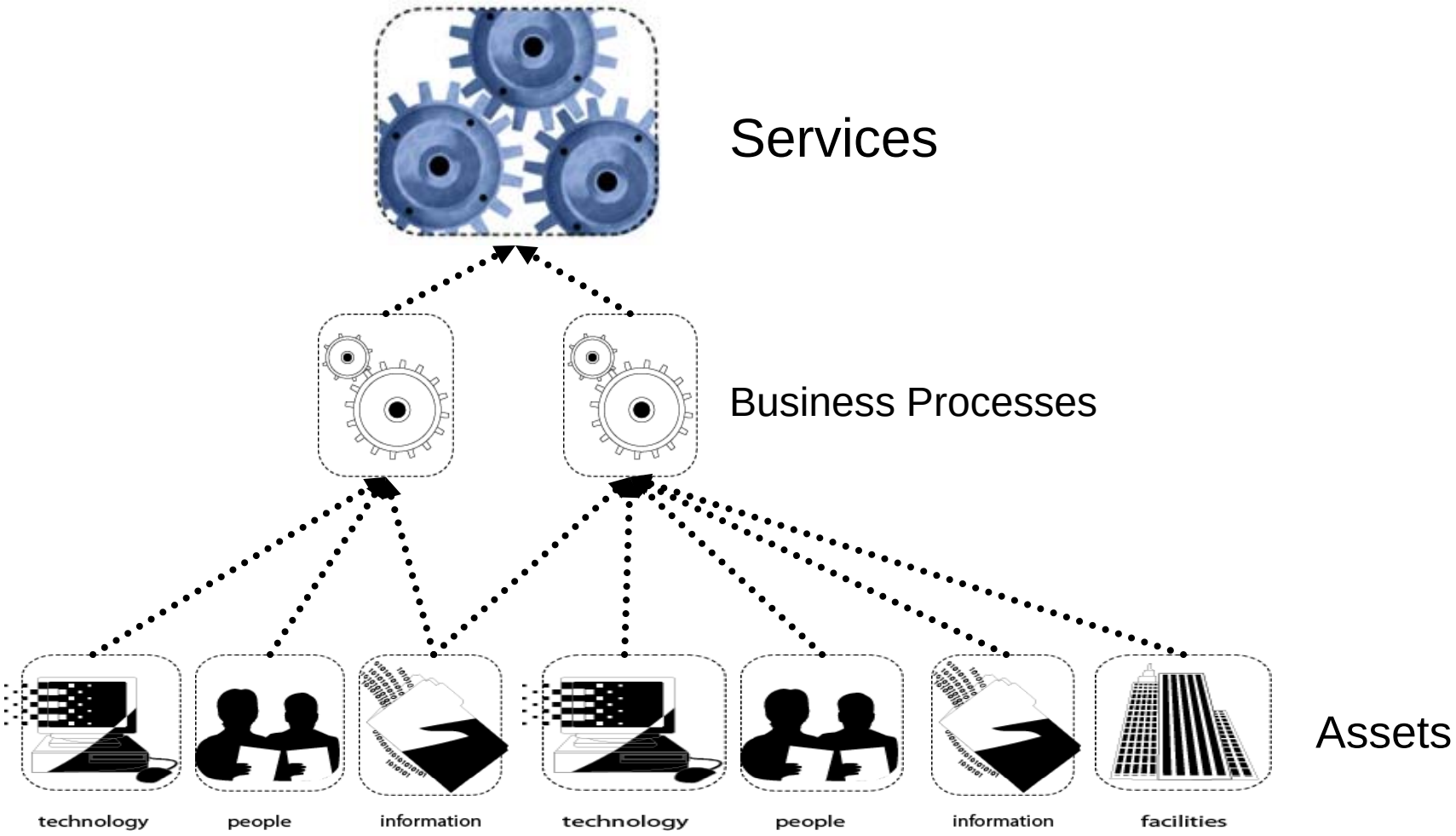
facilities

Assets

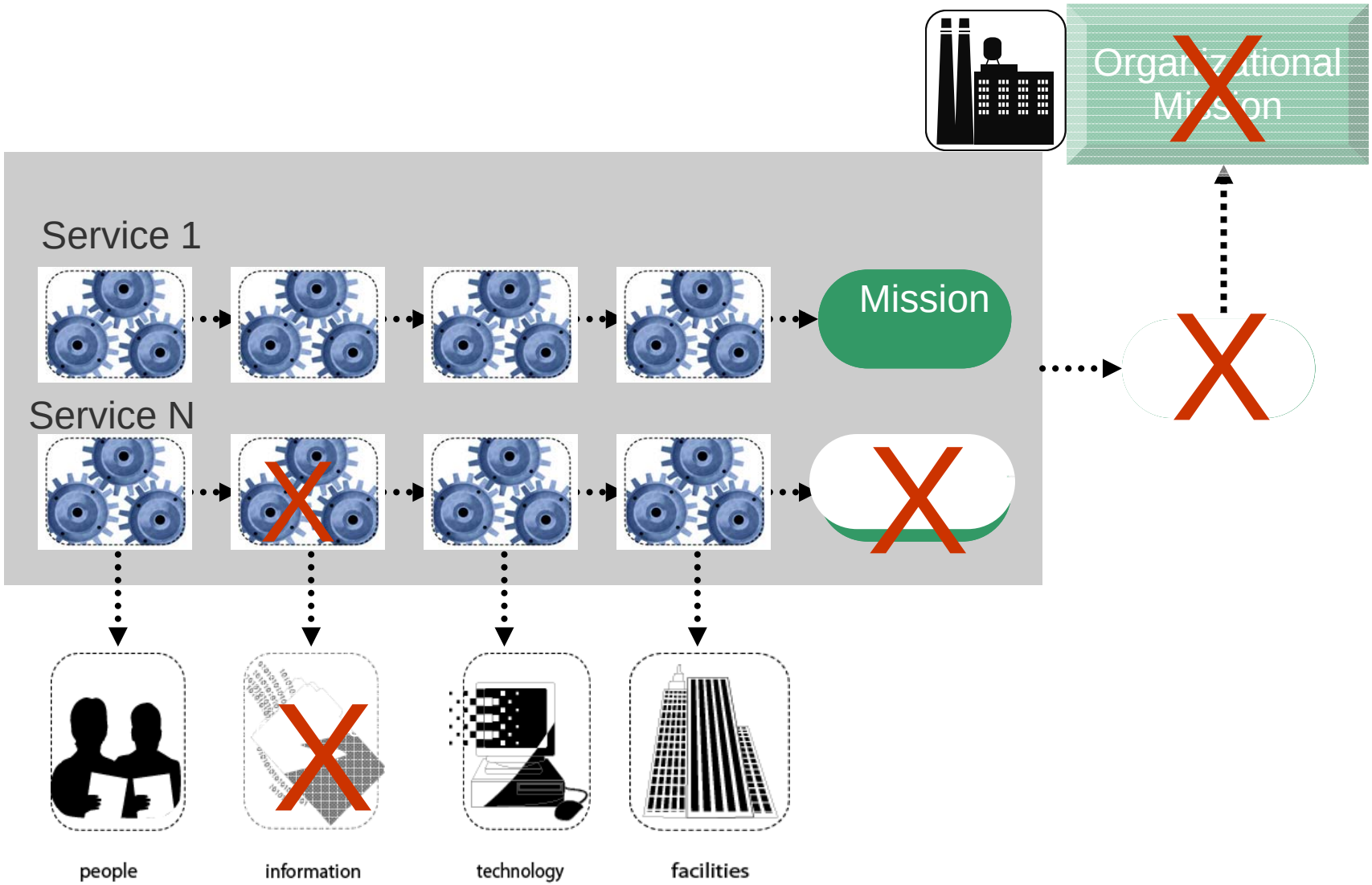
Assets Support Business Processes



Business Processes Support Services



Services Support the Mission



Step 1: Understand Your Services

- Formally identify the services that your organization must deliver in order to accomplish its mission
- Ask “what are the core competencies of the organization?”
  - Often, business units are divided along these lines
    - Manufacturing Operations
    - Sales and Marketing
    - Finance
    - Compliance
    - Research and Development
    - Customer Service

Operational Risks to Service Delivery

Risks to service delivery are what organizations need to care about

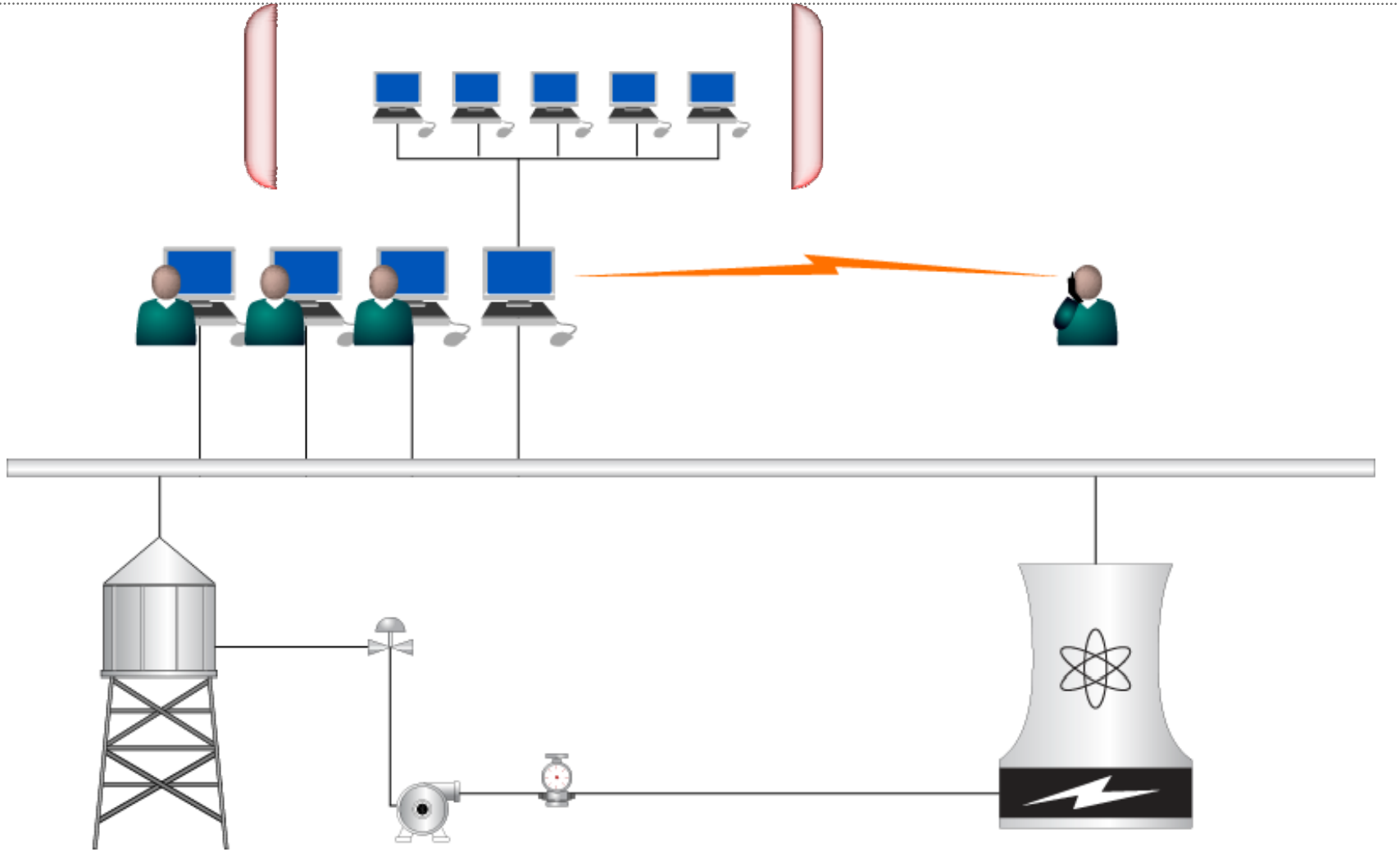
- These risks arise from both physical and cyber threats, therefore, both of these risks need to be mitigated efficiently and effectively
- Physical and cyber protection strategies for assets can be engineered and evaluated in terms of their ability to best ensure the service

Benefits of Adopting a Service View

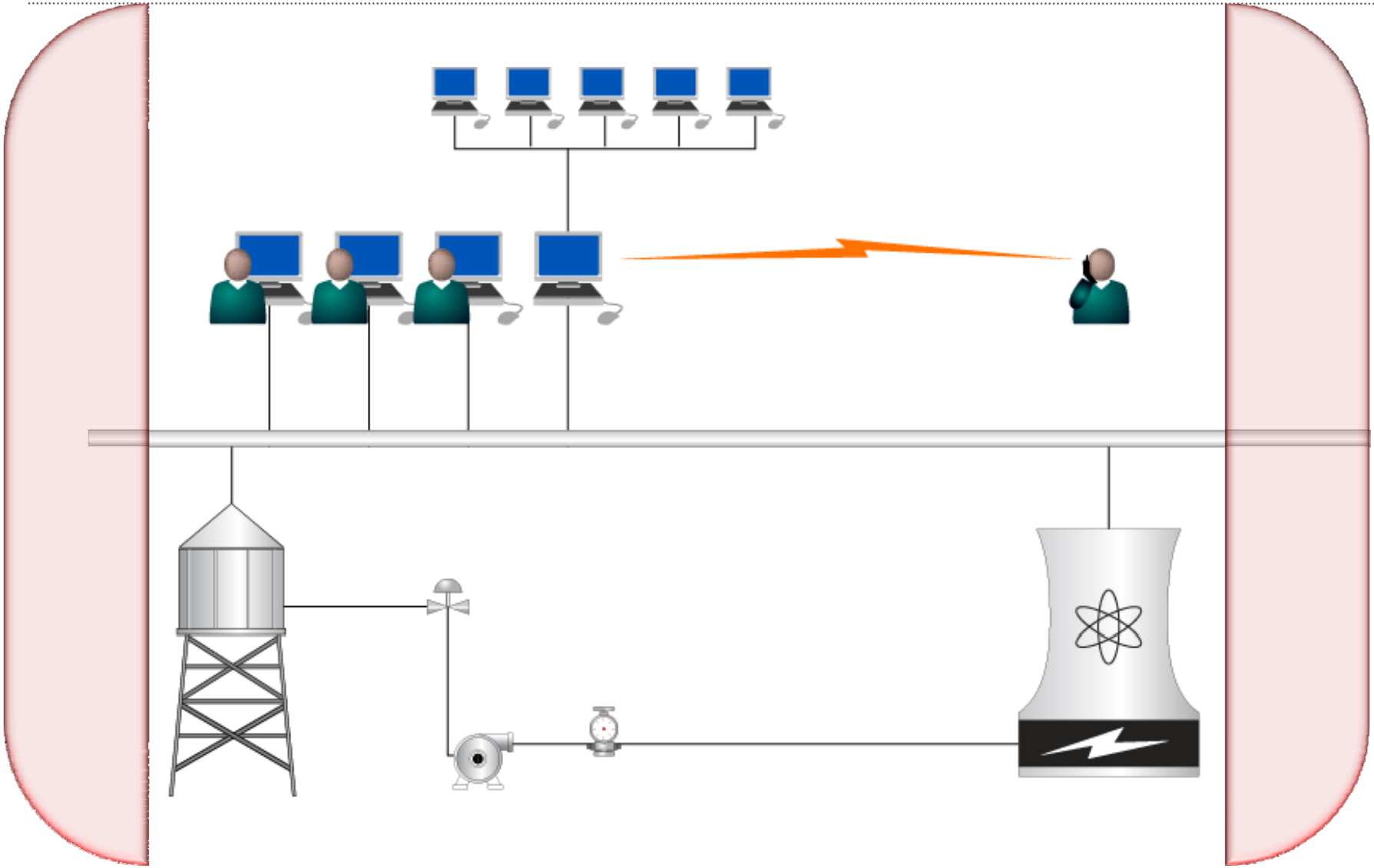
Align the protection and sustainment strategies to the organization's mission

- Engineer a unified approach to mitigating risks
- Evaluate protection strategies for effectiveness in protecting the mission
- Ensure efficiencies in the application of limited resources

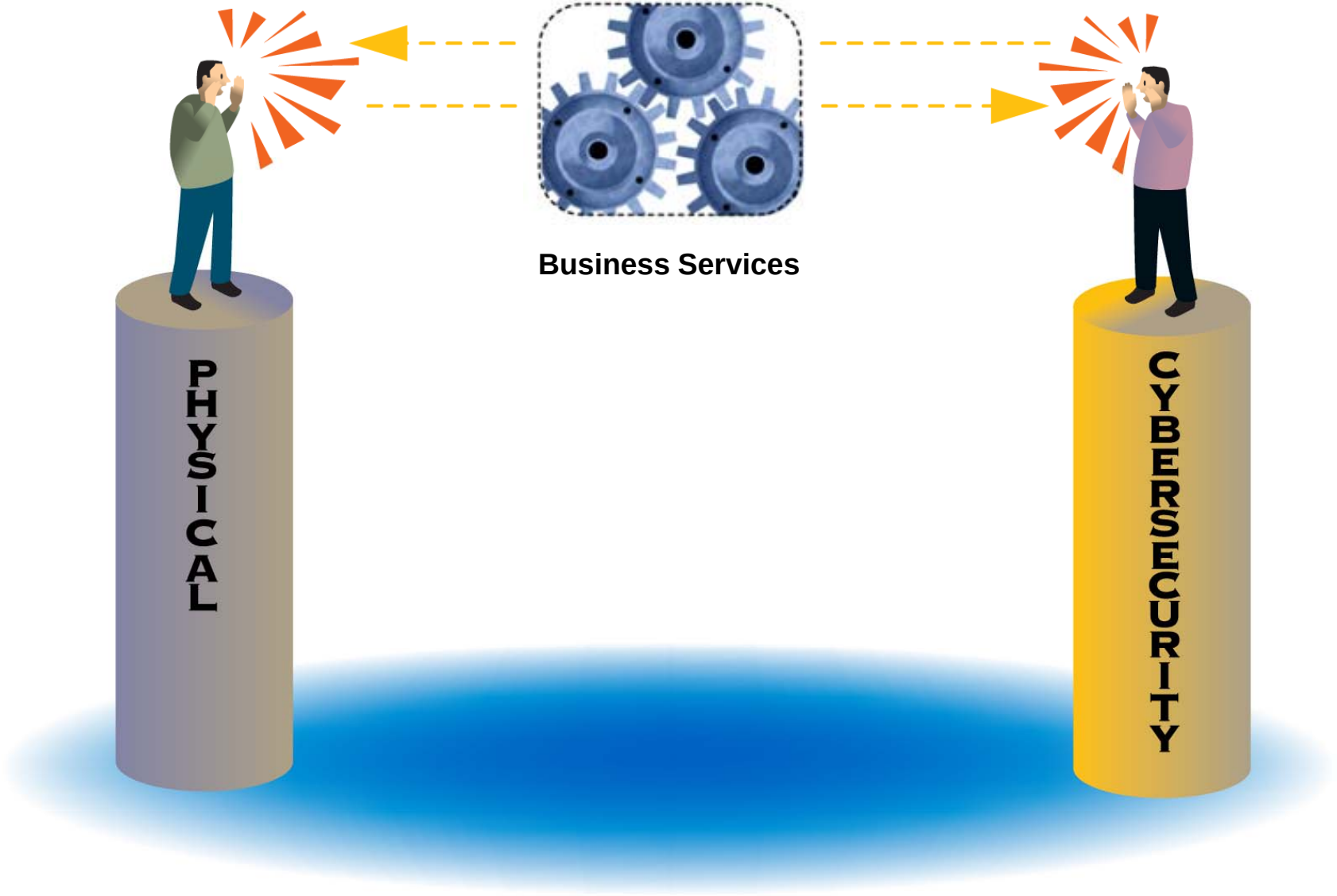
Engineer a Unified Approach to Mitigating Risks-1



Engineer a Unified Approach to Mitigating Risks-2



Select Effective Protection Strategies



Ensure Efficiencies

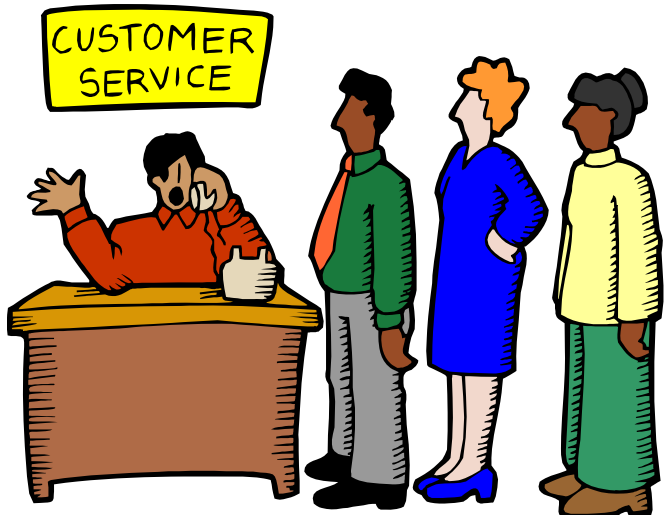
Maximize use of limited resources by incorporating the disciplines of physical and cyber security

- What works best for your environment: a guard at a post, an automated intrusion detection system, or both?

Step 2: Define Service Requirements

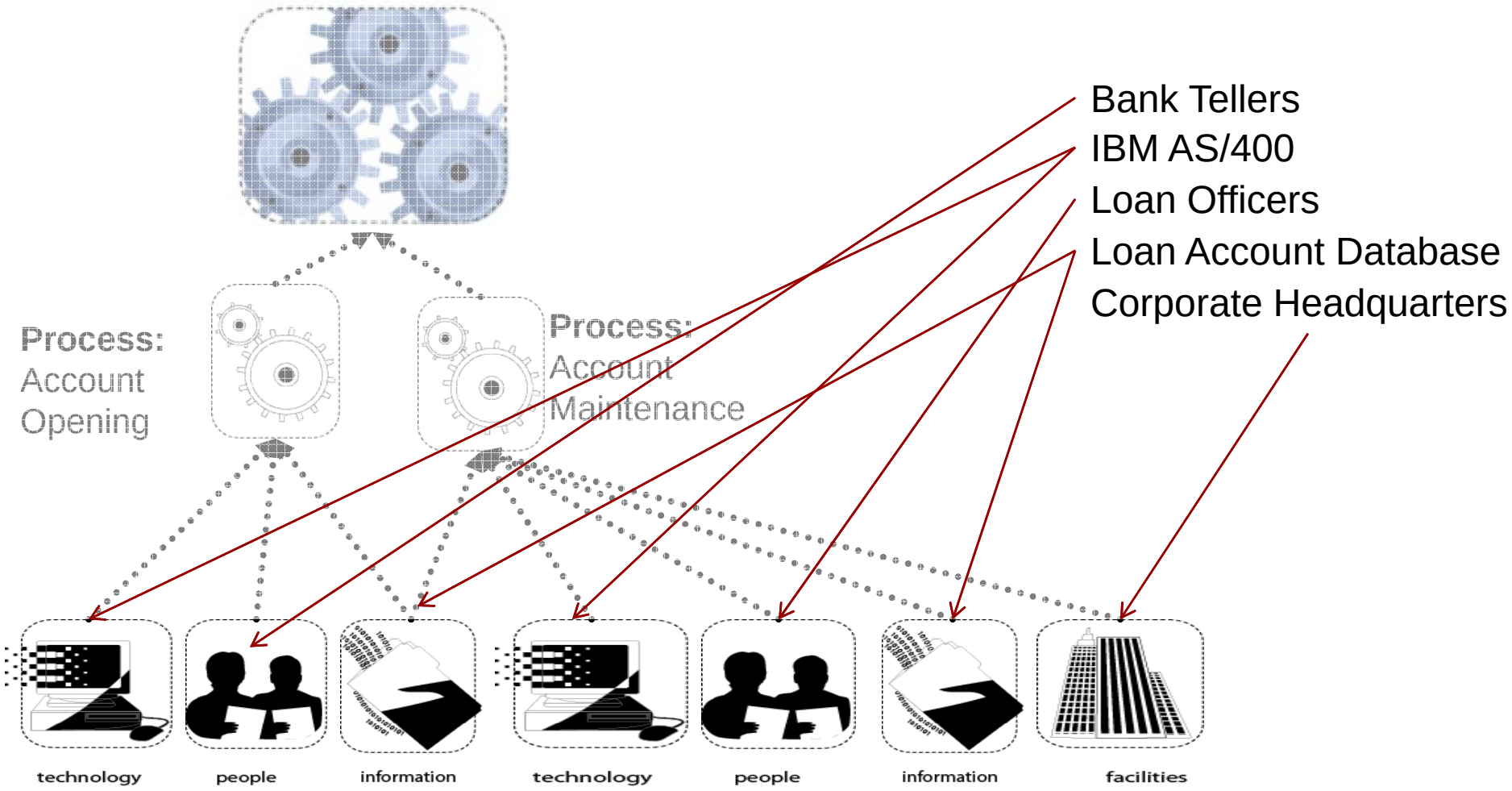
What are the needs of the services that you have identified?

- Customer Service is available between 9:00 am and 5:00 pm
- This monitoring system must operate 24 x 7

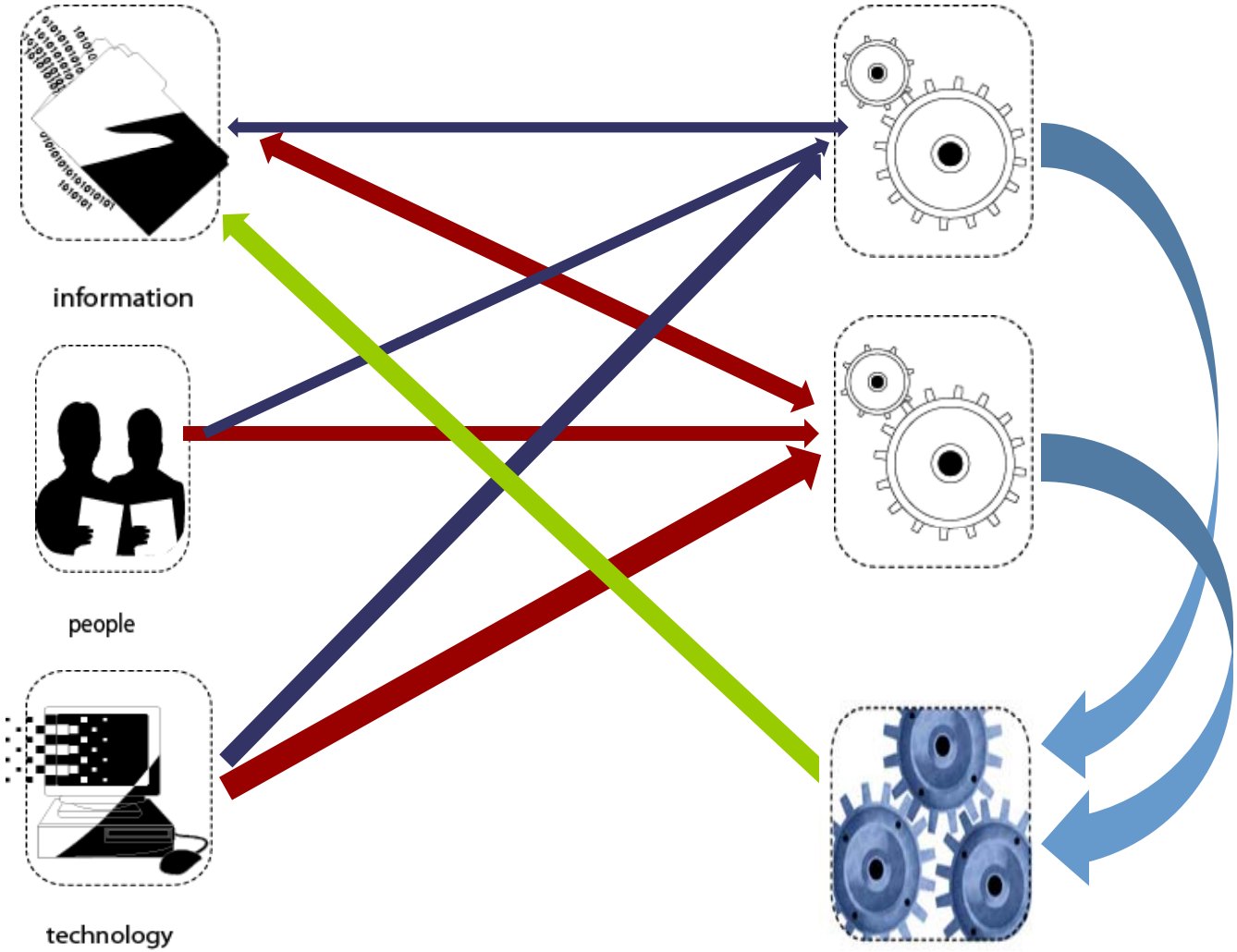


Step 3: Map Assets to Services

Service: Loan Operations

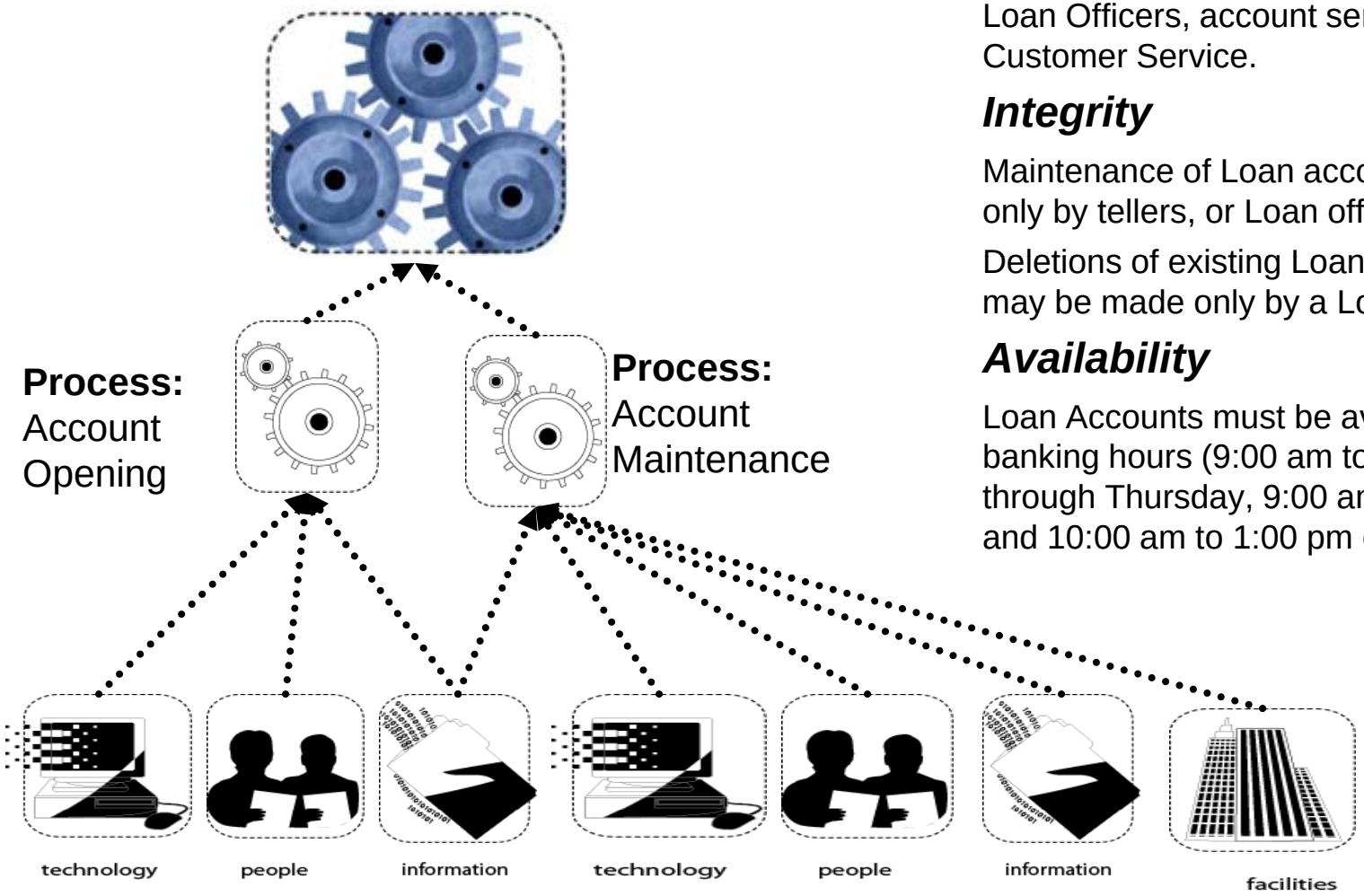


Identifying Interdependencies



Step 4: Define Resiliency Requirements

Service: Loan Operations



Confidentiality

Loan Account data may be viewed only by Loan Officers, account servicing staff, and Customer Service.

Integrity

Maintenance of Loan accounts may be made only by tellers, or Loan officers.

Deletions of existing Loan Account information may be made only by a Loan Officer.

Availability

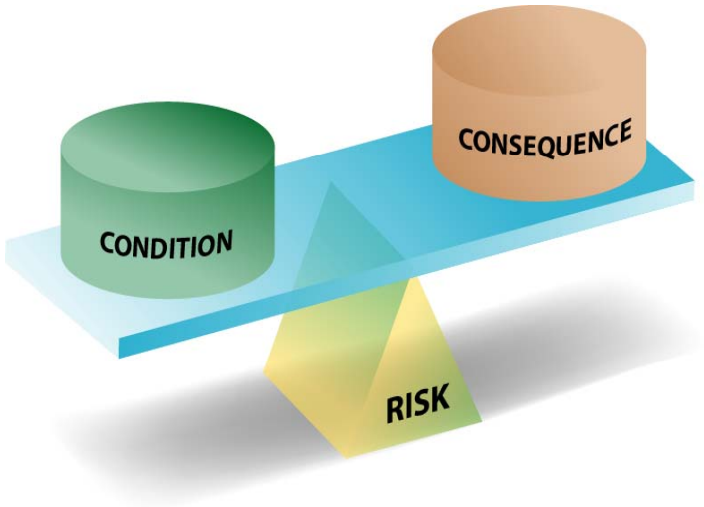
Loan Accounts must be available during normal banking hours (9:00 am to 5:00 pm, Monday through Thursday, 9:00 am to 7:00 pm Friday, and 10:00 am to 1:00 pm on Saturdays).

Step 5: Assess Risk to the Service

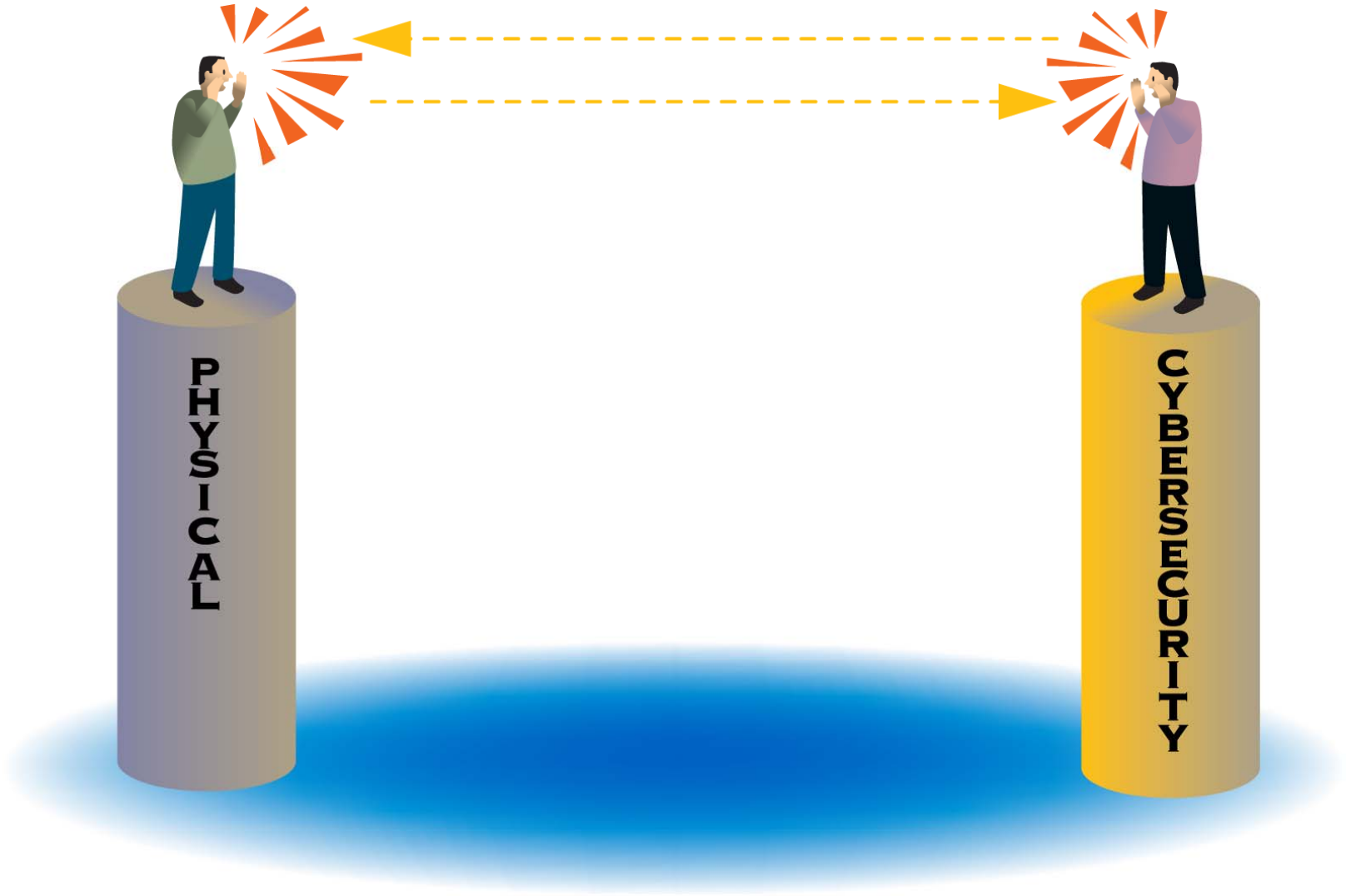
Risks to service delivery are what organizations need to care about

Identify how assets are exposed to conditions that can lead to service interruption

- Ensure that all possible vectors of threat are considered – both physical and cyber



Step 6: Develop an Integrated Mitigation Strategy



Step 7: Monitor for Change

Maintain vigilance in monitoring for changes in the operating environment.

- Ensure that changes do not introduce new risks.

Enterprise Perspective for Risk Management

1. Define enterprise services
2. Identify Impact Evaluation Criteria
3. Map assets to services
4. Define resiliency requirements for assets using the needs of the services
5. Assess risks to the reliable delivery of the service
6. Develop an integrated (using disciplines of physical and cyber security) approach effectively mitigate identified risks
7. Monitor for changes in the environment

Today's Agenda:

- Introduction
- Confluence of Physical and Cyber Security
- Risk Management Concepts
- Adopting a Service View
- A Service View for Critical Infrastructure
- Conclusion

Critical Infrastructure Protection

18 U.S. Critical Infrastructure Sectors Services

Agriculture and Food
Banking and Finance
Chemical
Commercial Facilities
Commercial Nuclear Reactors, Materials, and Waste
Dams
Defense industrial base
Drinking Water and Water Treatment Systems
Emergency Services
Energy
Government Facilities
Information Technology
Manufacturing
National Monuments and Icons
Postal and Shipping
Public Health and Healthcare
Telecommunications
Transportation Systems

Critical Infrastructure Asset Identification

Indiana	8,591
Wisconsin	7,146
New York	5,687
Virginia	4,231
Texas	3,804

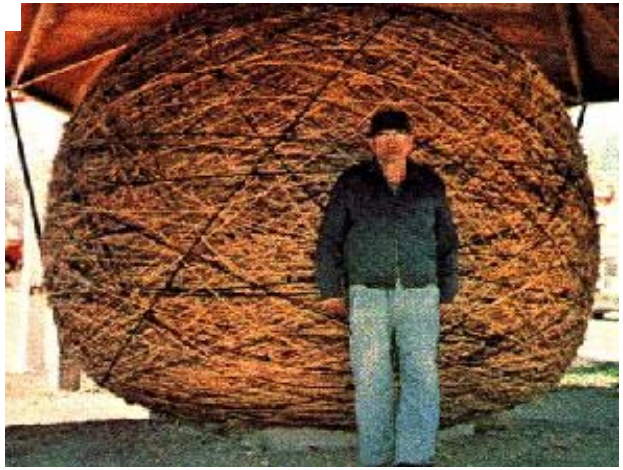
Odd priorities

States with the most 'critical' assets:

Source: Homeland Security Department's inspector general

By Julie Snider, USA TODAY

Old MacDonald's Petting Zoo, Alabama http://www.oldmacdonaldspettingzoo.com



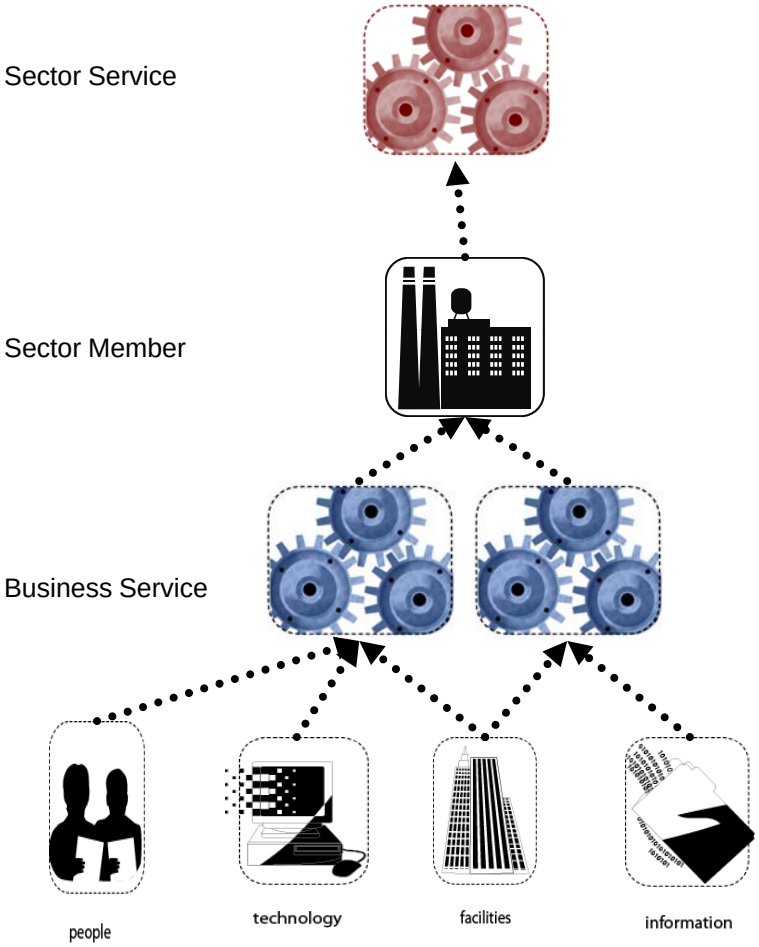
World's Largest Ball of Sisal Twine, Ks
http://skyways.lib.ks.us/towns/Cawker/twine.html

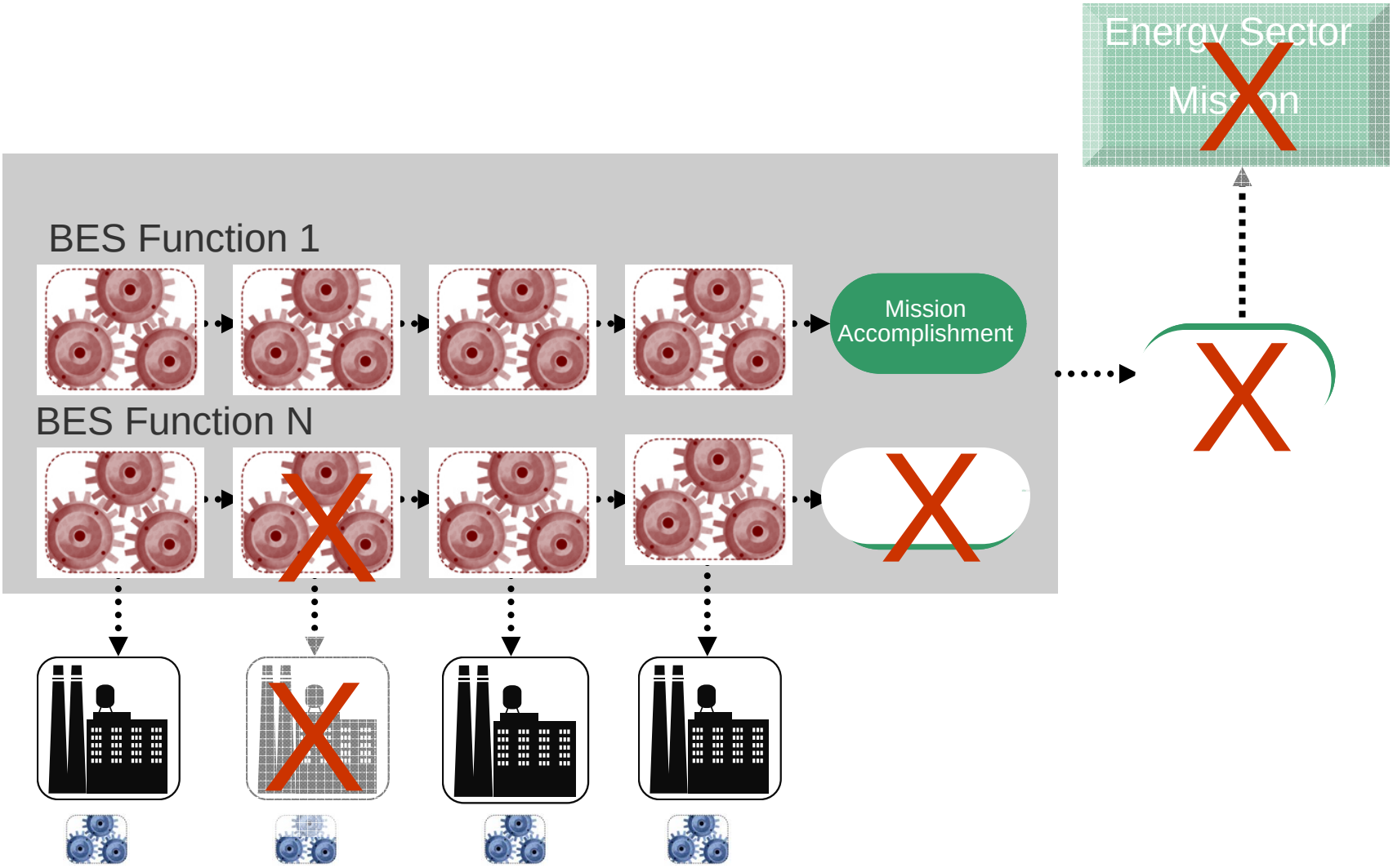
NERC's Struggle with Asset Identification

NERC's CIP standards

- NERC has robust physical security requirements
  - "N-1" and "N-1-1" contingencies
- Currently having difficulty in identifying critical infrastructure assets
  - Some BES organizations claim to operate no critical infrastructure

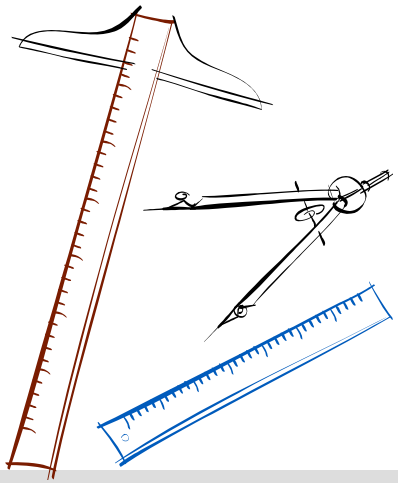
Managing Sector Risks




Energy Sector Mission
BES Function 1
Mission Accomplishment
BES Function N

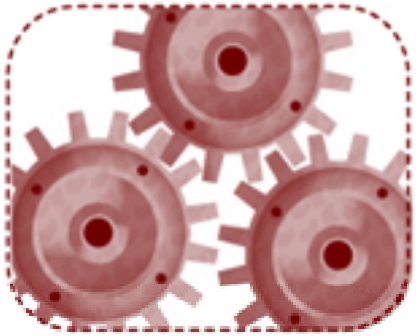
Benefits of Adopting a Service View

- Connect protection and sustainment strategies to the sector's mission
  - Risks can be defined in terms of service delivery
  - Impact evaluation criteria can be identified
- Physical and cyber protection strategies for assets can be engineered and evaluated in terms of their ability to best ensure the service

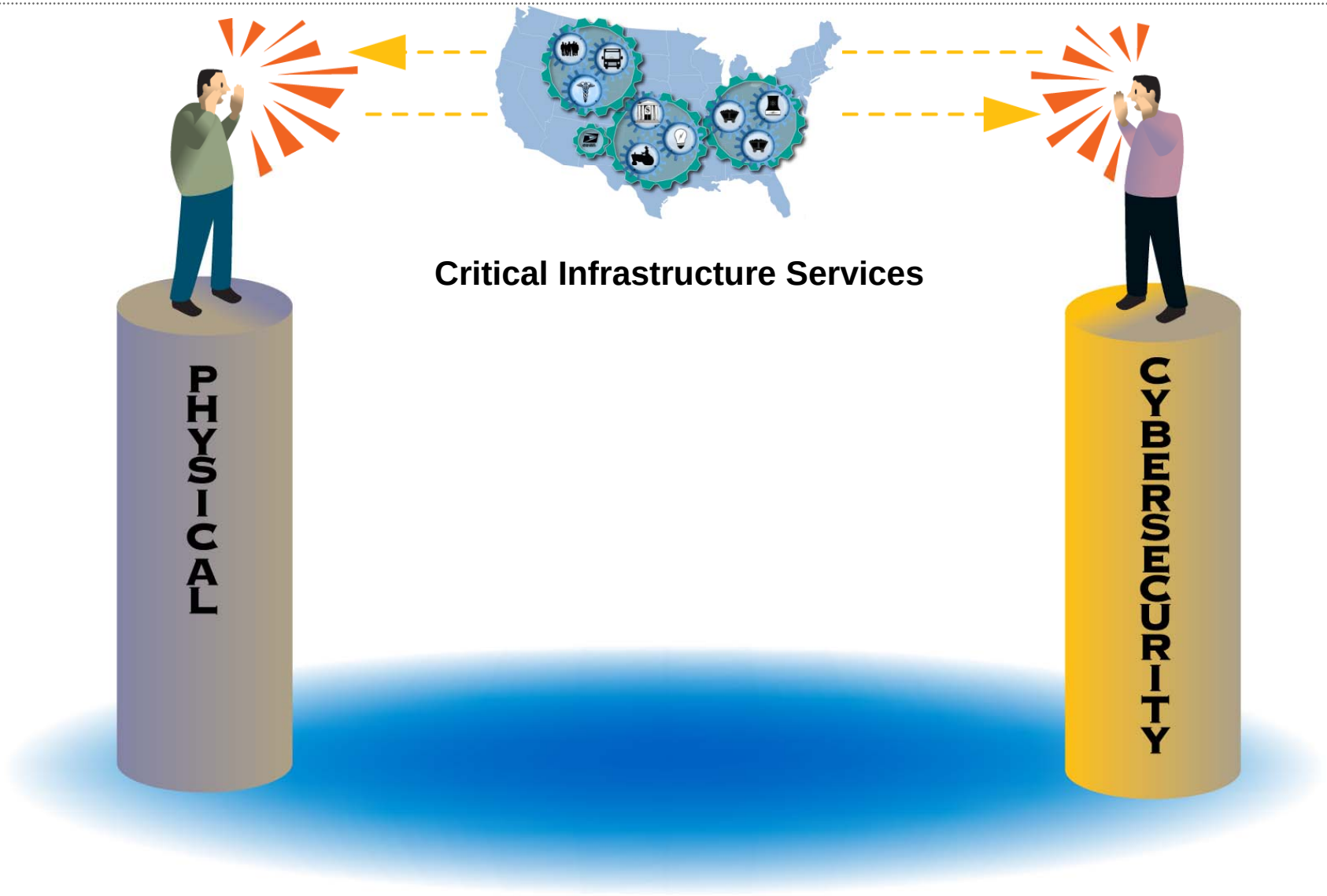


Connect to the Mission of the Sector

The requirements of the organization's contribution to the sector service are the basis for resiliency requirements for assets



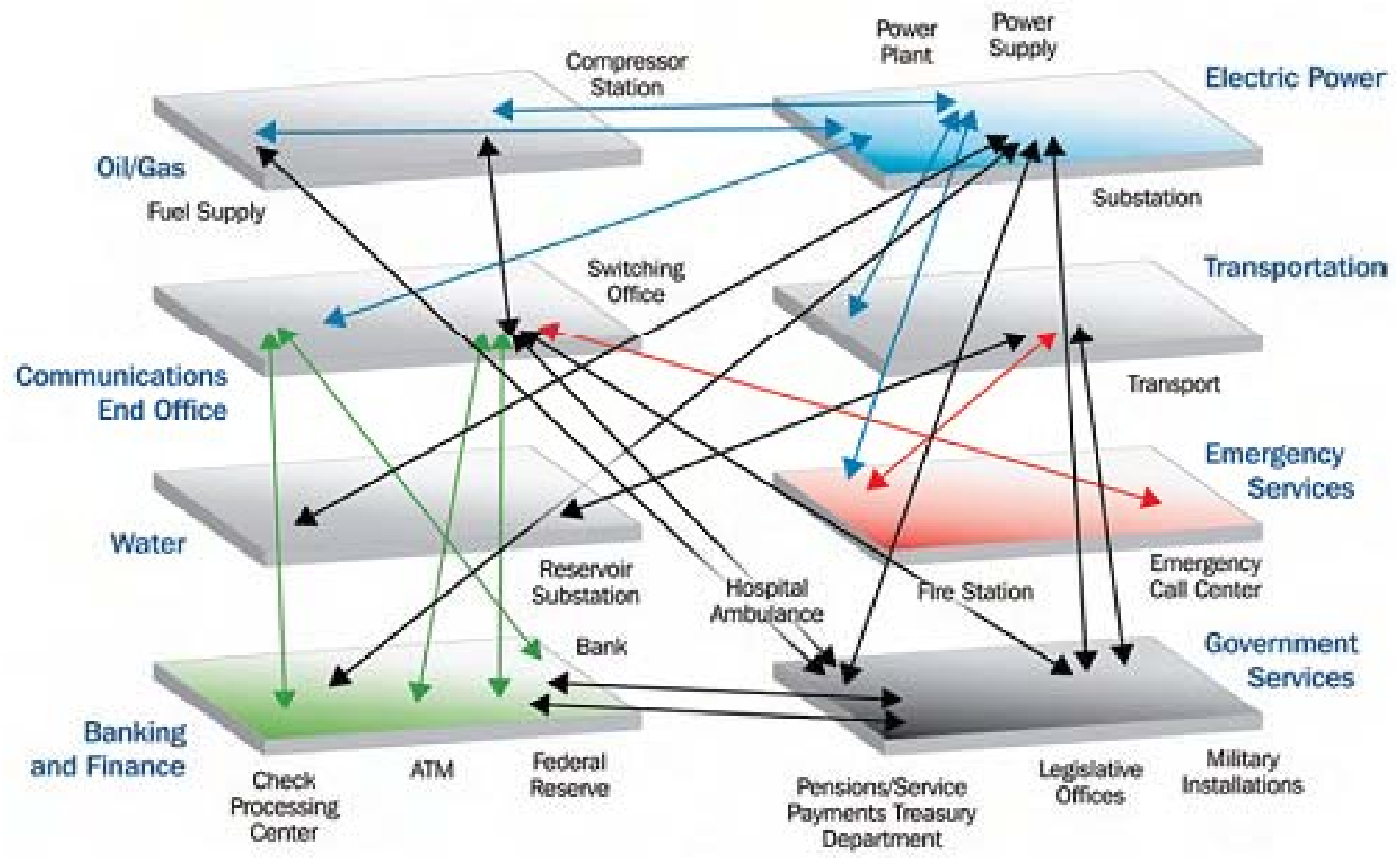
Select Effective Protection Strategies



Resiliency Requirements

- Connect requirements for Critical Infrastructure Services to a sector member's contribution to that service
- Establish service delivery requirements for that contribution
- Implement controls to effectively and efficiently meet the requirements.

Recognize Dependencies



http://science.nasa.gov/headlines/y2009/21jan_severespaceweather.htm

Critical Infrastructure Risk Management

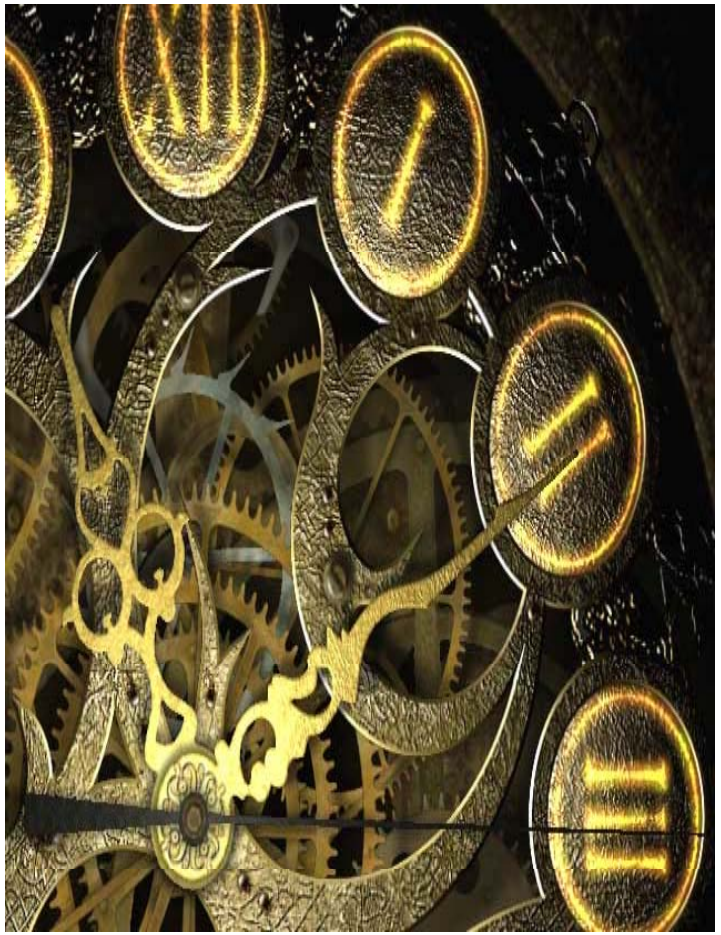
1. Define sector services
2. Identify service requirements
3. Map assets to how an organization contributes to sector services
4. Define resiliency requirements for assets using the needs of the services
5. Assess risks to the reliable delivery of the service
6. Engineer an integrated (using disciplines of physical and cyber security) approach effectively mitigate identified risks
7. Monitor for changes in the environment

Today's Agenda:

- Introduction
- Confluence of Physical and Cyber Security
- Risk Management Concepts
- Adopting a Service View
- A Service View for Critical Infrastructure
- Conclusion

Summary and Conclusion

- Adopt a structured approach to identify services
- Use business rules to define resiliency requirements
- Assess risks to assets that will affect reliable service delivery
- Engineer protection strategies to ensure infrastructure resiliency
- Continuously monitor for changes



http://www.3planesoft.com/img/clock_screen01.jpg

CERT® Resiliency Management Model

http://www.cert.org/resiliency

The CERT Resiliency Management Model is a capability model for operational resiliency management. It has two primary objectives:

- Establish the convergence of operational risk and resiliency management activities such as security, business continuity, and aspects of IT operations management into a single model.
- Apply a process improvement approach to operational resiliency management through the definition and application of a capability level scale that expresses increasing levels of process improvement.

Contact Us

Contact Information

Speakers
Samuel Merrell
e-mail: **smerrell@cert.org**

James Stevens
e-mail: **jfs@cert.org**

Phone
412-268-5800
(8:30 a.m. - 4:30 p.m. EST)

Web
http://www.cert.org

Postal Mail
Software Engineering Institute
ATTN: Customer Relations
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Questions?

Notices