Federal Information Systems Security Educators Association

I Touch the Future, I Teach.

Crista McAuliffe

A Product of the

National Information Assurance
Training and Education Center

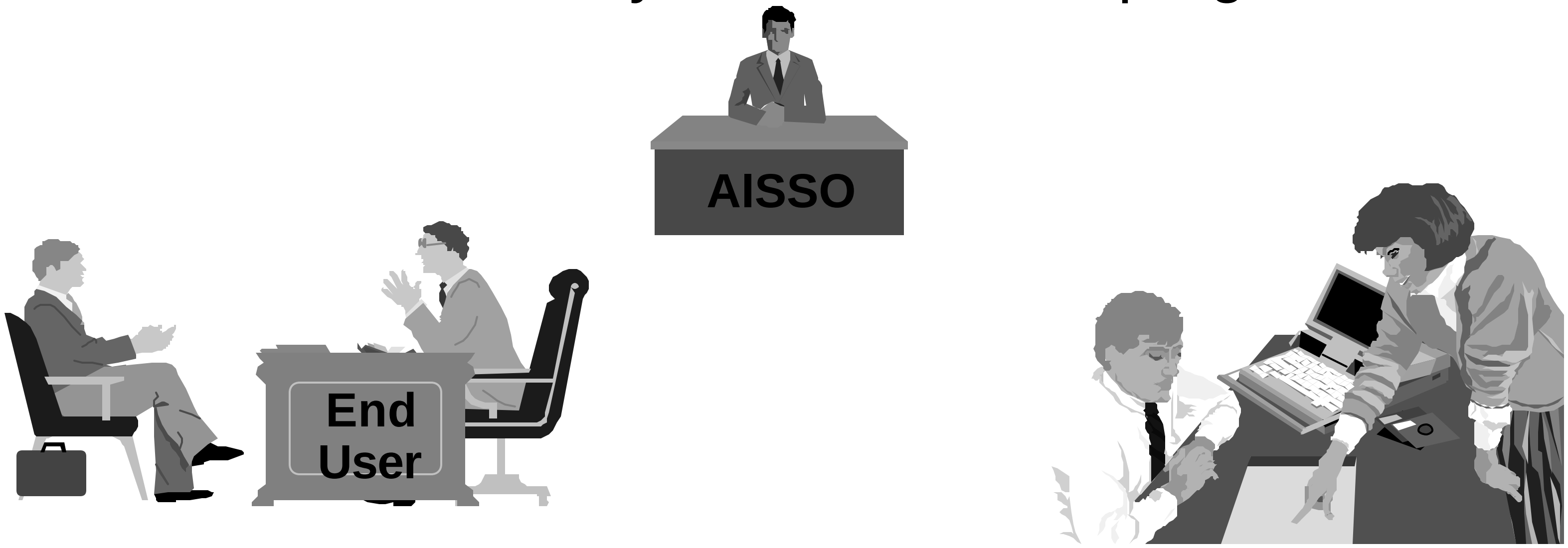
Idaho State University

Computer Security

A Program for Federal Government *Functional Managers*

Computer Security Is Everyone’s Responsibility

Cooperation and support from all personnel is an essential key to a successful program



AISSO

End User

End User Supervisor

FACT 1

COMPUTERS ARE CRITICAL TO FULFILL YOUR AGENCY MISSION!

FACT 2

THERE ARE DEFINED THREATS TO YOUR COMPUTER SYSTEM!

FACT 3

COMPUTER SYSTEMS ARE VULNERABLE!

FACT 4

COMPUTER SECURITY IS ESSENTIAL TO PROTECT YOUR SENSITIVE AND CLASSIFIED INFORMATION!

FACT 5

COMPUTER SECURITY AWARENESS AND TRAINING PROGRAMS REDUCE RISK!

Management Responsibility

- Set Standards
- Assure User Training
- Develop Policies & Procedures
- Provide Knowledge/Enforce Regulations
- Provide Assistance
- Supervise
- Set the Example

FIRST LINE SUPERVISOR'S RESPONSIBILITIES

- Set a personal example while carrying out computer security policies and procedures.
- Provide computer security orientation/awareness to employees.
- Provide input to the AIS Security Plan.
- Review audit logs periodically.
- Provide password management and system access control for employees.
- Identify mission critical AISs/networks.
- Report security violations and incidents.
- Support and promote good security practices.

Definitions

- INFOSEC
- COMSEC
- COMPUSEC

INFOSEC Concerns

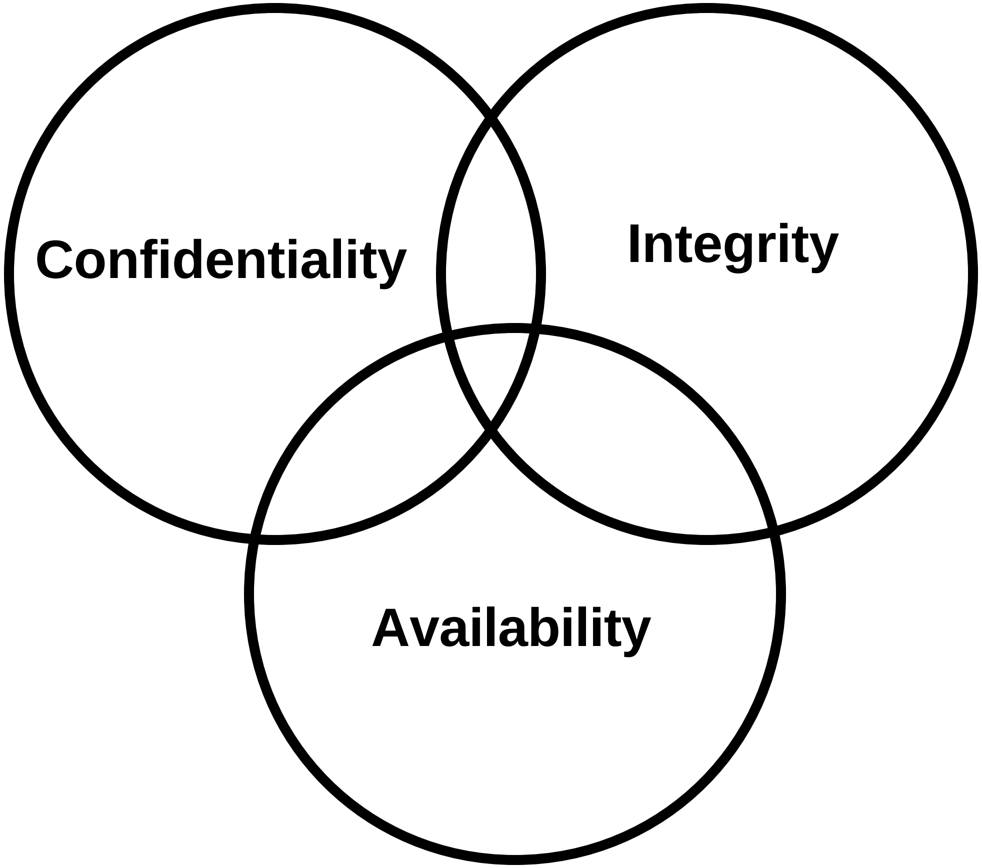
- Compromise
- Integrity

More Definitions

- Sensitive Information
- Confidentiality
- Integrity
  - Store
  - Process
  - Transmit

Current Issues

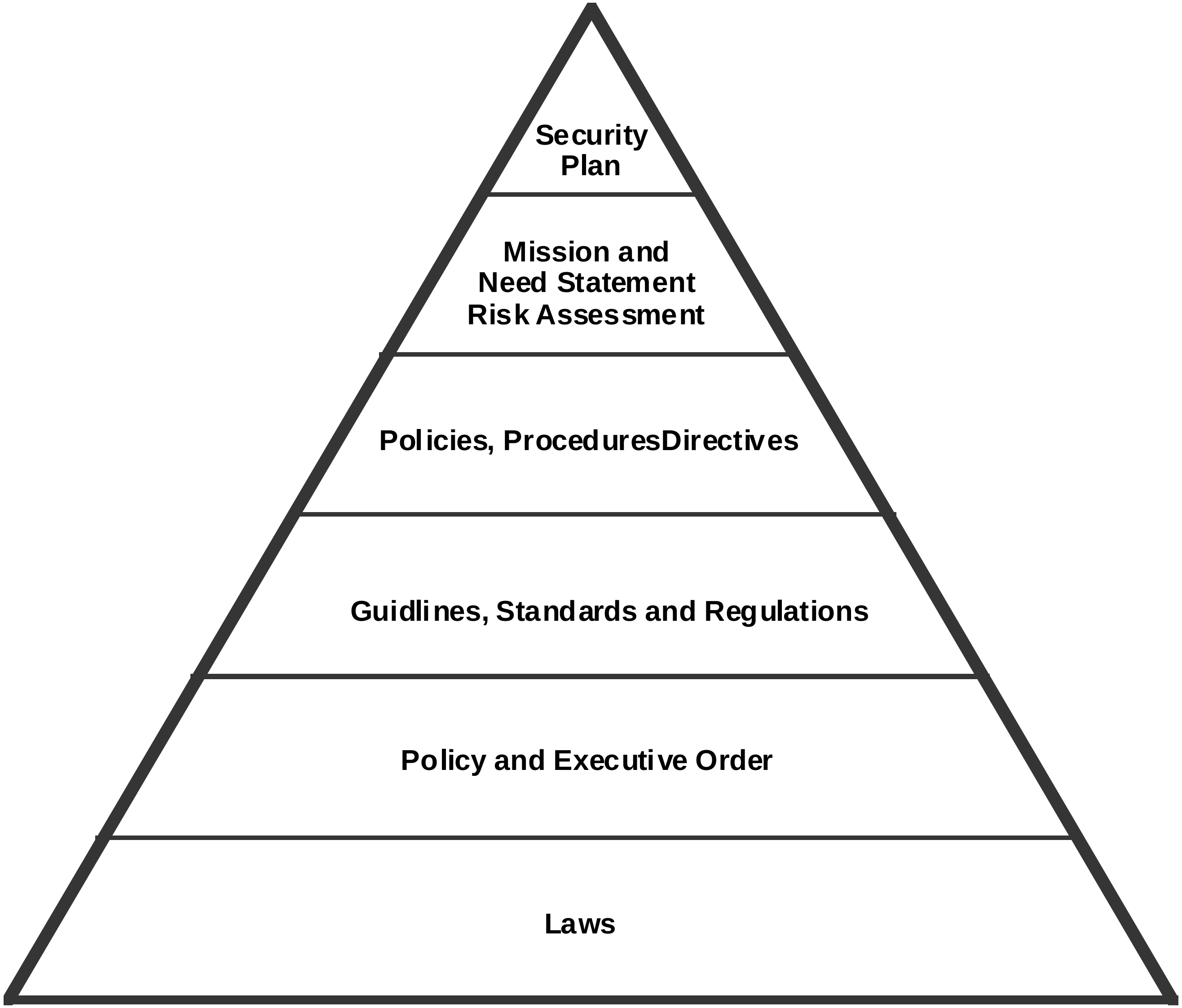
Confidentiality, Integrity, Availability



Organizational Impact

- Compromise of Data
- Loss of Confidence in System
- Loss of Money
- Loss of Time
- Repair or Replacement of Equipment

Policy Pyramid



Security Plan

Mission and Need Statement Risk Assessment

Policies, ProceduresDirectives

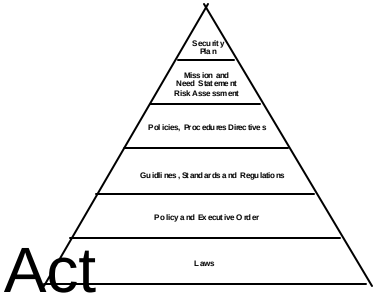
Guidlines, Standards and Regulations

Policy and Executive Order

Laws

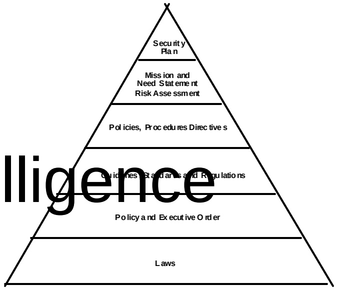
Applicable Computer Security Statutes

- Public Law 97-255
  - Federal Managers Financial Integrity Act of 1987
- Public Law 98-473
  - Comprehensive Crime Control Act of 1984
- Public Law 99-474
  - Computer Fraud and Abuse Act
- Public Law 99-508
  - Interception or Disclosure of Wire, Oral or electronic Communications
- Public Law 100-235
  - Computer Security Act of 1987
- Public Law 100-503
  - Computer Matching and Privacy Protection Act


Security Plan
Mission and Need Statement Risk Assessment
Policies, Procedures Directives
Guidlines, Standards and Regulations
Policy and Executive Order
Laws

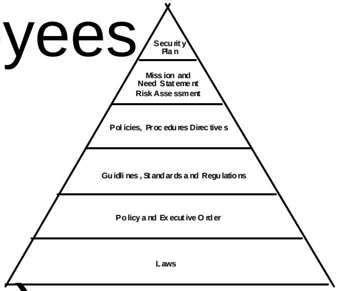
Applicable Policy and Executive Orders

- OMB Circular A-130
  - Management of Federal Information Resources
- OMB Circular A-123 & 127
  - Internal Control/Financial Management Systems
- OMB Bulletin 89-22
  - Computer Matching and Privacy
- OMB Bulletin 90-08
  - Agency Security Plans
- Executive Order 12333
  - United States Intelligence Activities
- Executive Order 12356
  - National Security Information
- DCI Directive 1/16
  - Security Policy for Uniform Protection of Intelligence Processed in AIS's and Networks


Security Plan
Mission and Need Statement Risk Assessment
Policies, Procedures Directives
Guidelines, Standards and Regulations
Policy and Executive Order
Laws

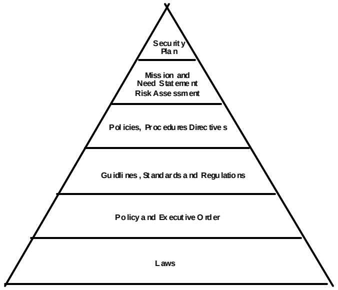
Guidelines

- National Institute of Standards and Technology (NIST)
  - Technical Publications, Training Assistance and Newsletter
- National Computer Security Center (NCSC)
  - Rainbow Series, Technical Reports
- Office of Personnel Management (OPM)
  - Training Requirements for all USG Employees
- Government Accounting Office (GAO)
  - Reports on AIS Deficiencies
- General Services Administration (GSA)
  - Provides Training Services for Users


Security Plan
Mission and Need Statement Risk Assessment
Policies, Procedures Directives
Guidlines, Standards and Regulations
Policy and Executive Order
Laws

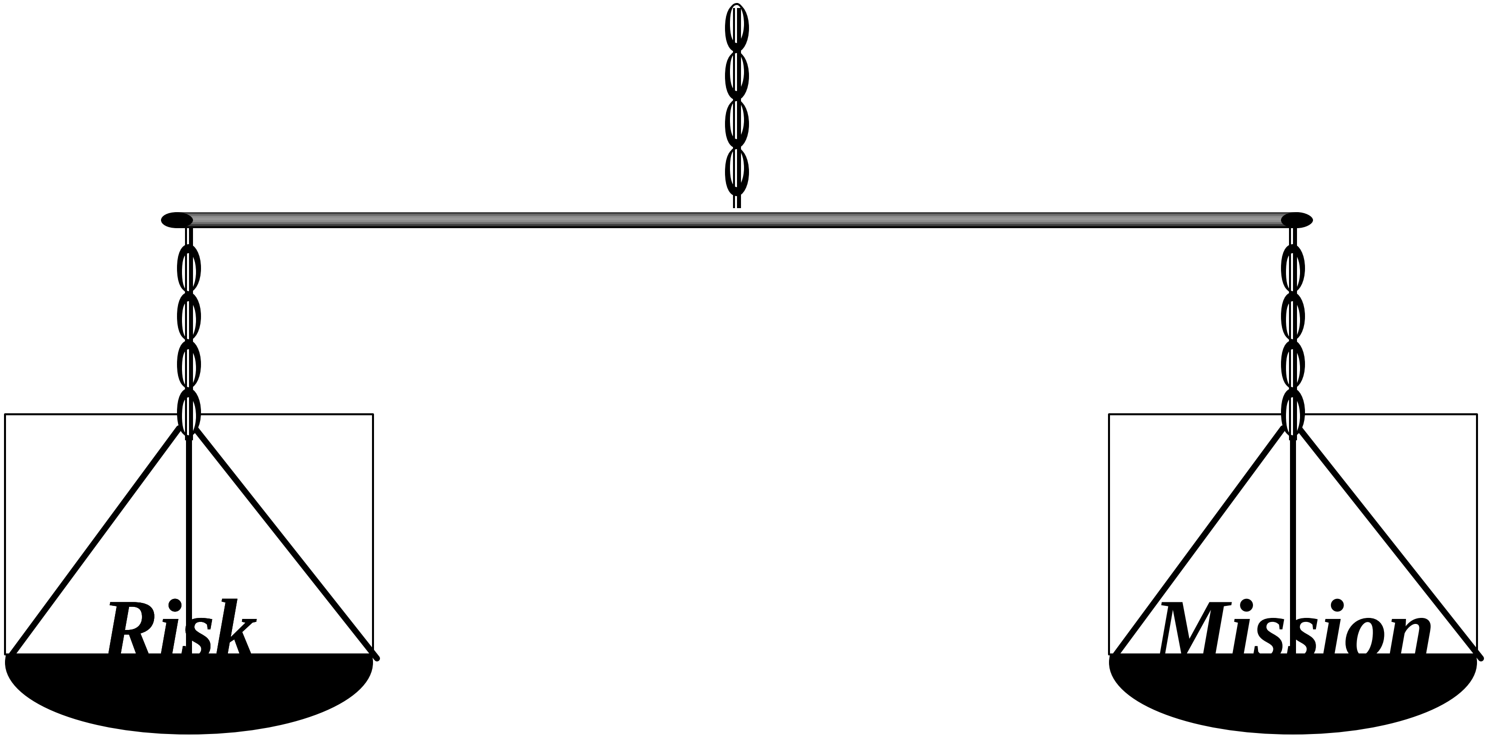
Agency and System Documentation

- Policies, Procedures, Guidelines
- Obtain These From Your Federal Agency
  - These are Agency-wide Computer Documents
  - They Will be Specific to Your Organization


Security Plan
Mission and Need Statement Risk Assessment
Policies, Procedures Directives
Guidlines, Standards and Regulations
Policy and Executive Order
Laws

Risk Management

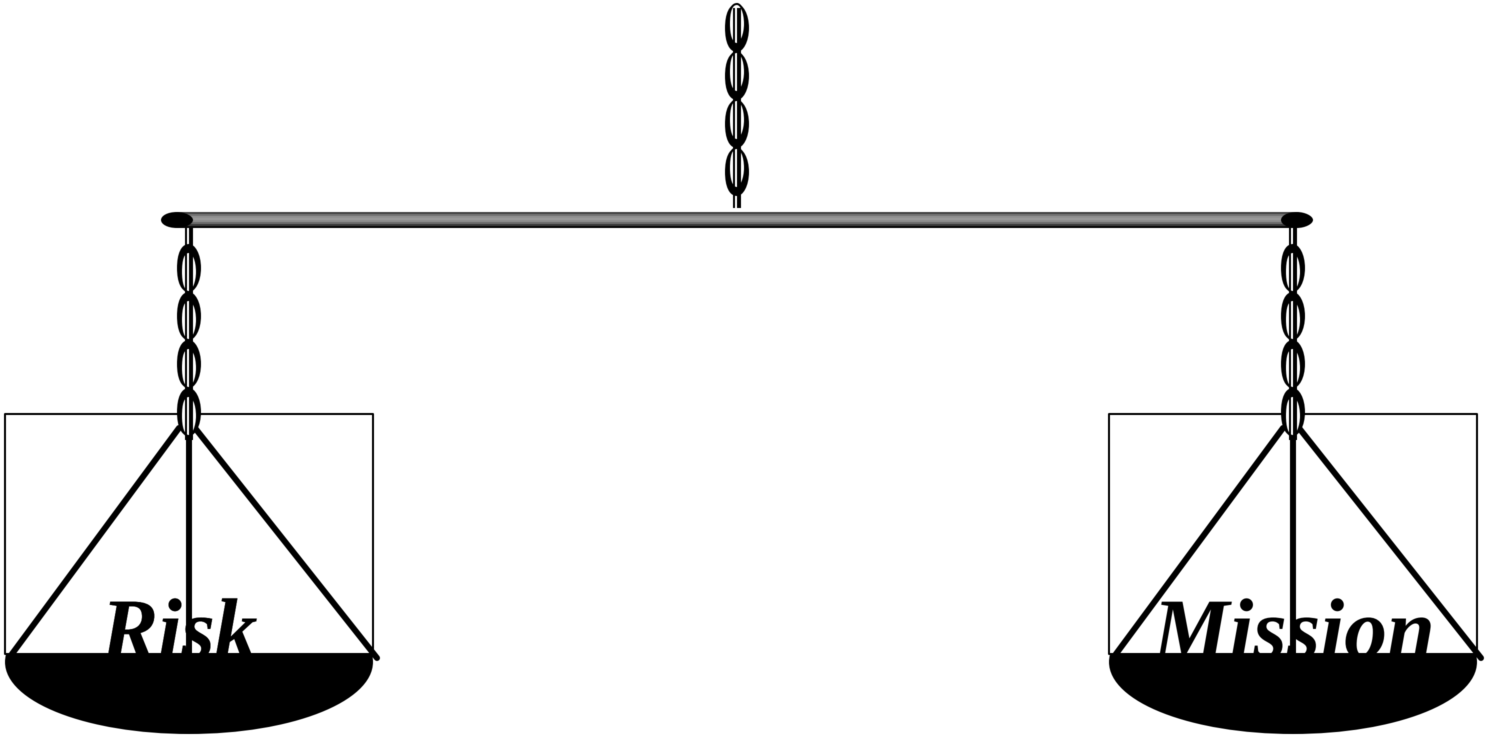
INFOSEC IS BASED ON RISK
“You Cannot Protect Everything From Everybody



Risk = *Threat* X *Vulnerability* — *Security*

Computer Security

The Key Question
“How Much”



The Balancing Act

Risk Management

- Risk Management is:
  - A systematic method to analyze security risks and bring in cost effective safeguards to reduce risk
  - Cost-benefit: Have to "sell" it to management
  - Risk Management in simpler terms:
    - 1. Decide what you need to protect.
    - 2. Decide what you need to protect it from.
    - 3. Decide how to protect it.

Steps In Risk Management Process

- Form a risk management team
  - One from EDP/ADP/IRM/etc.
  - User who knows what they can lose
  - Could be formal or informal
  - Depends on size of organization
- Identify and value the assets
- Identify potential threats (what could happen)
- Determine likelihood of occurrence of threats
- Calculate the exposures (the vulnerable areas and their values)
- Introduce safeguards
  - for largest exposure first
  - only when benefit exceeds cost

TREATS TO COMPUTER SYSTEMS

- Threats By People
  - Unintentional Employee Action 50-60%
  - Intentional Employee Action 15-20%
  - Outside Actions 1- 3%

- Physical & Environmental Threats
  - Fire Damage 10-15%
  - Water Damage 5-10%
  - Electrical Fluctuations
  - Other 5-10%

Technical Vulnerabilities

- Trap Door
- Time Bomb
- Trojan Horse
- Mouse Trap
- Virus

PC Vulnerabilities

- Population Increasing
- Portability
- Physical Accessibility
- Lack of Built-in Security
- Multiple Operators
- Nature of Data Handled
- Compactness of media
- User Education
- Local Area Networks
- Growth of Computer Crime
- Virus Infections
- Mechanisms

Hardware Concerns

- Access
- Theft
- Environmental considerations
- Media protection
- Media declassification/destruction
- Lack of built in security mechanisms
- Electromagnetic emanations (TEMPEST)
- Hardware modifications
- Hardware attacks

Software Concerns

- Viruses, unauthorized changes to programming code, backups not made, program errors
- Errors, inadequacies, backup system software
- Software not inventoried or controlled, Software Publisher's Association
- Worms along network - Morris/Cornell/INTERNET case
- Check all disks before using. Use of scanner or detector
- Problem of correct software use

Computer Viruses

- Self Propagating Routine That Can Have Destructive Properties

Sources of Virus Infection

- Bulletin boards
- Pirated software
- Shareware
- Public domain software
- Commercial software packages
- Networks
- Sabotage by employees, terrorists, crackers, or spies

Preventing Virus Infections

- Boot floppy based systems using a specific clearly labeled boot diskette
- Never boot a hard disk system from an unprotected diskette
- Never use untested software (test off line or on a single purpose dedicated system)
- Backup files and programs, securely store and routinely check for infection
- Minimize software sharing within the organization
- Prohibit use of unapproved software from any source
- Educate users to watch for changes in patterns of system activity
- Install virus detection software

Data Concerns

- Boot floppy based systems using a specific clearly labeled boot diskette
- Never boot a hard disk system from an unprotected diskette
- Never use untested software (test off line or on a single purpose dedicated system)
- Backup files and programs, securely store and routinely check for infection
- Minimize software sharing within the organization
- Prohibit use of unapproved software from any source
- Educate users to watch for changes in patterns of system activity
- Install virus detection software

Levels of Data

- DoD
  - Level I - Classified
  - Level II - Unclassified Sensitive
  - Level III - Unclassified
- Civilian Agencies
  - Level 1 - Low Sensitivity/Criticality
  - Level 2 - Medium Sensitivity/Criticality
  - Level 3 - High Sensitivity/Criticality - confidential
  - Level 4 - Extremely High Sensitivity/Criticality & Classified

Applying Common Sense

- Sophisticated security systems can fail if common sense is not used.
- Examples:
  - Fancy lock on computer room door, door propped open
  - List of instructions not secure
  - User ID, password taped to monitor
  - Password obvious (for example, person's name)
  - References not checked when hiring
  - Confidential diskettes left out in open

- APPLYING COMMON SENSE COSTS

Penetration and Countermeasure

- Access sensitive information
  - Encryption
- Features not used
  - Implement protection
- Implied Sharing Capabilities
  - Parameters Check user supplied
- Line disconnect
  - Hang up

- Carelessness Employee
  - Training
- Passwords
  - Proper Management
- Repetition
  - Hang up & Notify
- Leakage
  - Shielding, Encryption
- Waste
  - Destroy

Passwords

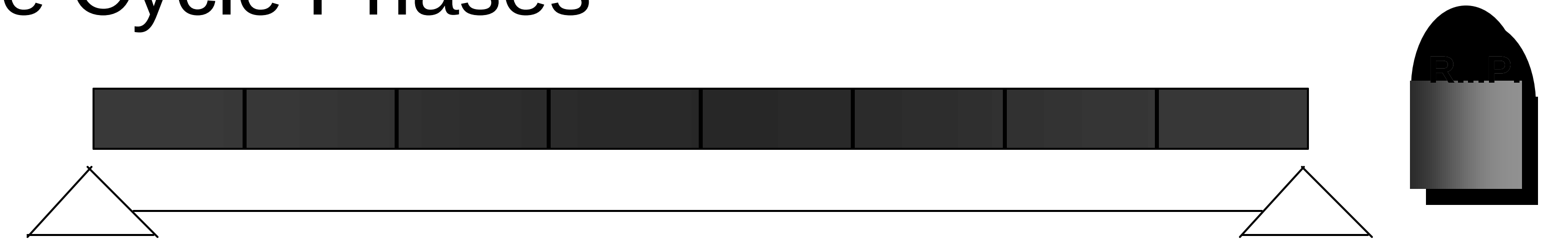
- The Use of Passwords Should Follow These Guidelines
- No repeat guesses
- Log unsuccessful attempts
- Review log
- Never write down sensitive combinations
- Hard to guess passwords
- Change frequently
- Easy to recall, hard to guess
- Don't disclose

Physical Access Controls

- Restricted access
- Signs, locked doors, etc.
- Solid doors
- ID cards and badges
- Computer controlled access cards
- Access log
- Closed-circuit TV
- Procedures re: unauthorized person

INFOSEC Life Cycle Management

- Life Cycle Phases



Design and Development

Fabrication and Production

AcquisitionTest and Evaluation

Shipping and Delivery

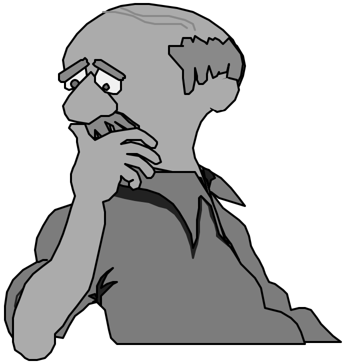
Operations

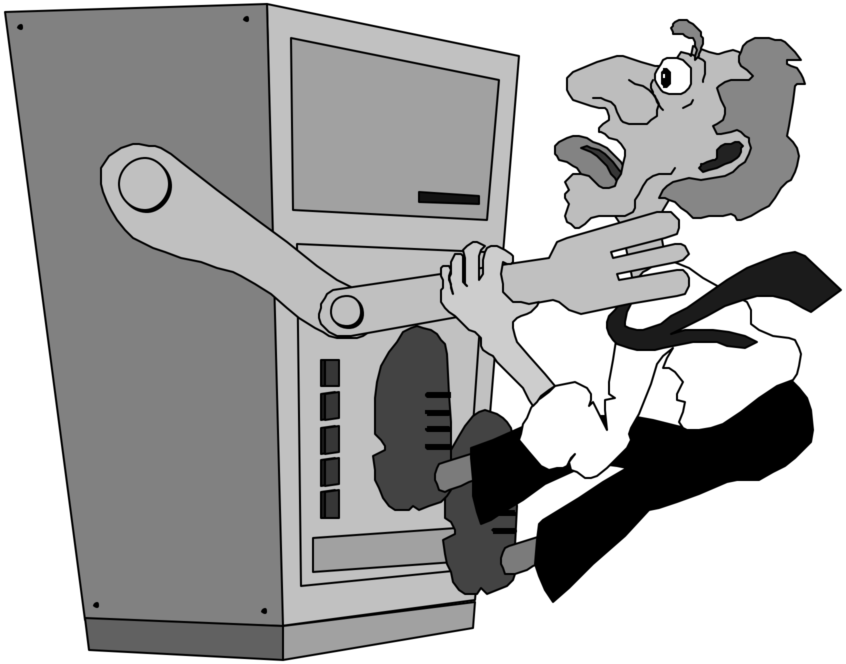
Maintenance

Obsolescence and Removal

Disaster Recovery

PRIOR PLANNING PREVENTS POOR PERFORMANCE





Contingency Planning

- Three major topics in contingency planning
- Backups and Procedures
  - How often?
  - Backup what?
- Catastrophe Planning
  - Making the plan
  - Disaster stages
  - Contents of plan
- Security in Backup

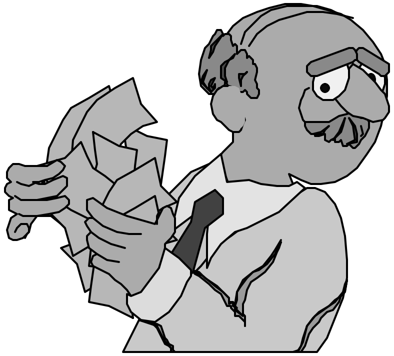
Items in Contingency Plan

- Emergency Response Team List
- Secure Storage Site
- Complete Archive Backup
- Current Complete Backup
- Current Incremental Data Backups
- Hardware Backups and Tests
- TESTING
- Insurance and Financial Matters

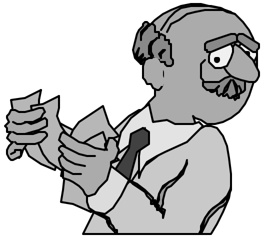
Resources and $$$

Our Security Mission Still Must Be Met With Ever Decreasing Budgets

Today

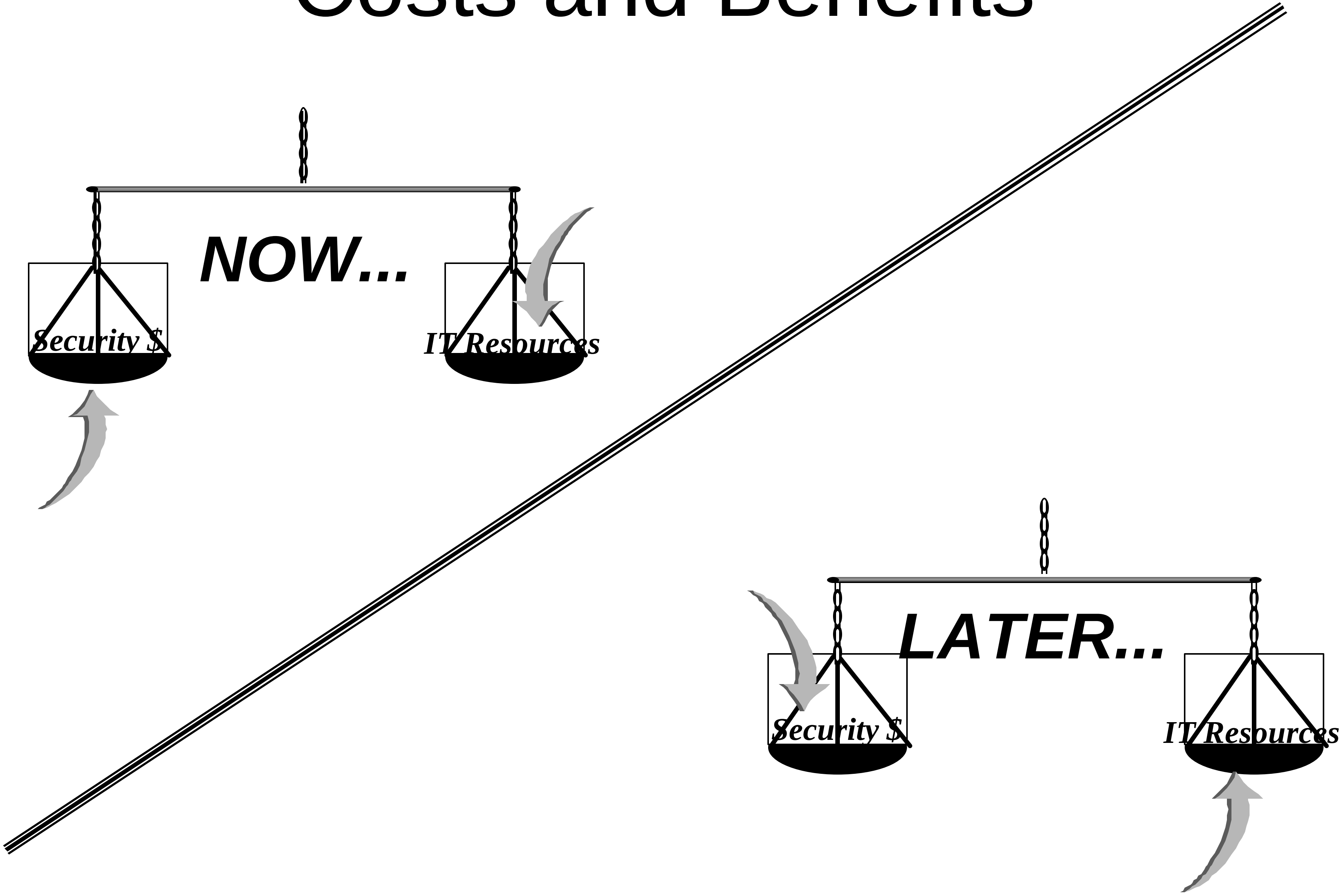


Tomorrow



Next Year

Costs and Benefits



NOW...

Security $

IT Resources

LATER...

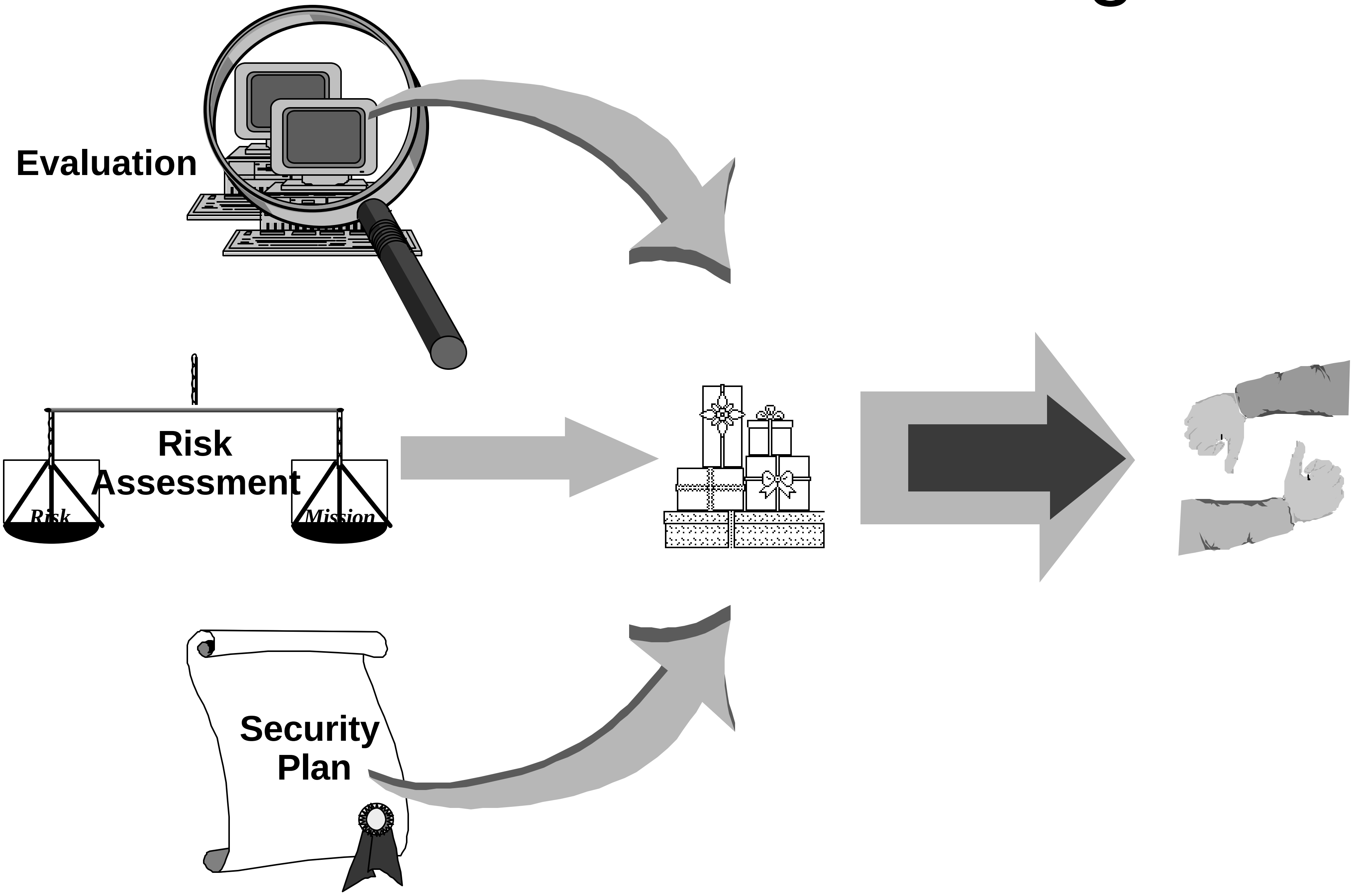
Security $

IT Resources

AIS Accreditation

- Supported by:
  - Certification
  - Risk Management Process
- Reviewed every three years or upon major modification

The Certification Package



Evaluation

Risk Assessment

Security Plan

Why Use a LAN

- Cost
- Reliability
- Distribution of Work
- Expendability
- Flexibility

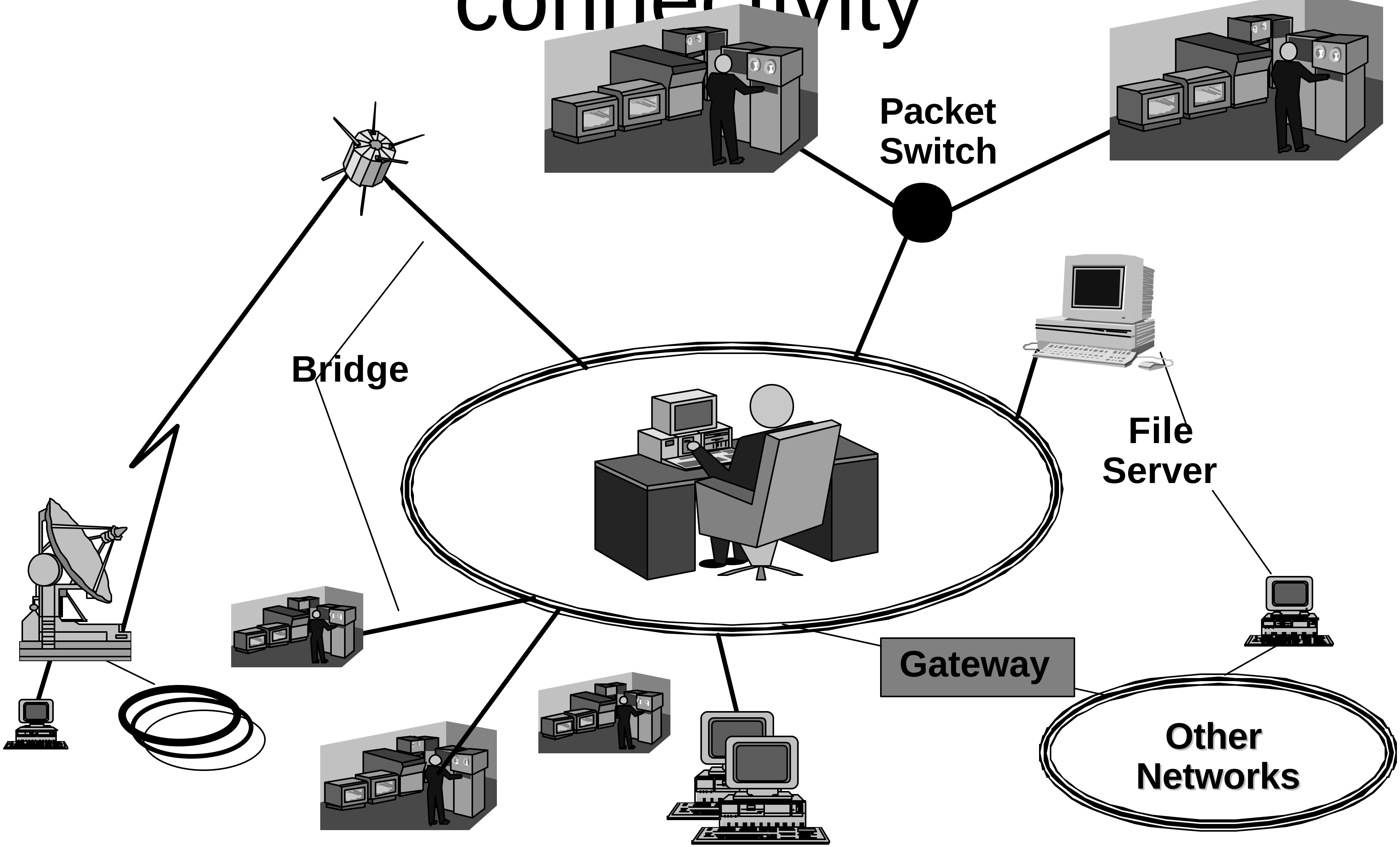
Metropolitan Area Network (MAN)

- Moves Information Between Buildings
- Also Called a “Campus Network”

Wide Area Network (WAN)

- An Integrated Voice/Data Network Which Links Metropolitan Networks
- Often Uses Established Common-Carrier Lines

Putting It Together Inter-connectivity



Network Vulnerabilities

- Access by unauthorized individuals
- Lack of physical control
- General lack of monitoring/auditing features
- Identification and control of dial-in-users
- Failure to backup critical data
- Sensitive to outside interference
- Virus infection

Role of Systems Security Officer (SSO)

- Administer the data security function
- Give service to management to make proper security easy
- In small environment, system manager may do the SSO duties
- Important to designate someone as being responsible and accountable for security and control