Security Briefing

National Information Assurance Training and Education Center
Idaho State University

Corey D. Schou

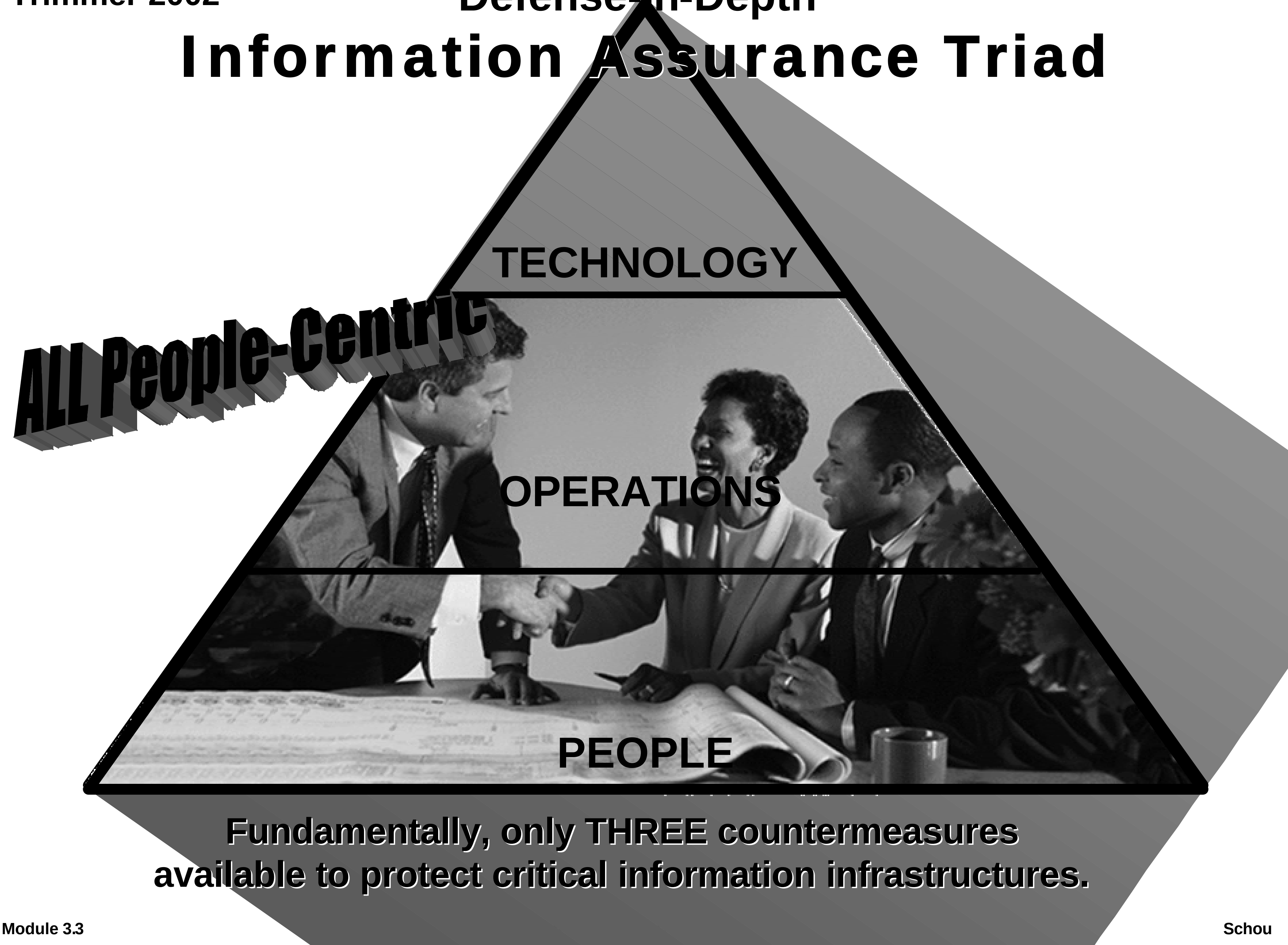
April 16 2002

Information Assurance

General Program Information

Trimmer 2002

Defense-In-Depth
Information Assurance Triad



Fundamentally, only THREE countermeasures available to protect critical information infrastructures.

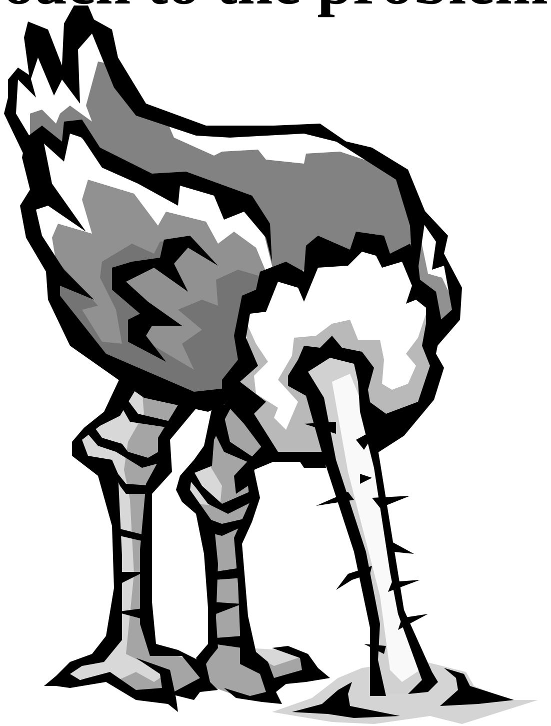
The Threat

“The greatest threat you face is not the viruses or the hackers or the whatever, but rather complacency.”

Michael Tucker, Editor, SC Magazine, Sep 99

There is nothing to worry about

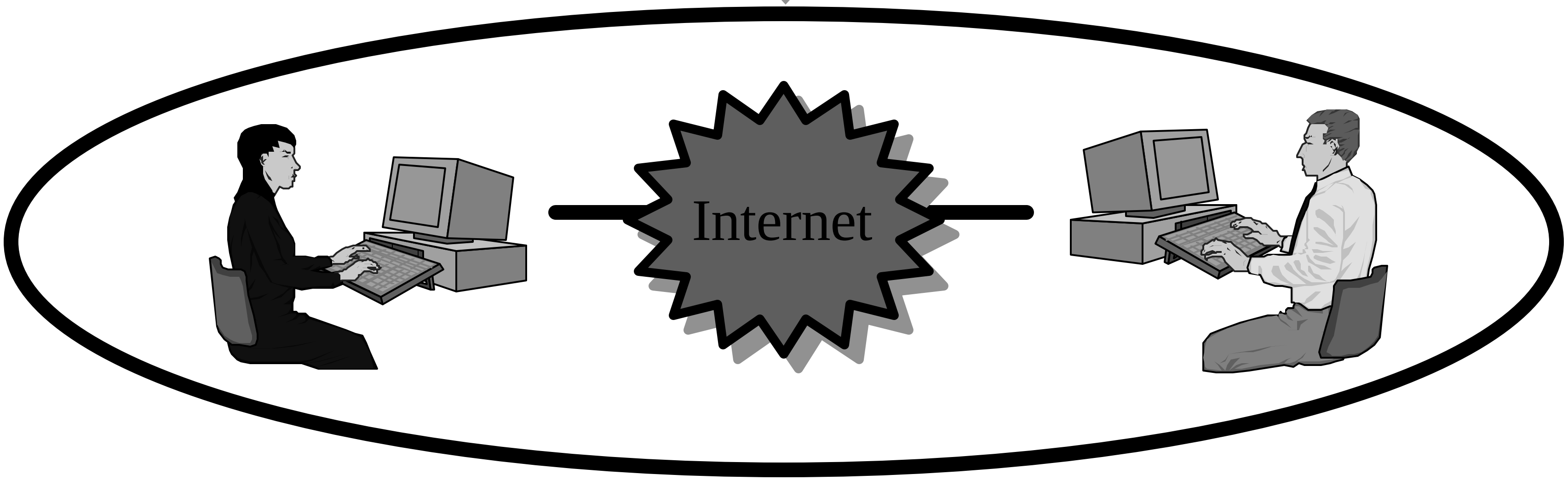
- **This is one approach to the problem**

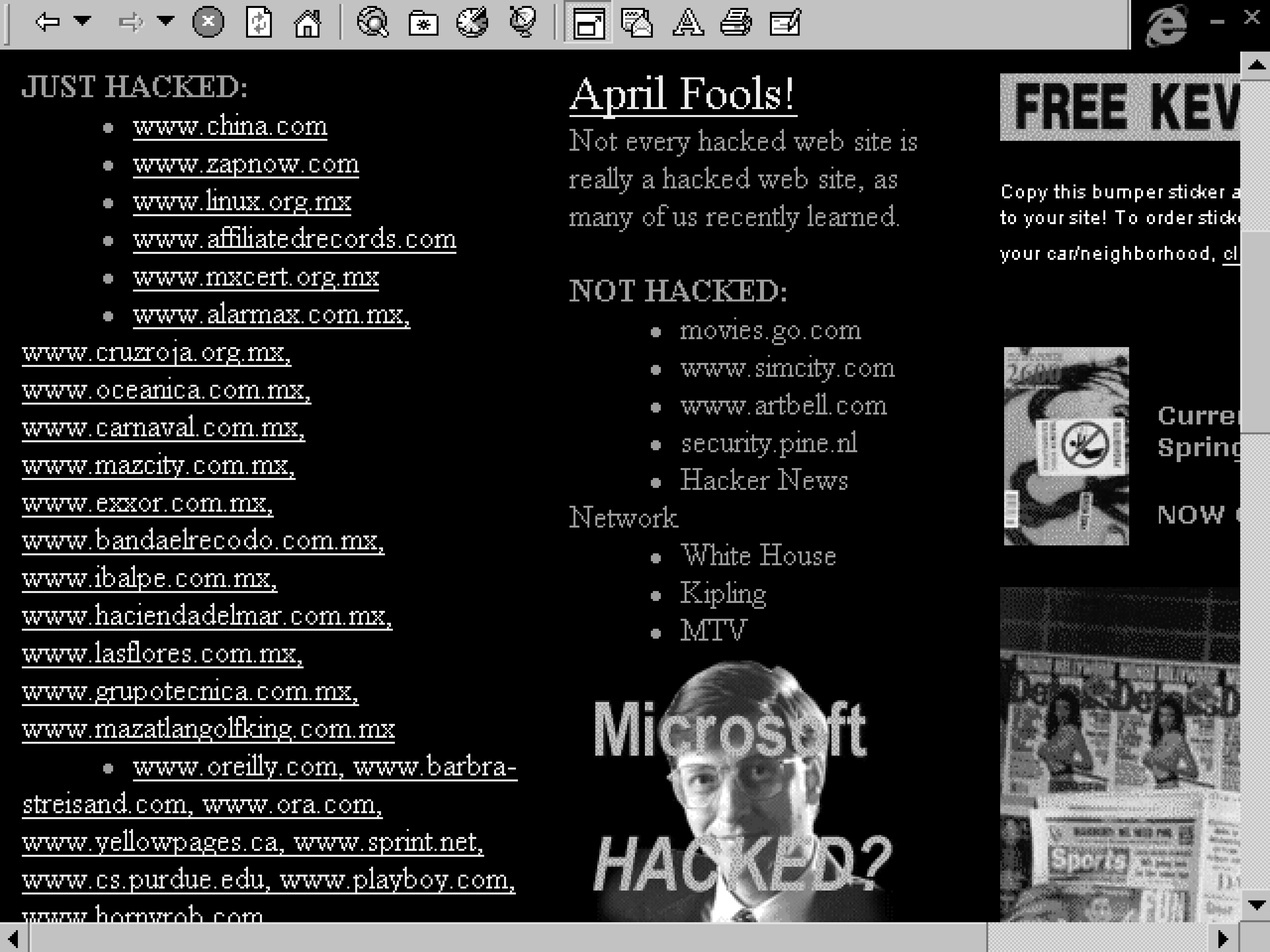


Where are
Computer Systems Vulnerable?

1. Hardware
2. Software
3. Data
4. Communications
5. PEOPLE

Here





JUST HACKED:

- www.china.com
- www.zapnow.com
- www.linux.org.mx
- www.affiliatedrecords.com
- www.mxcert.org.mx
- www.alarmax.com.mx, www.cruzroja.org.mx, www.oceanica.com.mx, www.carnaval.com.mx, www.mazcity.com.mx, www.exxor.com.mx, www.bandaelrecodo.com.mx, www.ibalpe.com.mx, www.haciendadelmar.com.mx, www.lasflores.com.mx, www.grupotecnica.com.mx, www.mazatlangolfking.com.mx
- www.oreilly.com, www.barbra-streisand.com, www.ora.com, www.yellowpages.ca, www.sprint.net, www.cs.purdue.edu, www.playboy.com, www.hornyrob.com

April Fools!

Not every hacked web site is really a hacked web site, as many of us recently learned.

NOT HACKED:

- movies.go.com
- www.simcity.com
- www.artbell.com
- security.pine.nl
- Hacker News Network
- White House
- Kipling
- MTV

Copy this bumper sticker a
to your site! To order stick
your car/neighborhood, cl

Curre
Spring

NOW c

Good News

Sound Management

Risk Management

Awareness

Training

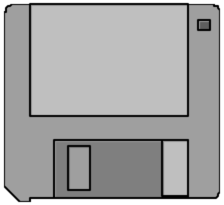
Education

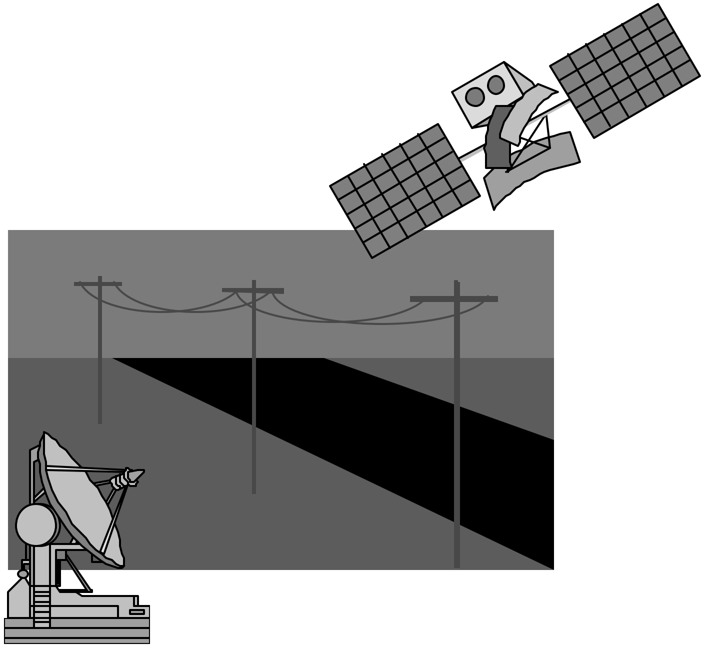
Good Practices

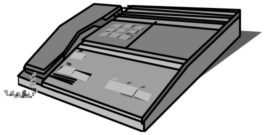
All Address The Problem

They Are Effective Countermeasures

Information Technology Security Is Everyone’s Responsibility





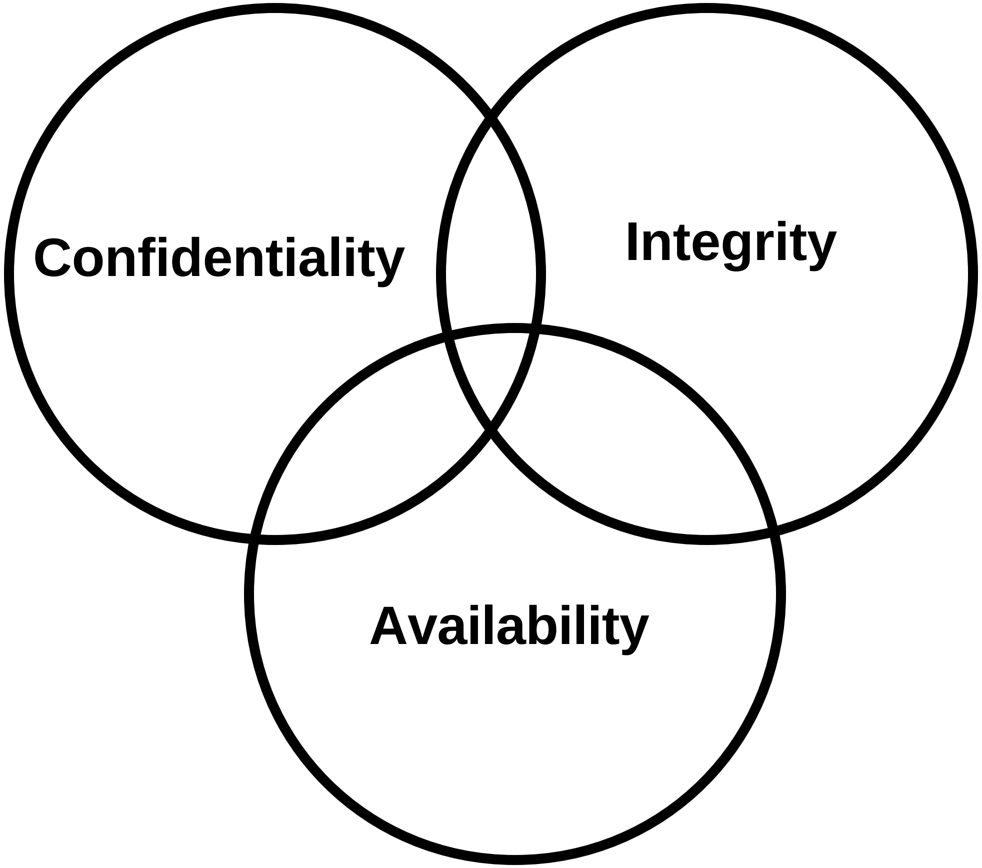


Trimmer 2002

The Question Is:

- What is Information Technology Security
- Why should you care?
- Who is responsible
- How do you get there

What Is
Information Technology Security?



FACT 1

- **COMPUTERS ARE CRITICAL TO FULFILL YOUR AGENCY MISSION!**

Oil & gas delivery & storage

Telecommunications

Electric power

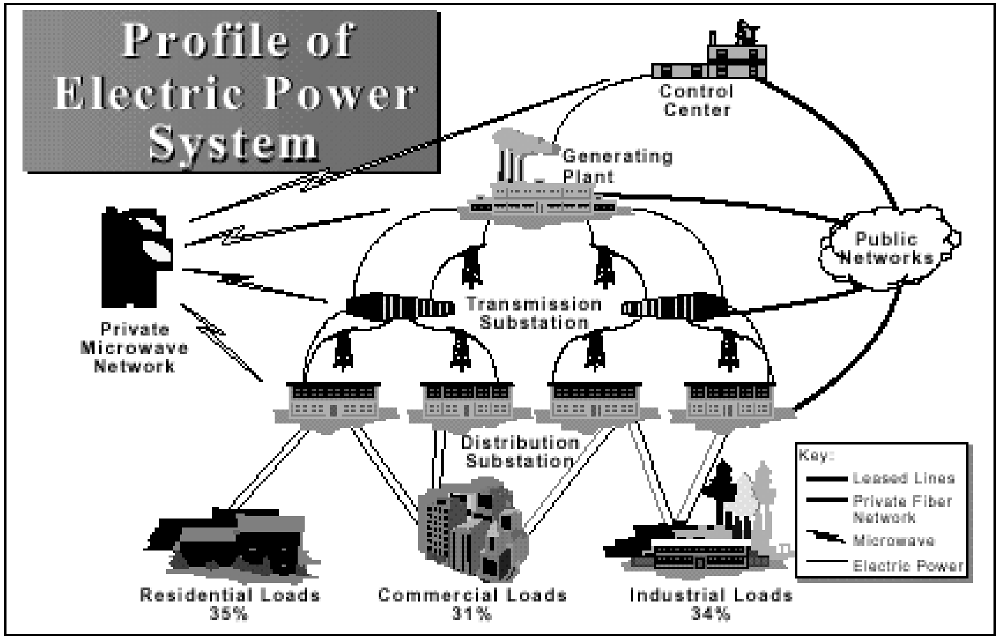
Transportation

Banking & finance

Water

Emergency services

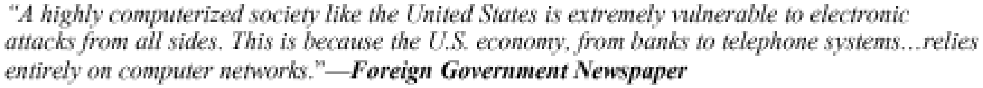
Government services



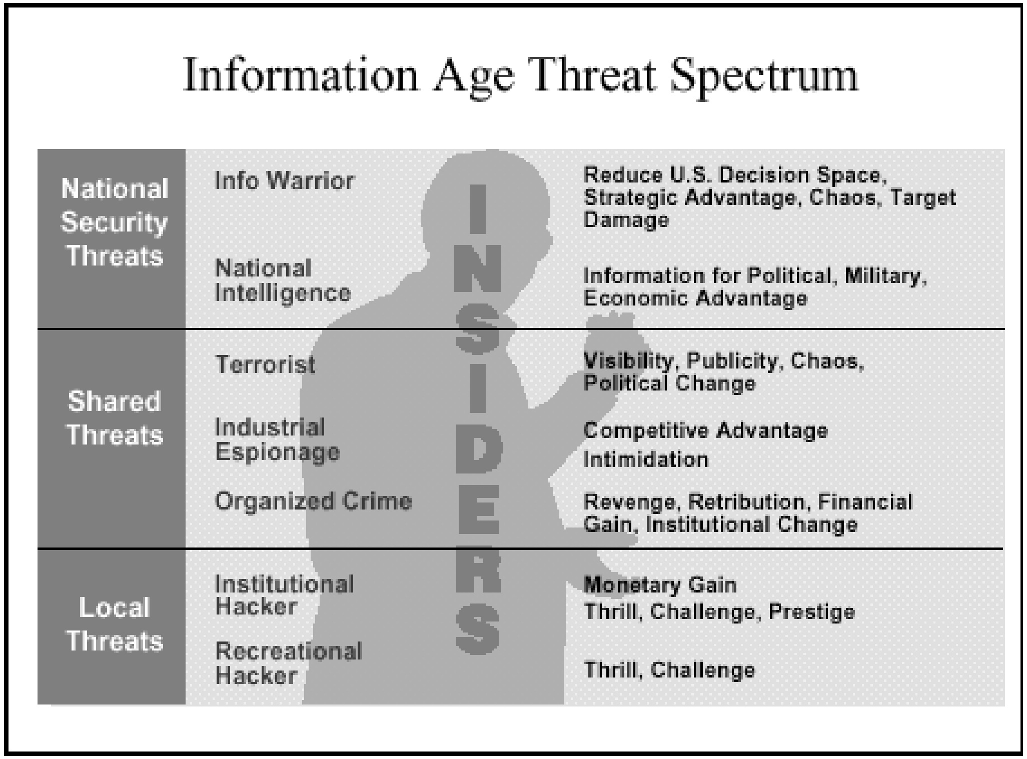
Trimmer 2002

FACT 2

- **THERE ARE DEFINED THREATS TO YOUR COMPUTER SYSTEM!**



"A highly computerized society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems…relies entirely on computer networks."—***Foreign Government Newspaper***



Information Age Threat Spectrum

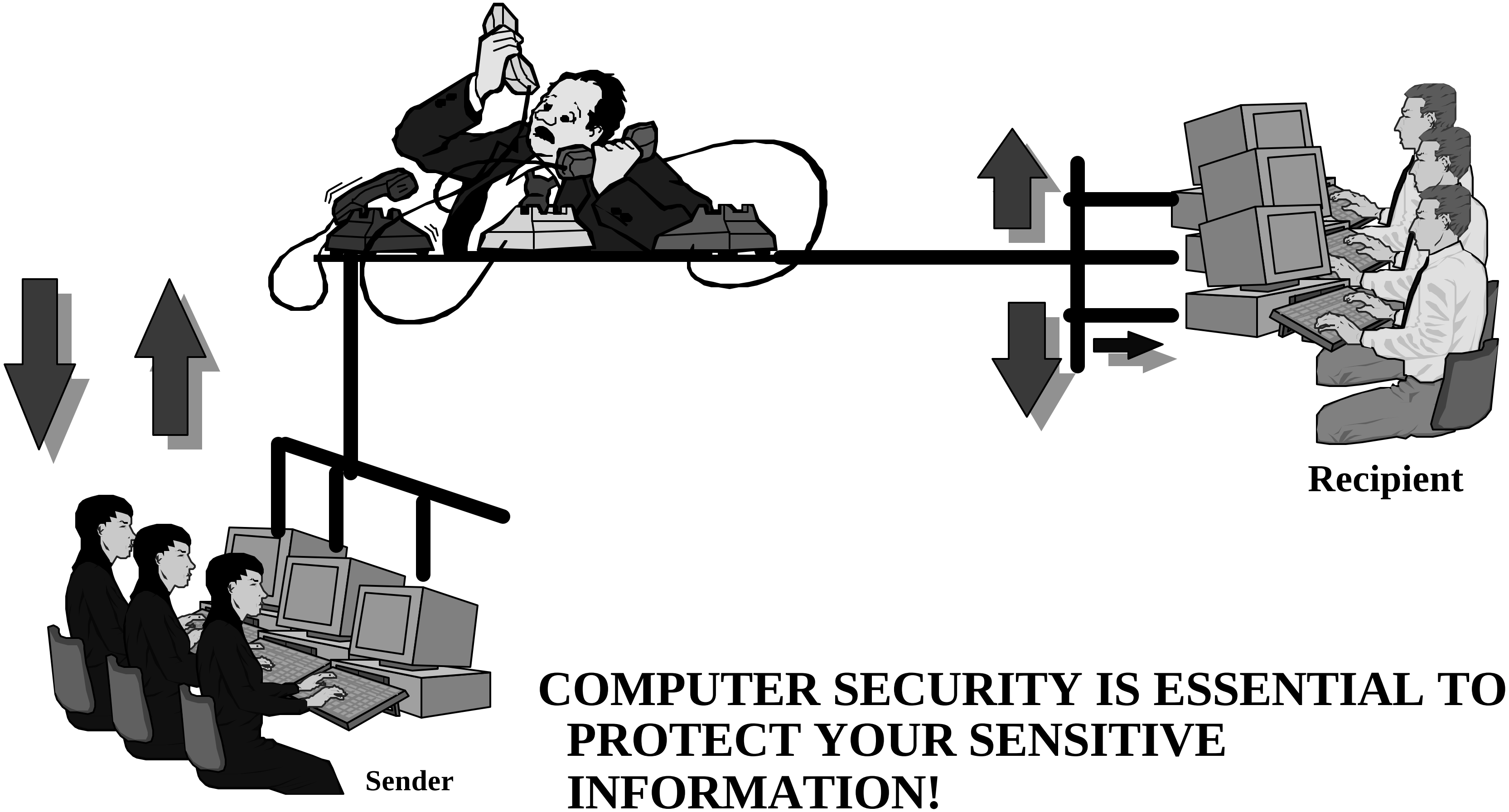
National Security Threats	Info Warrior	Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage
	National Intelligence	Information for Political, Military, Economic Advantage
Shared Threats	Terrorist	Visibility, Publicity, Chaos, Political Change
	Industrial Espionage	Competitive Advantage Intimidation
	Organized Crime	Revenge, Retribution, Financial Gain, Institutional Change
Local Threats	Institutional Hacker	Monetary Gain Thrill, Challenge, Prestige
	Recreational Hacker	Thrill, Challenge

FACT 3

- **COMPUTER SYSTEMS ARE VULNERABLE!**

  - ♦ THREATS BY PEOPLE
    - – Unintentional Actions => 50-60%
    - – Intentional Actions => 15-20%
    - – Outside Actions => 1-3%
  - ♦ PHYSICAL and ENVIRONMENTAL THREATS
    - – Fire Damage => 10-15%
    - – Water Damage => 1-5%
    - – Natural Disaster => 1%
  - ♦ Other => 5-10%

FACT 4



COMPUTER SECURITY IS ESSENTIAL TO PROTECT YOUR SENSITIVE INFORMATION!

FACT 5

- **RISK MANAGEMENT IS AN EXECUTIVE RESPONSIBILITY!**

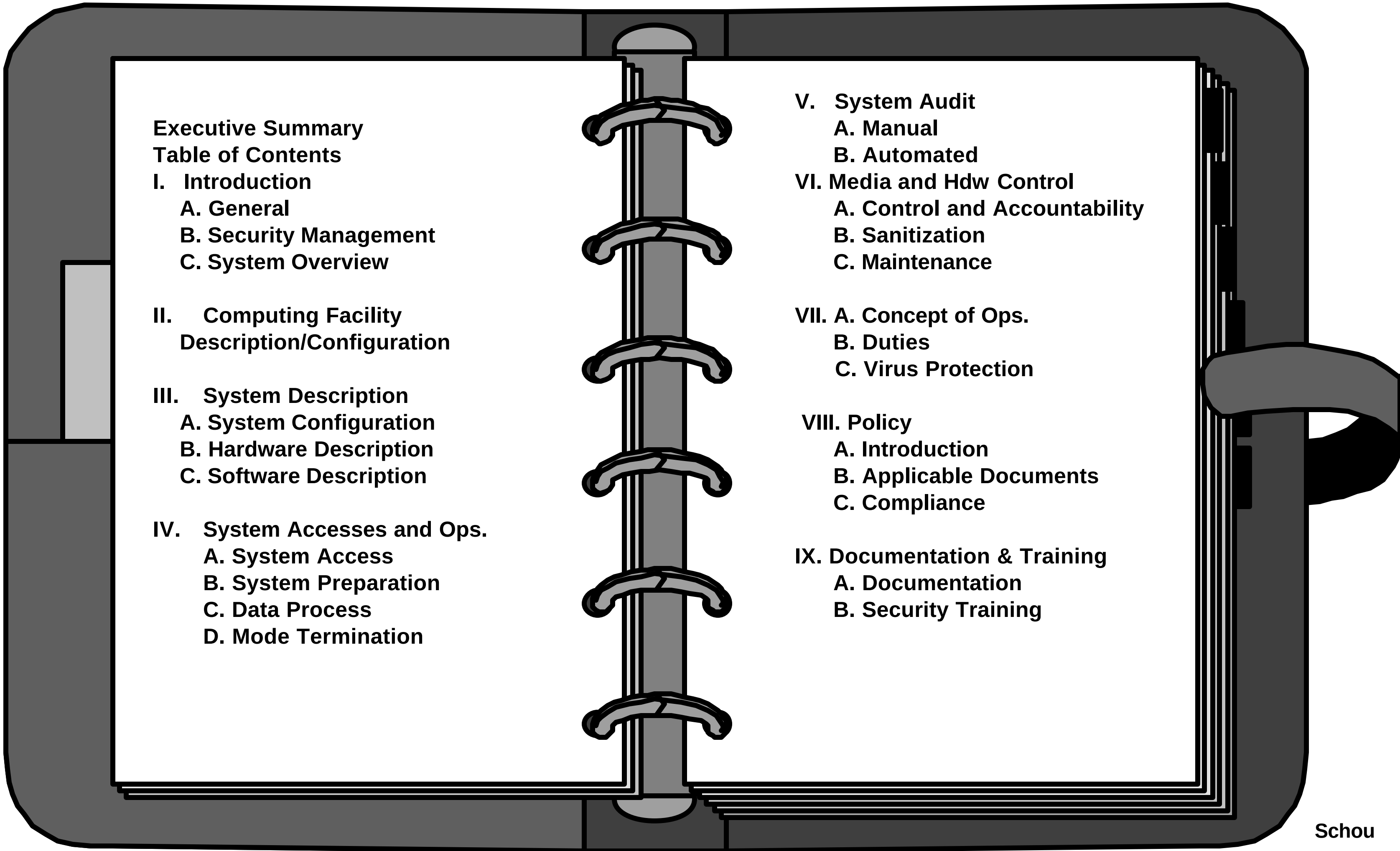
What do you do if you find a problem?

FACT 6

- **COMPUTER SECURITY AWARENESS AND TRAINING PROGRAMS REDUCE RISK!**

FACT 7

- **A COMPUTER SECURITY PLAN IS AN EFFECTIVE EXECUTIVE TOOL**



Executive Summary
Table of Contents
I. Introduction
  A. General
  B. Security Management
  C. System Overview

II. Computing Facility
  Description/Configuration

III. System Description
  A. System Configuration
  B. Hardware Description
  C. Software Description

IV. System Accesses and Ops.
  A. System Access
  B. System Preparation
  C. Data Process
  D. Mode Termination

V. System Audit
  A. Manual
  B. Automated
VI. Media and Hdw Control
  A. Control and Accountability
  B. Sanitization
  C. Maintenance

VII. A. Concept of Ops.
  B. Duties
  C. Virus Protection

VIII. Policy
  A. Introduction
  B. Applicable Documents
  C. Compliance

IX. Documentation & Training
  A. Documentation
  B. Security Training

Security Plan

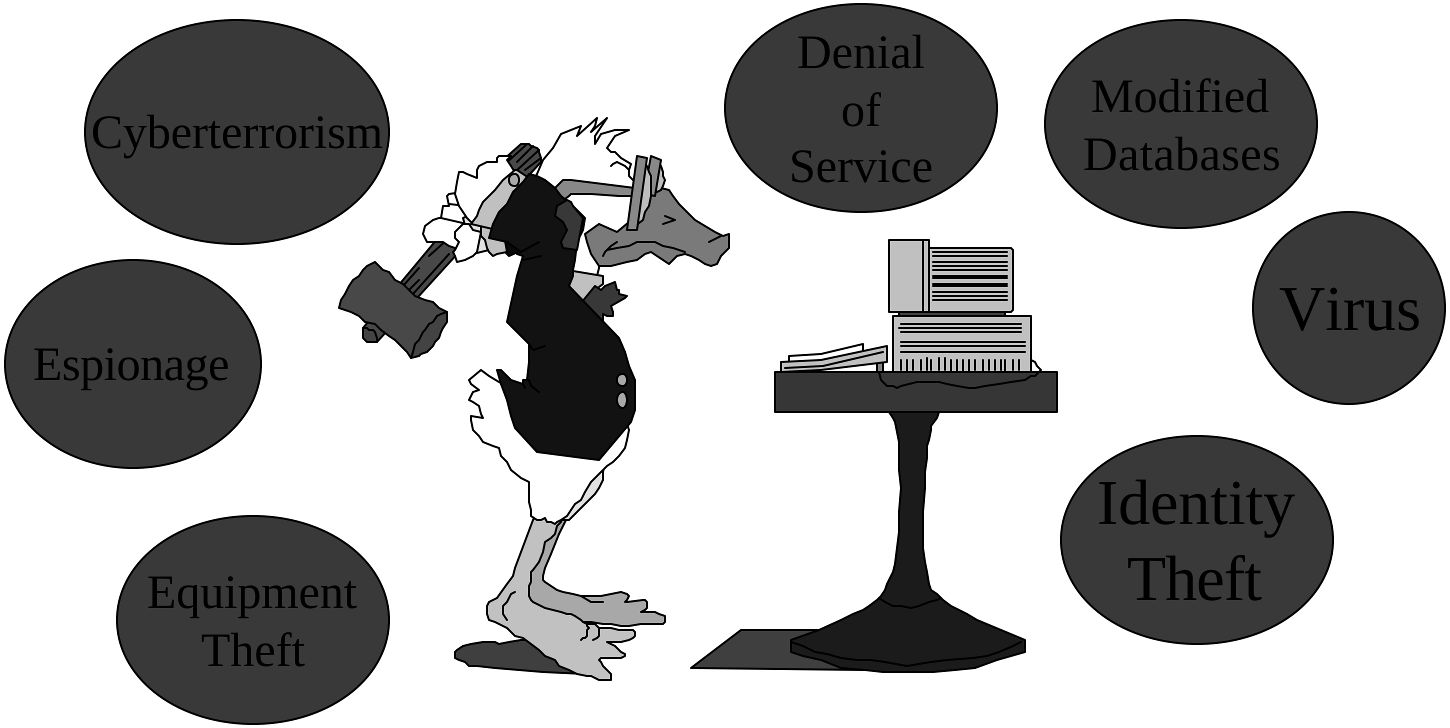
- **The Plan Must**
  - **Identify All Actions Needed To Implement Security Safeguards**
  - **Cite All Applicable Laws, Policies and Regulations**
  - **Describe Degree of Compliance With Regulations**
  - **Provide For A Review and Revision Process**

Risk Management

Risk = Threat X Vulnerability — Security

What is "Security"?

- To decide whether a computer system is "secure", you must first decide what "secure" means to you, then identify the threats you care about.



Cyberterrorism

Denial of Service

Modified Databases

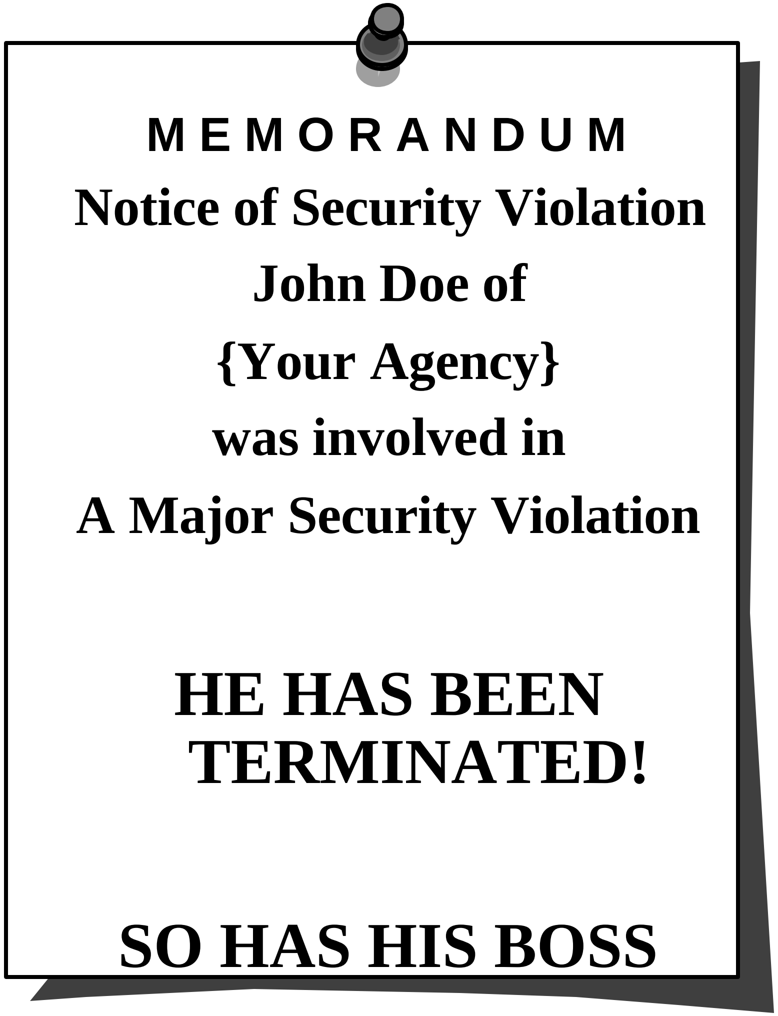
Espionage

Virus

Equipment Theft

Identity Theft

Why Should You Care?



MEMORANDUM

Notice of Security Violation

John Doe of

{Your Agency}

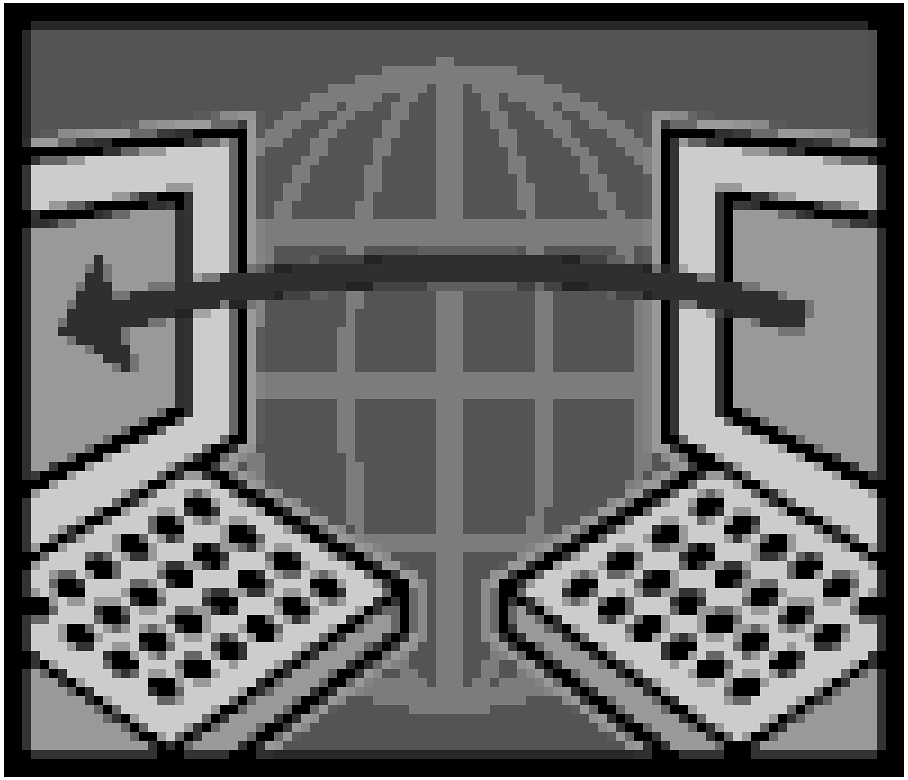
was involved in

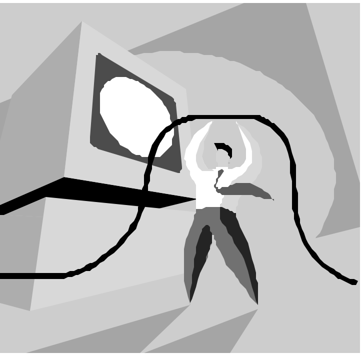
A Major Security Violation

HE HAS BEEN
TERMINATED!

SO HAS HIS BOSS

Poor Security Practices Lead to Downtime



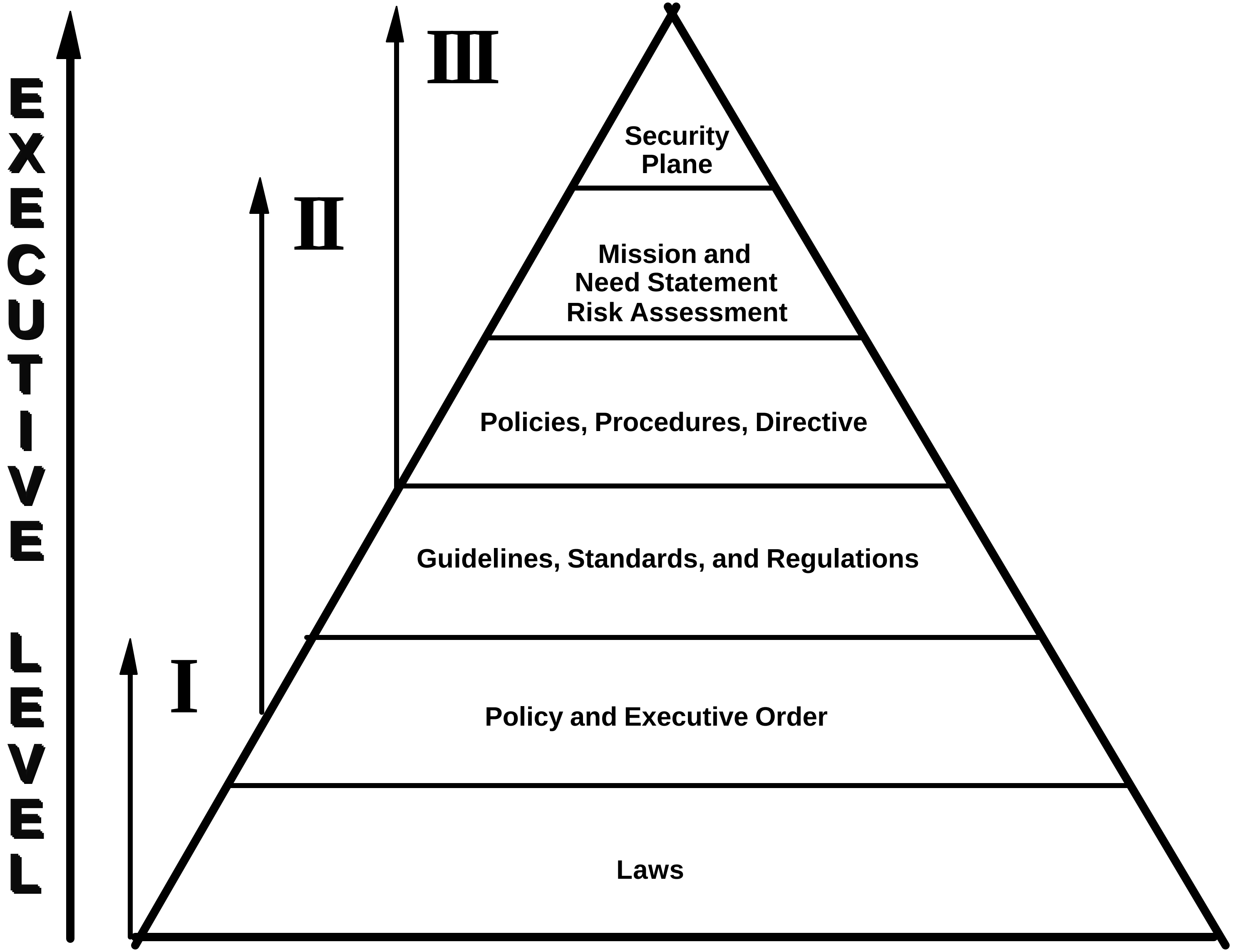


Disruption or Denial of Critical Services

- **Medical**
- **Payroll**
- **Privacy**
- **etc.**

This may cost your organization lives, time, or money

Policy Pyramid


EXECUTIVE LEVEL
III
II
I
Security Plane
Mission and Need Statement Risk Assessment
Policies, Procedures, Directive
Guidelines, 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

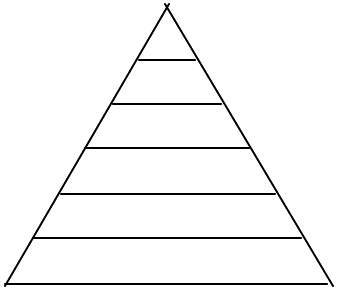
Interception or Disclosure of Wire, Oral or electronic Communications

Public Law 100-235

Computer Security Act of 1987

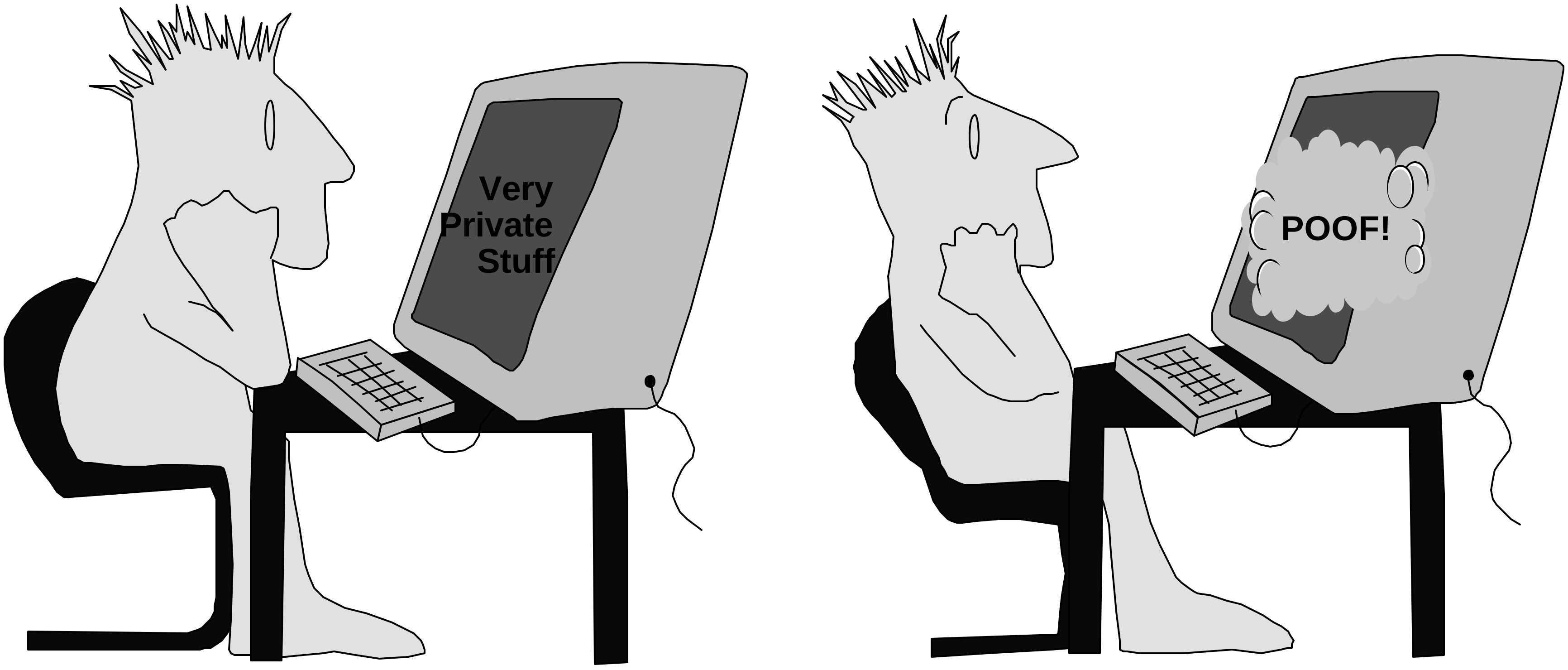
Public Law 100-503

Computer Matching and Privacy Protection Act

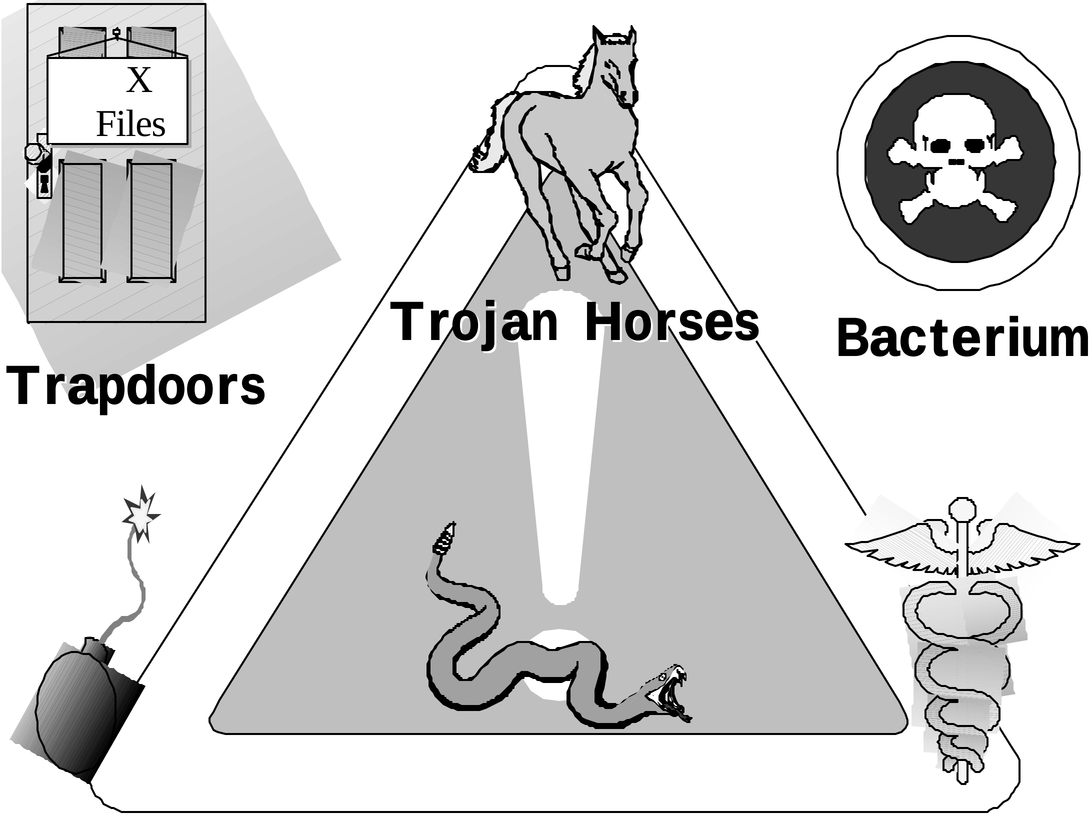


Who Is The Threat

I Just Didn’t Know



MALICIOUS CODE



Trapdoors

Trojan Horses

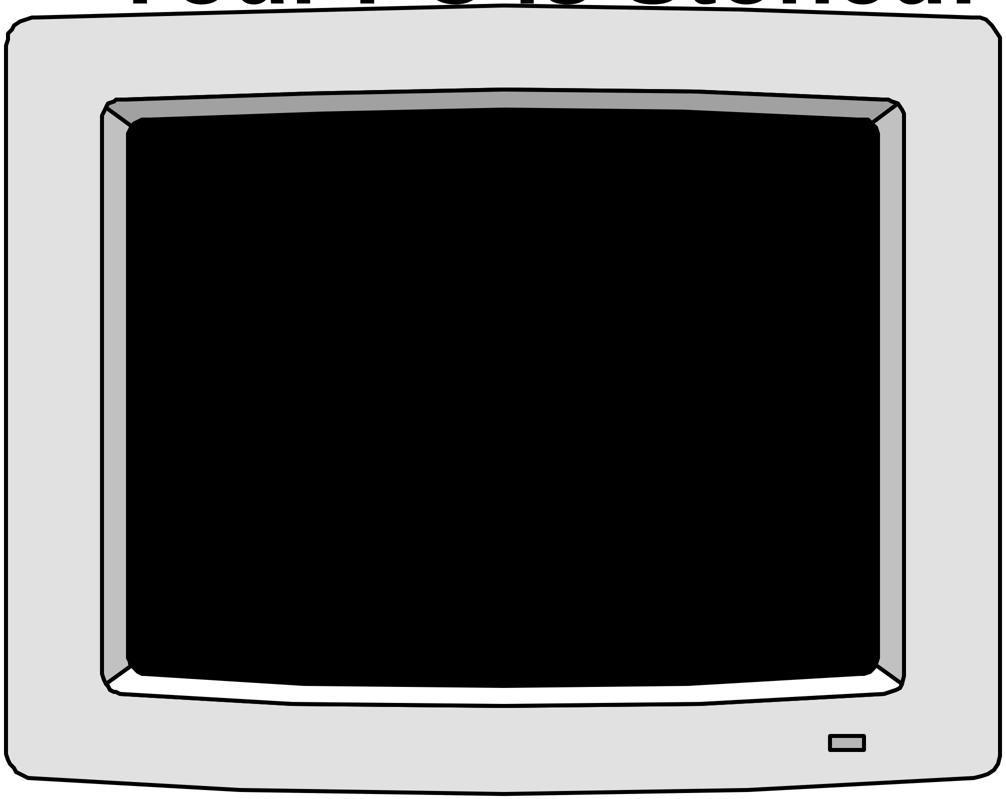
Bacterium

Logic Bombs

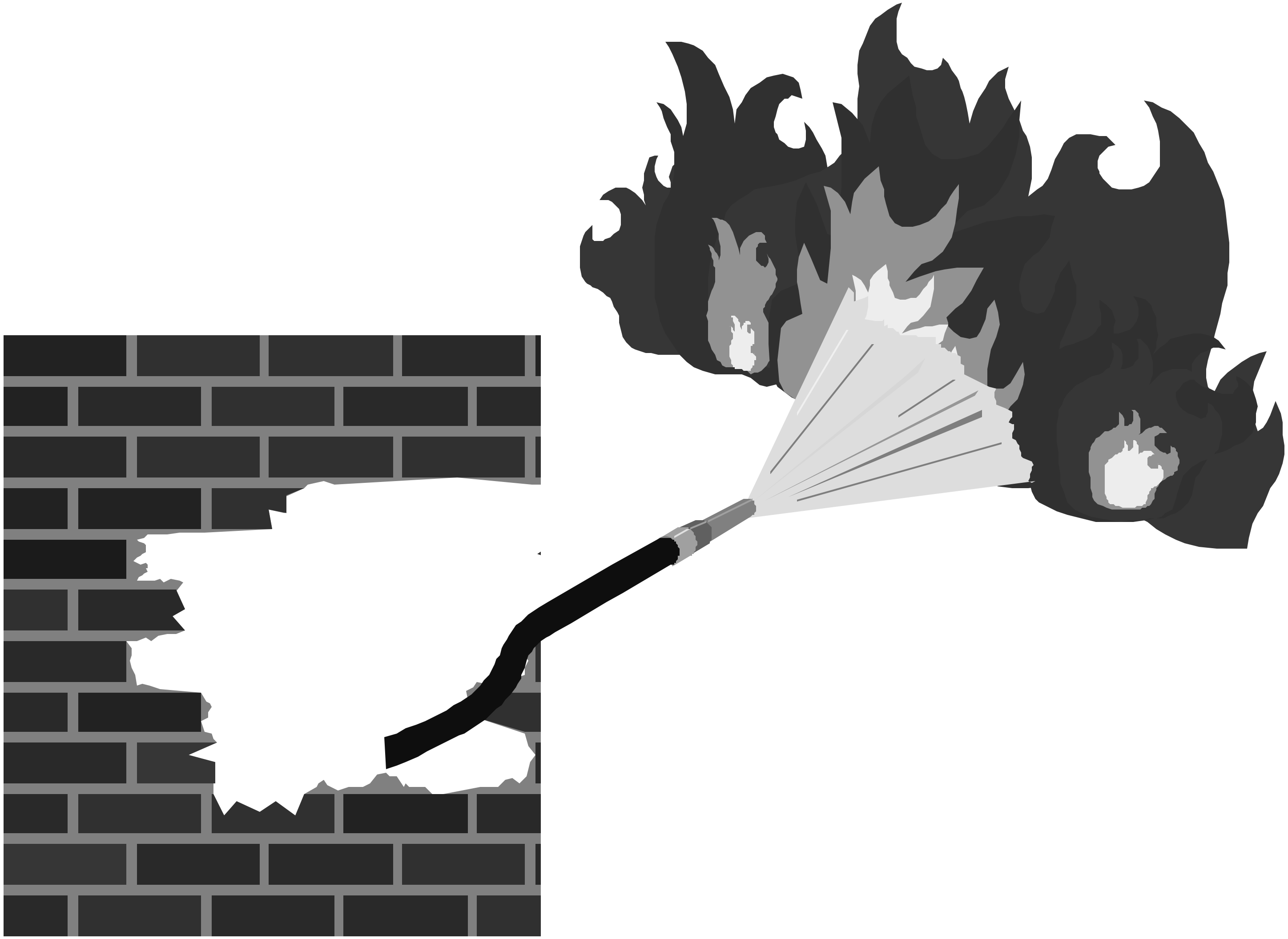
Worms

Virus

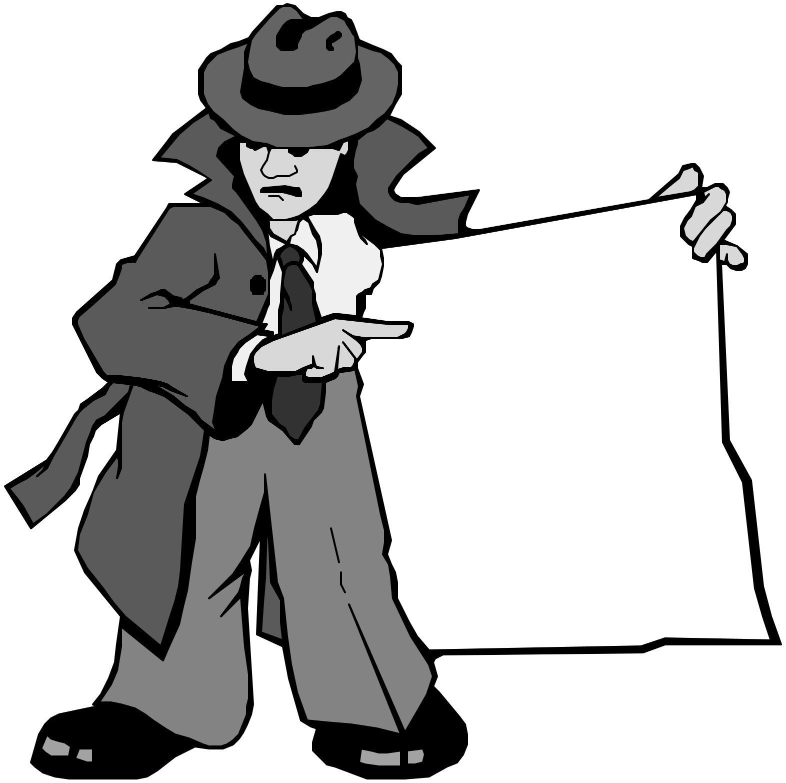
Your PC is Stoned!



Environmental Hazards



Industrial Espionage



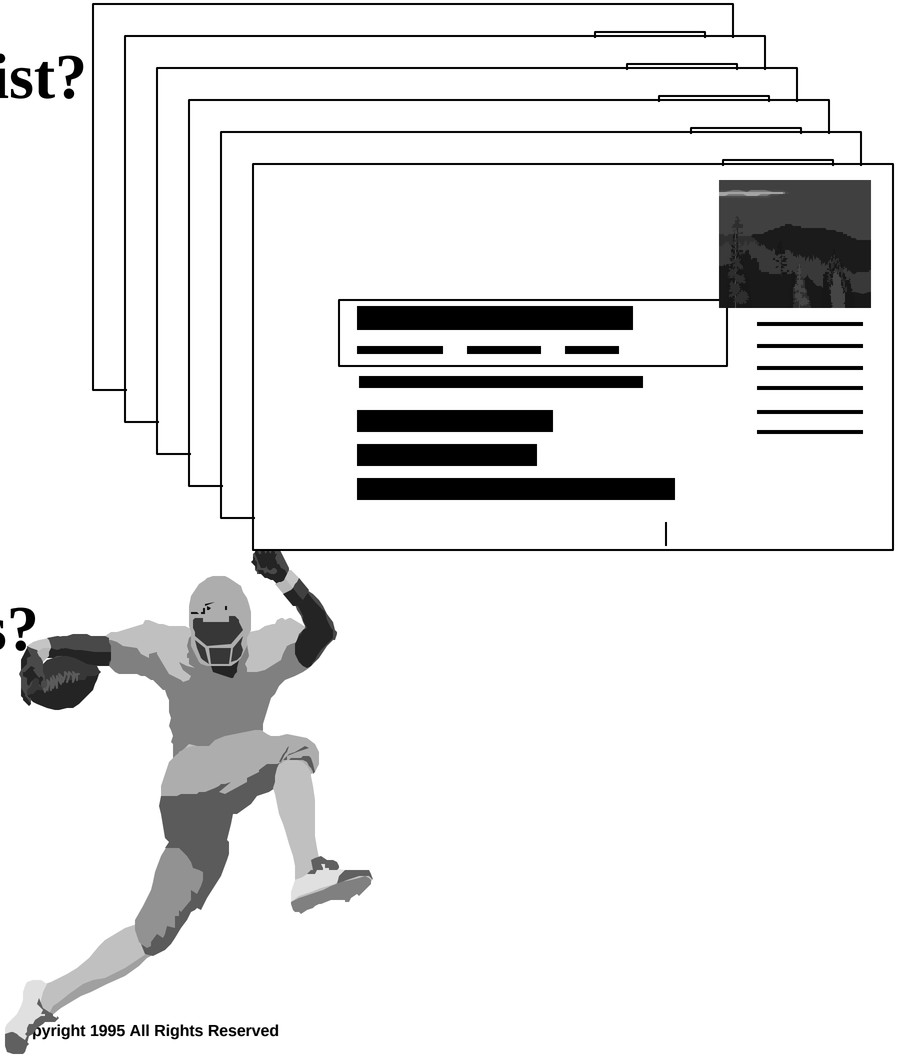
Contrast of Laws Versus Ethics

- Ethics are different from laws.
- Laws apply to everyone while ethics are personal
- If two laws conflict, a judicial process can determine which takes precedence.
- Ethics often come into and must be resolved by individuals
- the laws and must determine what is ‘right’ (legal) or what is ‘wrong’ (illegal).
- Ethical values must be determined individually.
- What one person views as ethical may be viewed by another as completely unethical

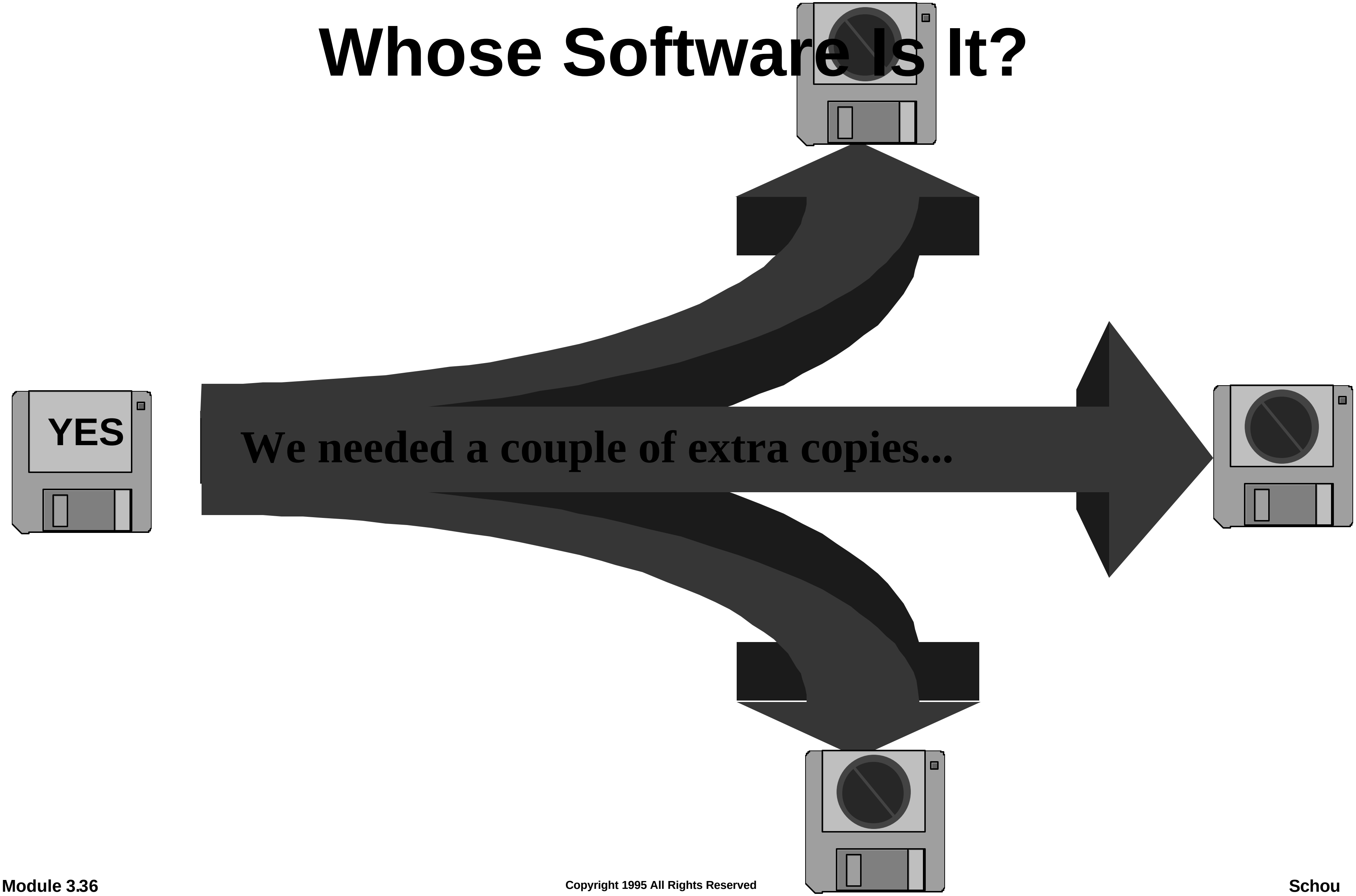
What Belongs On Government Systems?

- **Christmas Card List?**

- **Football Pool Stats?**



Whose Software Is It?



We needed a couple of extra copies...

Risk Management

Risk Management is:

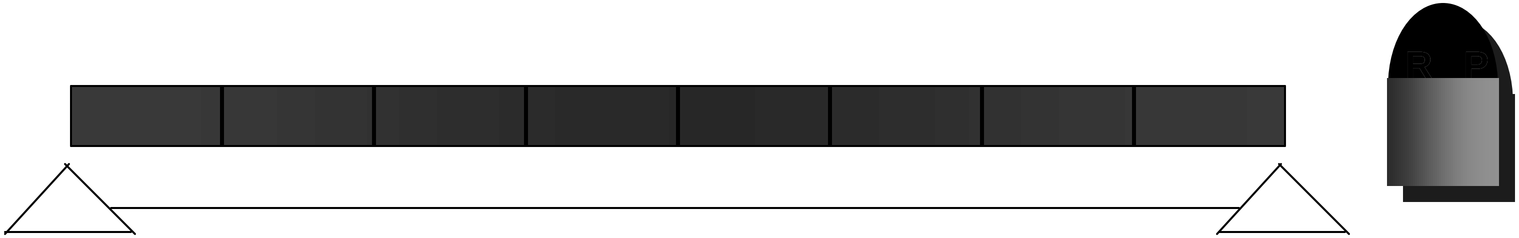
- A systematic method to analyze security risks and bring in cost effective safeguards to reduce risk
- Cost-benefit: Have to "sell" it to management
- Risk Management in simpler terms:
  - 1. Decide what you need to protect.
  - 2. Decide what you need to protect it from.
  - 3. Decide how to protect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

INFOSEC Life Cycle Management

- **Life Cycle Phases**



Design and Development

Fabrication and Production

Acquisition and Procurement

Test and Evaluation

Shipping and Delivery

Operations

Maintenance

Obsolescence and Removal

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

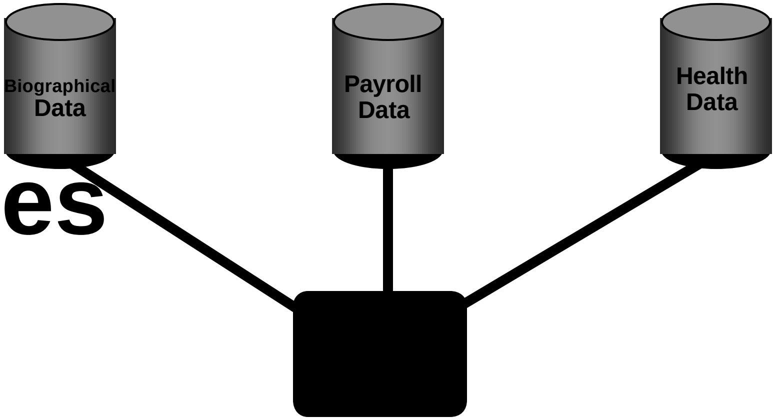
- The Use of Passwords Should Follow These Guidelines
  - No repeat guesses
  - Log unsuccessful attempts
  - Review log
  - Never write down sensitive combinations
  - Hard to guess passwords
  - Change frequently
  - Easy to recall, hard to guess
  - Don't disclose

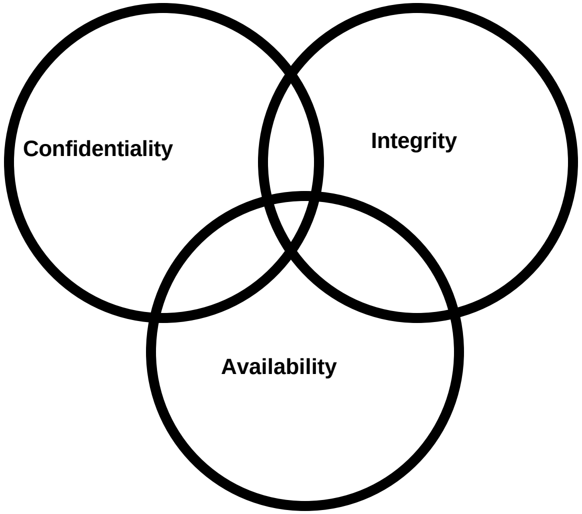
Cyber Terrorism

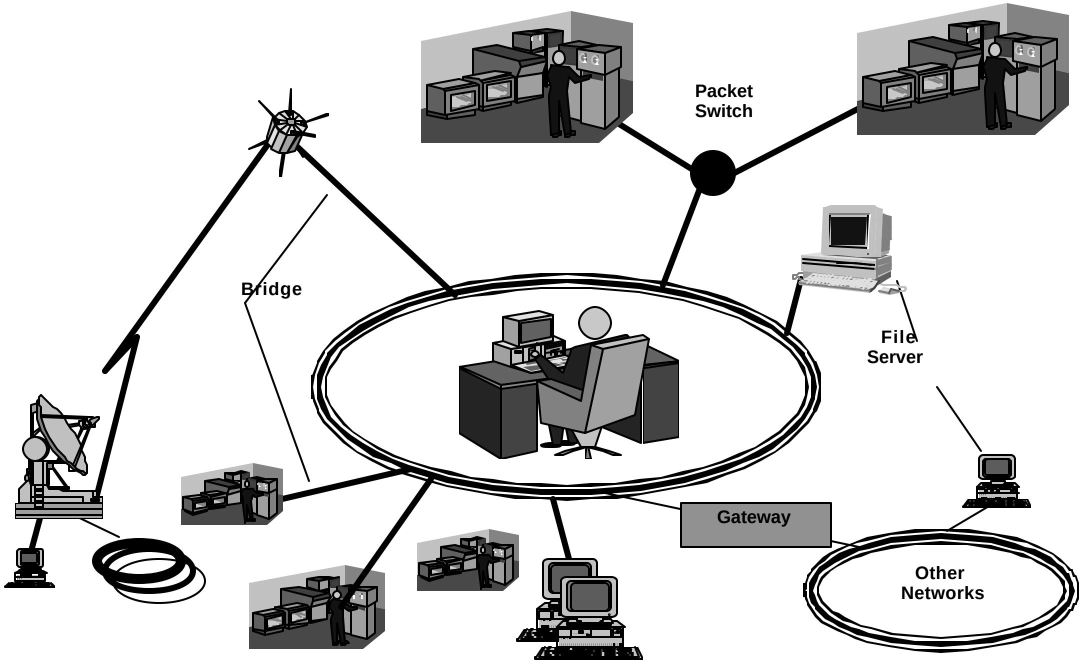
- The Internet Black Tigers conducted a successful "denial of service" attack on servers of Sri Lankan government embassies
- Italian sympathizers of the Mexican Zapatista rebels attacked web pages of Mexican financial institutions.
- Rise of “Hack-tivism”

Freeh, Testimony before Senate, 2000.

Current Issues

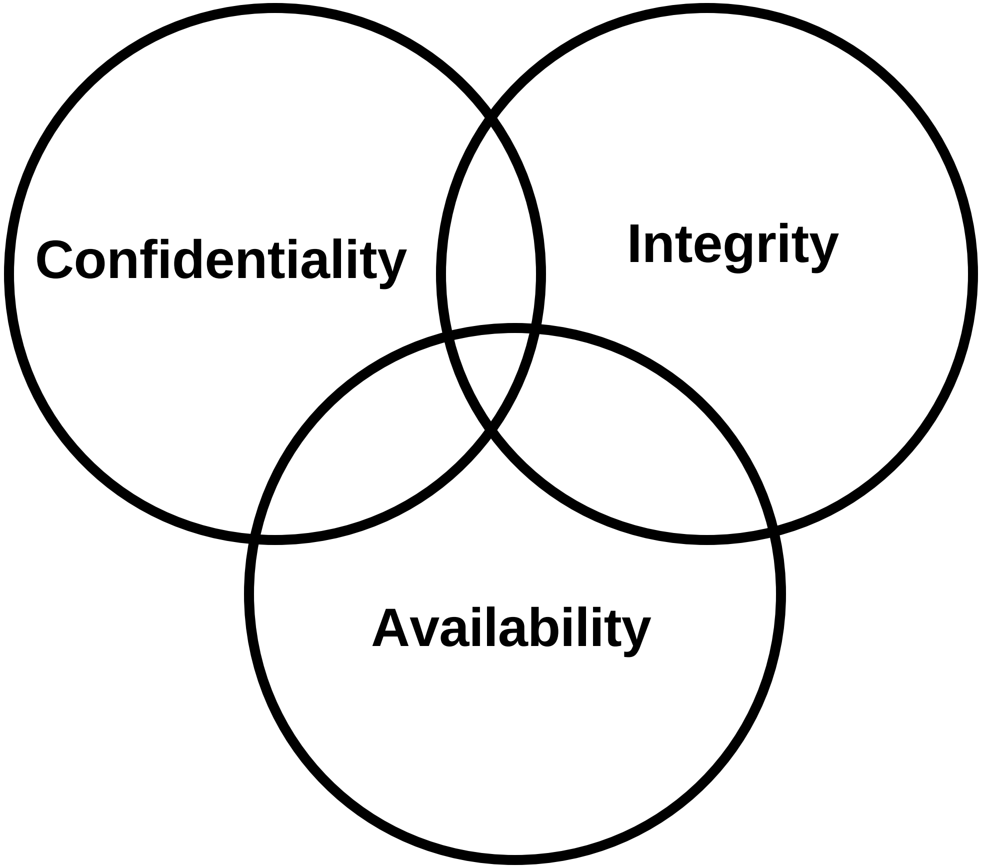






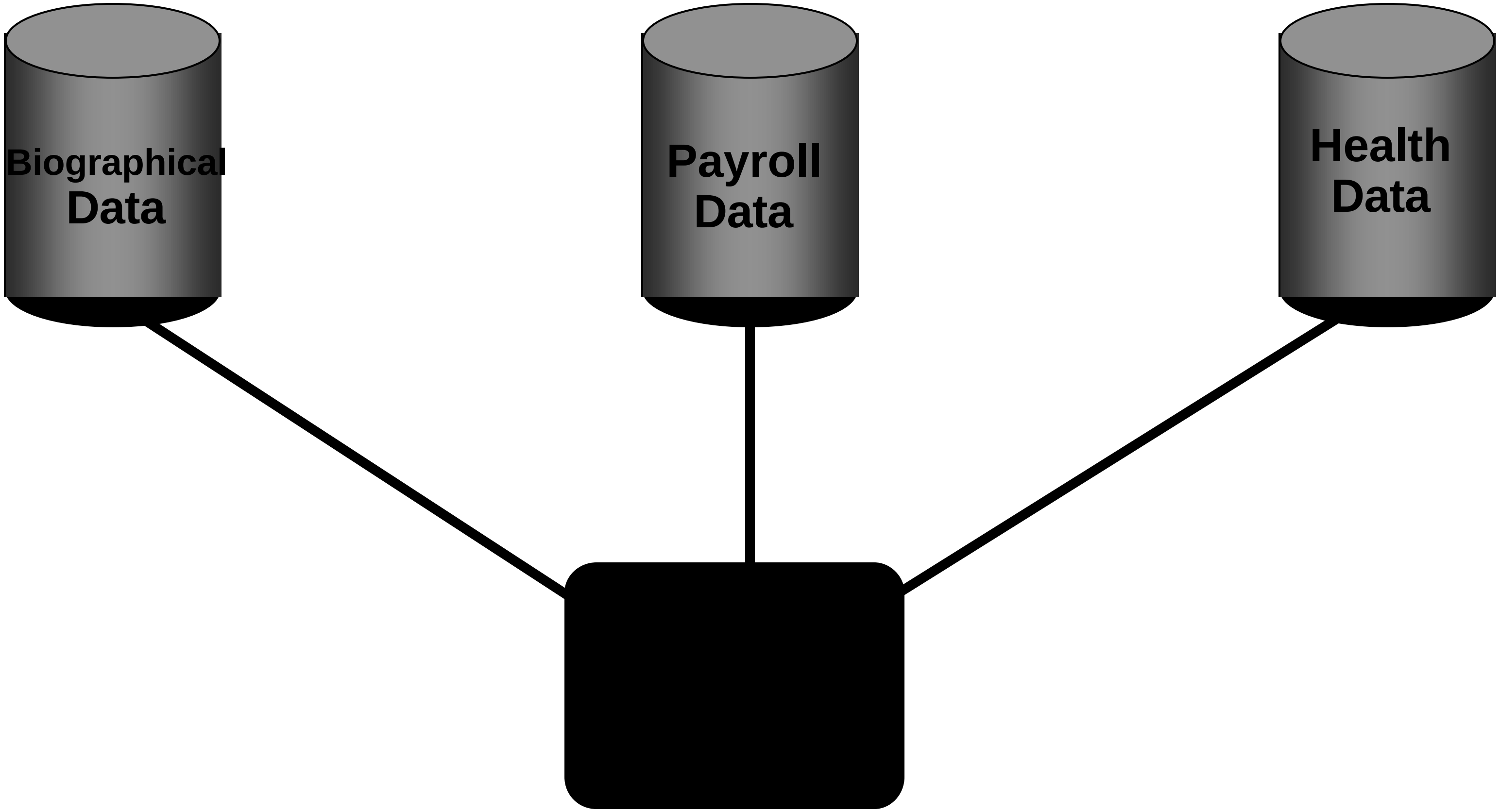
Current Issues

Confidentiality, Integrity, Availability



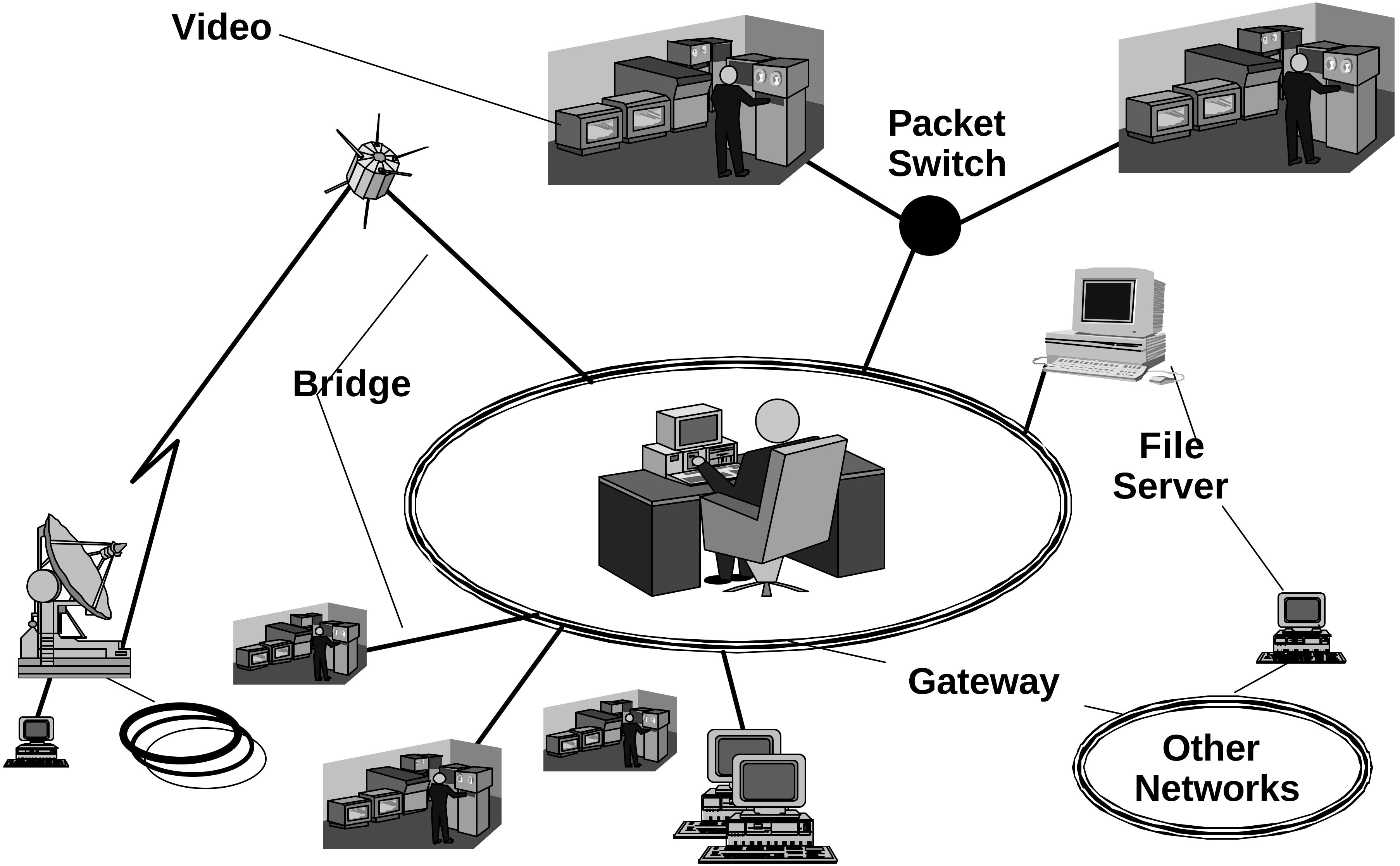
Current Issues

Data Aggregation and Sensitivity



Current Issues

Inter-connectivity



Threats to Personal Privacy

- **Buying and selling confidential information from Social Security files.**
- **Browsing IRS files.**
- **Buying and selling bank account name lists.**
- **A Princeton University student stole ~1800 credit card numbers, customer names, and user passwords from an e-commerce site.**

House Ways and Means Committee, 102nd Congress, 1992.
10., Washington Post, S. Barr, 2 Aug. 1993
(4) Freeh, Testimony 2000

Executive Action Items – Step 1

- Validate Number and Function of Systems
- Appoint Security 'Officer' To Each System/Network
- Assign Responsibility and Deadline for Documentation Package of Each System

Executive Action Items – Step 2

- Appoint Program Manager
- Determine Boundary For Each System/Network
- Assign Responsibility For Evaluation
- Develop Security Policy For Each System/ Network
- Assign Organizational Responsibility To:
  - Security Tasking
  - Configuration Management Tasking
  - Mission and Function Tasking

Executive Action Items – Step 3

- Prepare Program Management Plan
  (Include Security Plan)
- Implement Security Policy
- Develop And Implement Risk Analysis
- Evaluate and Monitor Resource Expenditures