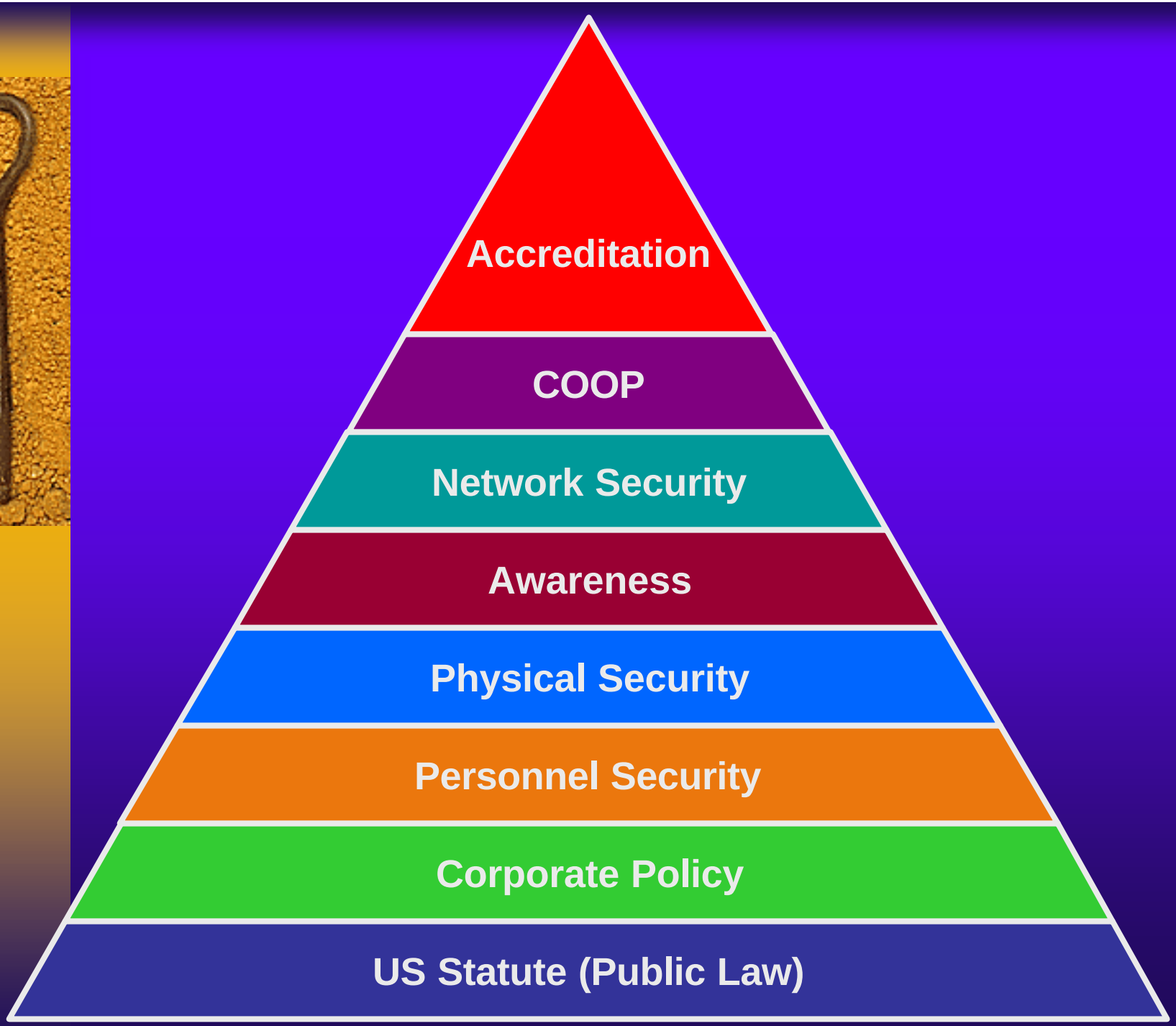
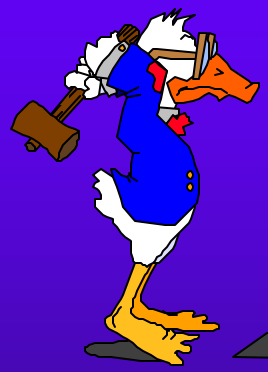
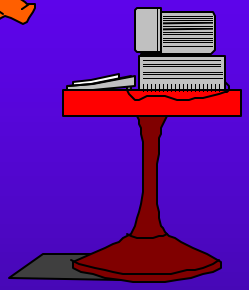
Building an Information Assurance Program

Harry L. Bouris, CISSP
Sumaria Systems, Inc.


Accreditation
COOP
Network Security
Awareness
Physical Security
Personnel Security
Corporate Policy
US Statute (Public Law)

PUBLIC LAW





1970s

- 1974-Freedom of Information Act
  - Only applies to the Executive Branch of the Federal Government
- 1974-Privacy Act
  - Pertains only to the Executive Branch of the Federal Government
- 1978-Right to Financial Privacy Act

1970s

- 1978-Right to Financial Privacy Act
  - Congress' response to a U.S. Supreme Court decision that found bank customers had no legal right of privacy for their financial information held by financial institutions.
  - Largely procedural
  - Requires government agencies to provide notice and an opportunity to object before a bank or other institution can disclose personal financial information to a government agency, usually for law enforcement purposes.
  - The law was amended in the latter 1980s to allow postponement of notice in investigations dealing with drug trafficking and espionage.

1980s

- 1986-Electronic Communications Privacy Act (ECPA)
  - Prohibits monitoring of wire, oral, or electronic communications (includes email, network traffic, and keystrokes)
  - Determined that email can be monitored if it is in the course of normal business
  - Can make “consent to monitor” a condition of employment

1980s

- 1984-Computer Fraud and Abuse Act (amended in 94/96/01)
  - makes it certain activities designed to access a "federal interest computer" illegal
    - Activities range from knowingly accessing a computer without authorization or exceeding authorized access to the transmission of a harmful component of a program, information, code, or command.
    - A federal interest computer includes a computer used by a financial institution, used by the United States Government, or one of two or more computers used in committing the offense, not all of which are located in the same State.

1980s

- 1987-Computer Security Act
  - Must protect Federal computer systems
  - Federal Executive Agencies must have a computer security program

1980s

- 1988-Foreign Corrupt Practices Act
  - Applies to all companies registered with the SEC
  - Requires companies to start a computer security program

1990s

- Economic Espionage Act
  - Obtaining trade secrets to benefit a foreign power
- 1996-Child Pornography Act
  - Enacted specifically to combat new technology
- 1996-Electronic Espionage Act
  - Deals with Industrial Espionage

1990s

- 1996-Health Insurance Portability and Accountability Act (HIPAA) PL 104-191
  - Standardization of electronic patient health administrative and financial data
  - Unique health identifiers for individuals, employers, health plans, and health care providers
  - Security standards protecting the confidentiality and integrity of “individually identifiable health information”, past, present and future

1990s

- HIPAA—3 Basic Rules
  - Code sets
    - Standardized format for transmitting and storing health information
  - Privacy
    - Addresses who has access (need to know) to patient health information, written, spoken, or electronic
  - Security
    - How to protect who has access, and prevent disclosure, either accidental or intentional

1990s

- 1998-PDD 63 Protecting America's Critical Infrastructure
  - Establish national center for warning
  - Federal Government to serve as a model
  - Secure information systems infrastructure by 2003
  - Seeks voluntary participation of private industry

1990s

- 1999-Graham-Leach-Biley Act (GLB)
  - Governs financial institutions
- 1999-Fair Credit and Reporting Act
  - Governs type of data a company may collect on private individuals

2000s

- 2001- US Patriot Act
  - Sweeping new powers to domestic law enforcement and intelligence agencies
  - eliminated the checks and balances that previously gave courts the opportunity to ensure that these powers were not abused
  - Permits public and private organizations to compare client records against lists of criminal suspects and fugitives published by the U.S. and international government agencies.

2000s

- US Patriot Act
  - Changed 15 different statutes
  - ACLU not happy ☹

2000s

- 2003-The National Strategy to Secure Cyberspace

Policy Development

Corporate Policy

US Statute (Public Law)

Policy Development

- Policies
- Guidelines
- Standards
- Procedures

Policy Development

- POLICY
  - High level statement that provides direction to workers.
  - Indicate management intention about operation of the organization
  - Mandatory
  - Requires special approval (waiver) to take a different course of action
  - Update infrequently

Policy Development

- GUIDELINE
  - High level statements, similar to policy
  - NOT mandatory, they are recommendations and are optional ("should" vice "shall")
  - NOT recommended for use in IA
    - Violate Principle of secure system design (universal application)
    - Controls are somewhat weakened if not consistently applied
  - Can be of use when…

Policy Development

- Management backing is not strong
  - They don't understand
- Management is indecisive
  - Weak
- Management doesn't want to come across as dictatorial
  - Want to be liked
- Possibility of approval when policy would be rejected

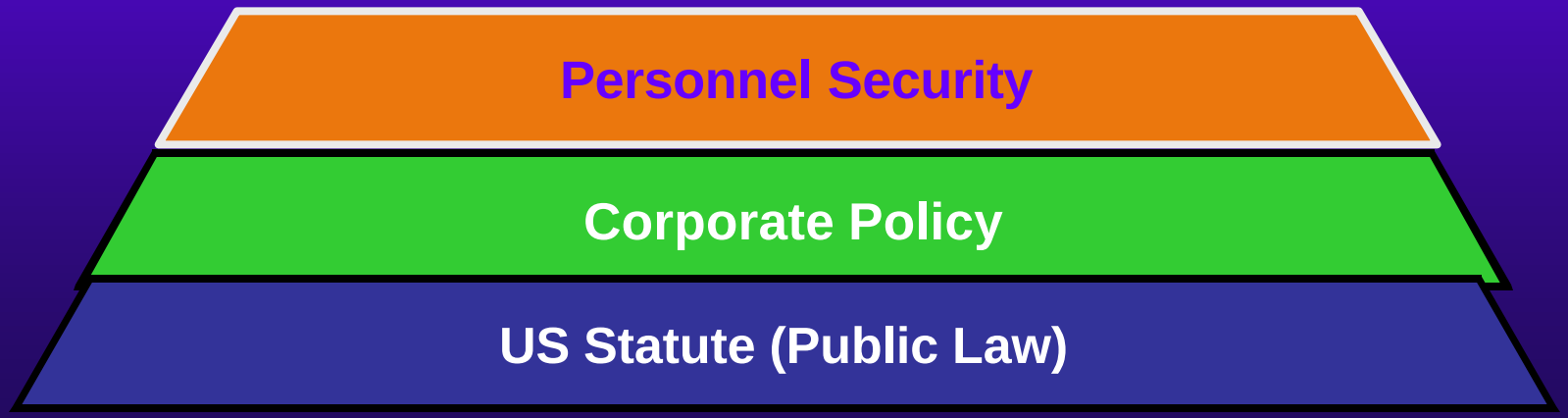
Policy Development

- A guideline is better than nothing at all
  - You can always ease into a policy
  - Key is to have something to start with

Policy Development

- How long should a good policy be?

- AS LONG AS IT NEEDS TO BE!!!
  - Must be tailored to the needs of the organization—there is no cookie cutter answer


Personnel Security
Corporate Policy
US Statute (Public Law)

Personnel Security

- Not just an IT issue
  - HR is the main player
  - Cross reference and provide input to HR policies

Personnel Security

- Background checks
- Security clearances (govt only)
- Employment agreements
- Hiring and termination practices
- Job descriptions
- Job rotation
- Separation of duties and responsibilities

Personnel Security

- Background Checks
  - Supports hiring decision
  - Provides some protection and assurance

- Who should be checked
  - Security Personnel
  - Net Admins
  - Managers
  - Auditors
  - All?

Personnel Security

- What can be checked on an applicant
- Credit Report
- SSN searches
- Workers Compensation reports
- Criminal record
- Motor Vehicle report
- Education verification
- Reference checks
- Prior employment verification

Personnel Security

- Security clearances
  - Uniformed members of the military
  - Civilian employees working for DoD and other government agencies
  - Employees of government contractors

Personnel Security

- Employment agreements
- Non-compete
- Non-disclosure
- Restriction on dissemination of corporate information (press, analysis, law enforcement)

Personnel Security

- Hiring and Termination Practices
- Strictly an HR policy
- Hiring manager responsible for review of background checks
- Managers must take timely and appropriate disciplinary action
- Applicability to contractors/sub contractors

Personnel Security

- From an IT perspective
- Shutting down accounts-how notified
- Forwarding email and voice-mail
- Lock and combination changes
- System password changes
- Notification to all personnel

Personnel Security

- Job Descriptions
- Be based on designated position sensitivity
- Be based on sensitivity of information handled
- Address security responsibilities of the position
- Be considered in performance evaluation

Personnel Security

- Job Rotation Implemented Where Feasible
- Discourage fraud, waste, and abuse
- Requires collusion
- Promotes cross-training
- Often not possible in highly specialized jobs

Personnel Security

- Separation of Duties
- People checking for inappropriate use are not capable of the inappropriate use
- No person should be responsible for completing a task involving sensitive, valuable, or critical information from beginning to end
- A person must not be responsible for approving their own work

Personnel Security

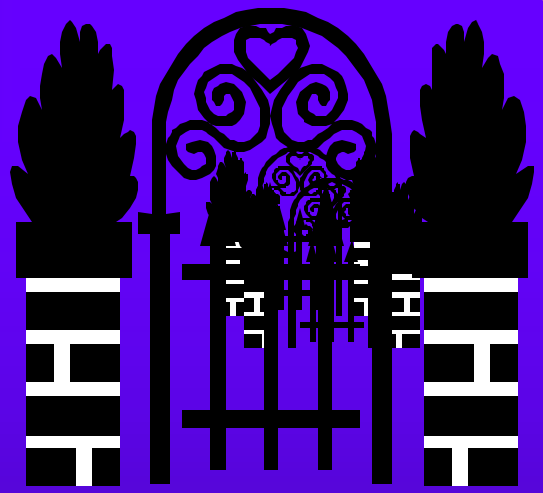
- What to separate
- Development from Production
- Security from Audit
- Accounts payable and Accounts receivable
- Security and Privacy

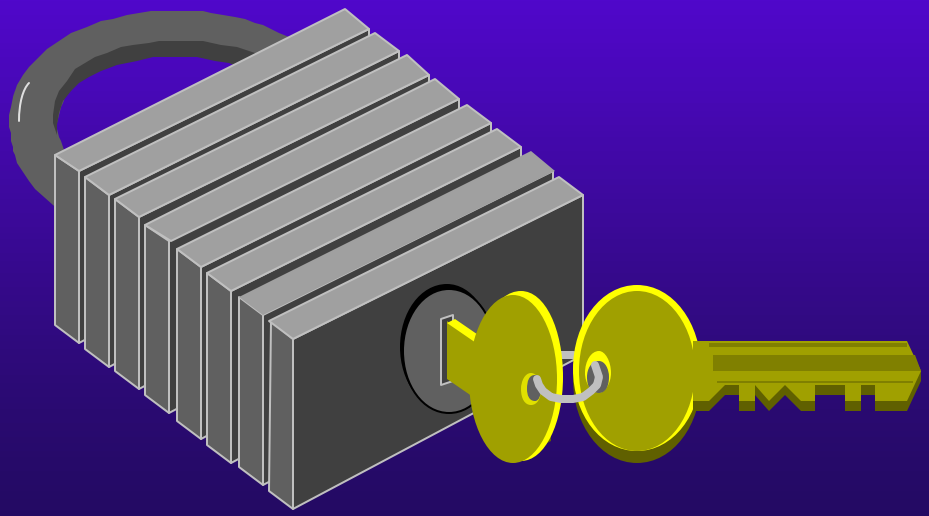
Personnel Security

- Summary

- Make sure you hire only “good guys”
- Make sure employees know their responsibilities
- Do thing to keep the good guys good
- If good guys turn bad, know what to do with their accounts

Physical Security





Physical Security

- Why the clock?

- Time Based Security
  - P=Protection (bank vault)
  - D=Detection (sensors and alarms)
  - R=Response (the cops)

- $Pt > Dt + Rt$

(where $Pt > 0$)

Physical Security

- Fortress Mentality
- 1200 BC Troy under siege for nine years
  - Walls of city were strong, as long as they didn’t open the gates to permit commerce
- 1368 The Great Wall of China completed
  - No real military value
- Middle Ages Castles with moats, high/thick walls defeated by catapults
- 1932 The Maginot Line bypassed by the Germans and captured in 1940

Physical Security

- Not to say Physical Security is no longer important, Still a vital consideration

- 4 Questions to ask

- What are you protecting?
- How important is the information?
- For whom are you protecting it and which part of CIA is most important?
- What or who are you protecting it from?

Physical Security

- Physical Access Controls
- Environmental Protection
- External Threats
- Internal Threats
- Site Design & Configuration Considerations
- Computer Facility Requirements

Physical Security

- Facility Classification
- Owned facility—easiest to secure
- Leased facility—separation of responsibility
- Shared facility—most complicated to secure

Physical Security

- Physical Access Controls
  - Guards
  - Fences
  - Barriers
  - Lighting
  - Keys and locks
  - Badges and Escorts
  - Monitoring/Detection System

Physical Security

- Environmental Protection
  - Power Protection
  - HVAC
  - Water Protection
  - Fire Detection
  - Fir Suppression
  - Ease of Evacuation
  - Environmental monitoring/detection

Physical Security

- External Threats
  - Storms
  - Rising Water
  - Earth Movement
  - Fire/Smoke
  - Toxic Materials
  - Explosion

Physical Security

- Internal Threats
  - Fire and Smoke
  - Utility Loss
  - Falling Water
  - Communications Loss
  - Equipment Failure
  - Building Collapse
  - Personnel Loss (Strikes/Illness etc.)

Physical Security

- Site Design & Configuration Considerations
  - Local Crime Rate
  - Visibility
  - Emergency Access
  - Natural Hazards
  - Air and Surface Traffic
  - Joint Tenants
  - Existing Boundary Protection

Physical Security

- Computer Facility Requirements
  - Backup power
    - Alternate Feeds
    - UPS (failsoft)
  - Emergency Power Generator
    - Lighting
    - Physical Access Control
    - Fire Protection System
    - Computer equipment
    - HVAC
    - Communications Equipment

Physical Security

- Computer Facility Requirements (Cont)
  - Humidity Controls
  - Air Quality (dust)
  - Water Protection

Physical Security

- Industry Standards
  - Fencing
    - 3’-4’—deter casual trespasser
    - 6’-7’—deter young vandals
    - 8’ + with 3 strand barbed wire—deter determined intruder
  - Lighting
    - Street lights—deter casual trespasser
    - Flood lights—deter young vandals
    - Fresnel Units—deter determined intruder

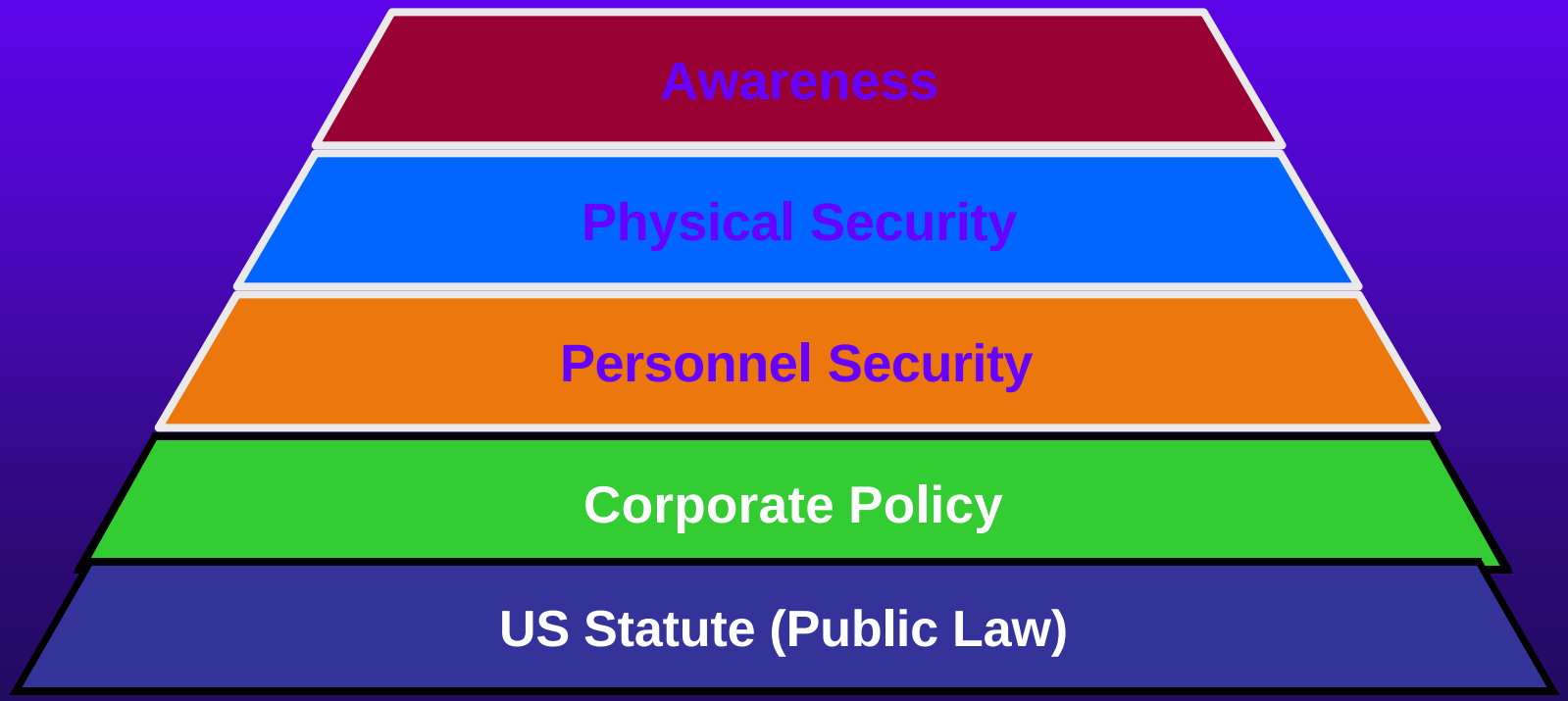
Physical Security

- Industry Standards (cont)
  - Fire classes
    - A-Common combustibles (wood, paper, etc)
    - B-Liquid (petroleum products, coolants etc)
    - C-Electrical equipment (computers, wires etc
    - D-Magnesium/Sodium

Physical Security

- Summary

- Physical security alone won’t hack it
- Fortress mentality won’t work anymore
- Keeping the bad guys out is not enough
- New technologies make it a moving target


Awareness
Physical Security
Personnel Security
Corporate Policy
US Statute (Public Law)

IA AWARENESS

Principals

- Must be based on organization's security policy
- Base awareness priorities on actual security needs
- Target awareness messages to the audience
- Must be comprehensive
- Must be interesting, current, and timely

IA AWARENESS

Elements

- Behavior
  - OBJECTIVE: affect human behavior
  - OBJECTIVE: change user attitude
  - User affected by behavior of management
- Accountability
  - Dissemination
  - Enforcement

IA AWARENESS

- Awareness
  - Stimulate
  - Motivate
  - Remind
- Training
  - Tech skills
- Education
  - Specialized
  - In-depth
  - Career development oriented

IA AWARENESS

	AWARENESS	***TRAINING***	***EDUCATION***
ATTRIBUTE	"What"	"How"	"Why"
LEVEL	Information	Knowledge	Insight
OBJECTIVE	Recognition	Skill	Understanding

IA AWARENESS

- Implementation
  - Identify scope, goals, and objectives
    - Awareness, Training, Education—who needs it?
  - Identify training staff
    - Normally just you
  - Identify target audience
    - Management
    - General User
    - MIS professional

IA AWARENESS

- Motivate management and employees
  - Example of motivation for managers

- Administer the program
  - Methods
  - Topics
  - Materials
  - Evaluate the program

IA AWARENESS

- Administer the program
  - Topics –tailor for relevance
    - Threats
    - Federal laws that apply
    - Where to report security incidents
    - Specific policies
  - Materials
    - Must be interesting
    - Must be varied
    - Must be credible

IA AWARENESS

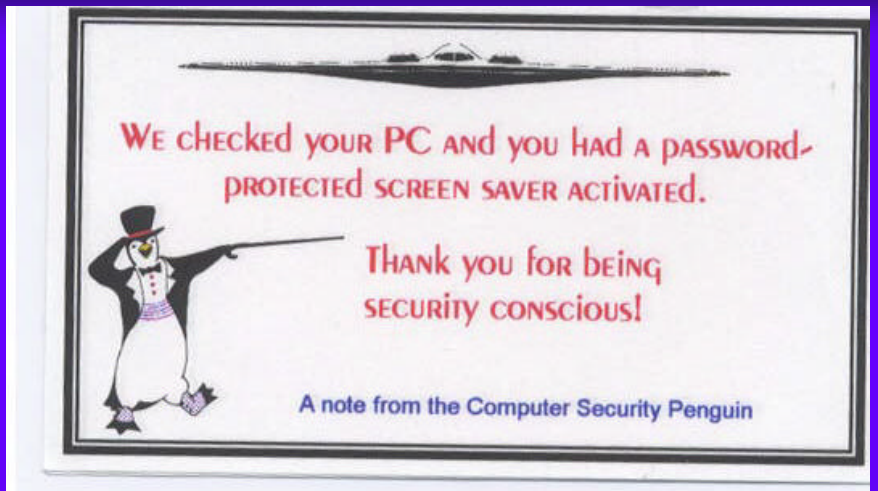
- Methods
  - Get something identifiable

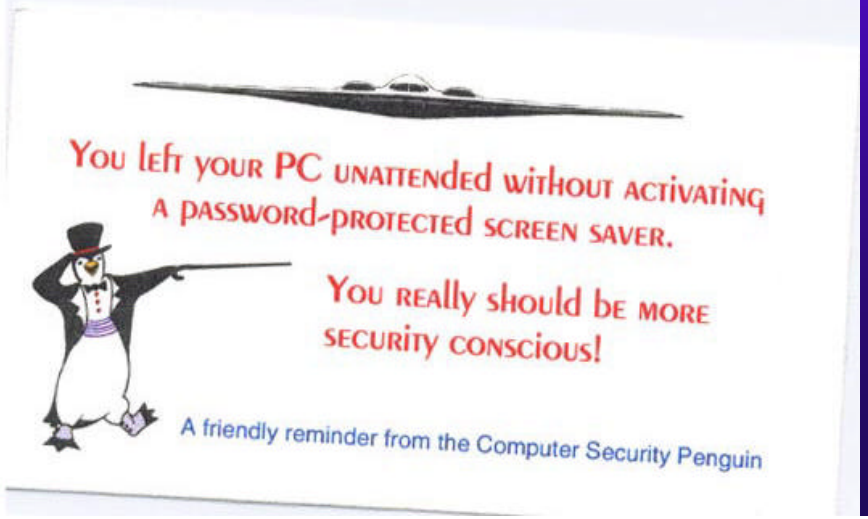
IA AWARENESS

- What employees must be aware of
- Local Threats
- How to identify and protect sensitive info
- Rules for storing, labeling, and transporting
- Federal Laws (HIPAA, GLB, copyright)
- Where to report incidents
- Specific policies (email, internet use)

IA AWARENESS

- Implementation Options
- Posters/Cartoons
- Motivational slogans
- Videos
- Classroom instruction
- CBT
- Brochures/flyers
- Trinkets
- Email Notices
- Contests
- Walk-arounds


We checked your PC and you had a password-protected screen saver activated.
Thank you for being security conscious!
A note from the Computer Security Penguin


You left your PC unattended without activating a password-protected screen saver.
You really should be more security conscious!
A friendly reminder from the Computer Security Penguin

IA AWARENESS

- Awareness program need not be
  - Expensive
  - Complicated
  - Overly technical

- Apply the KISS Principle
  - *KEEP IT SIMPLE STUPID*

IA Awareness

- Program should be
- Led by example from management
- Simple
- Positive
- Motivating (example)
- A continuous effort
- Repetitious for important items
- Humorous—to the extent of being camp
- Informative

IA Awareness

- Types of Employee Reactions
- Positive
- Passive Resistance
- Active Resistance

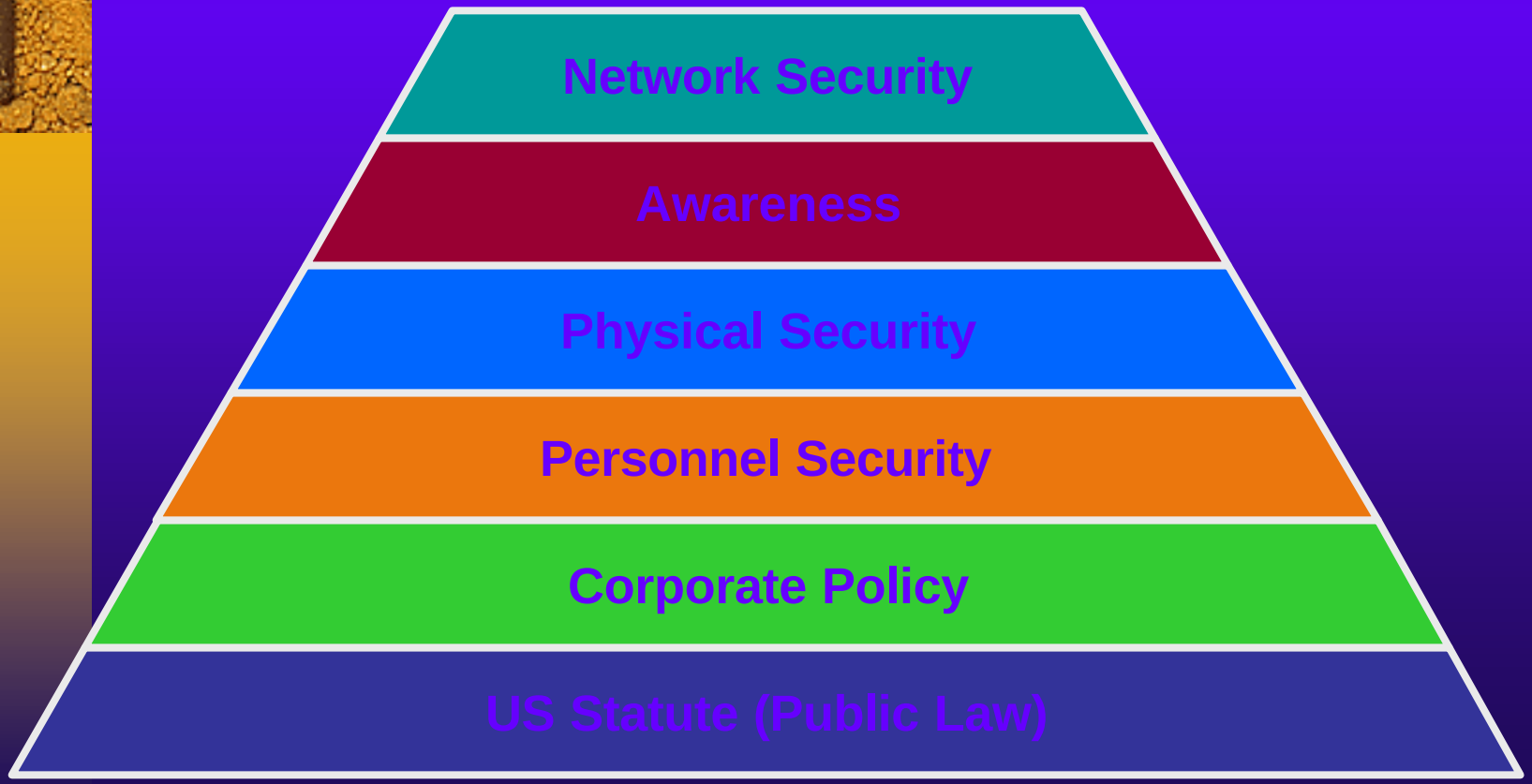
- Most employees want to do what is right, you need to convince the others

IA Awareness

- Evaluation
- Survey or questionnaire
- Ask others
- Track the # and types of incidents
- Spot checks of behavior
- Track attendance at training
- Use automated tools (L0phtCrack)

IA Awareness

- START EARLY AND SPREAD THE MESSAGE OFTEN
  - The Cage, Bird, and the Bat
  - (Precautions are useless after crisis)


Network Security
Awareness
Physical Security
Personnel Security
Corporate Policy
US Statute (Public Law)

Open System Interconnect (OSI) 7 Layer Model

APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

DATALINK

PHYSICAL

OSI MODEL

- Network devices provide different levels of security depending on how high up the protocol stack they can read.

Physical Layer

Function

- Transmission Media
  - Fiber
  - Coax
  - Twisted Pair
  - Cat 5

Security

- Provides confidentiality only

Datalink Layer

Function

- Error detection and correction between adjacent nodes
  - checksums

Security

- Provides confidentiality and integrity

Network Layer

Function

- Routing, access control and data integrity

Security

- Provides integrity, confidentiality and authentication

Transport Layer

Function

- Data integrity, end to end error detection and correction

Security

- Integrity, authentication, and confidentiality

Session Layer

Function

- Manages sessions between applications

Security

- No security function associated

Presentation Layer

Function

- Converts information into standard form for applications

Security

- Authentication and confidentiality

Application Layer

Function

- Data modeling, file management

Security

- Non-repudiation

Firewalls

- MAIN FUNCTION—centralize access control
  - Can also be used to
- Block unwanted traffic
- Hide vulnerable systems
- Log traffic
- Hide information like system names
- Provide more robust authentication

Firewalls

- ARE NOT THE PANACEA OF SECURITY
- They can only reduce the risk of breech of security

Firewalls

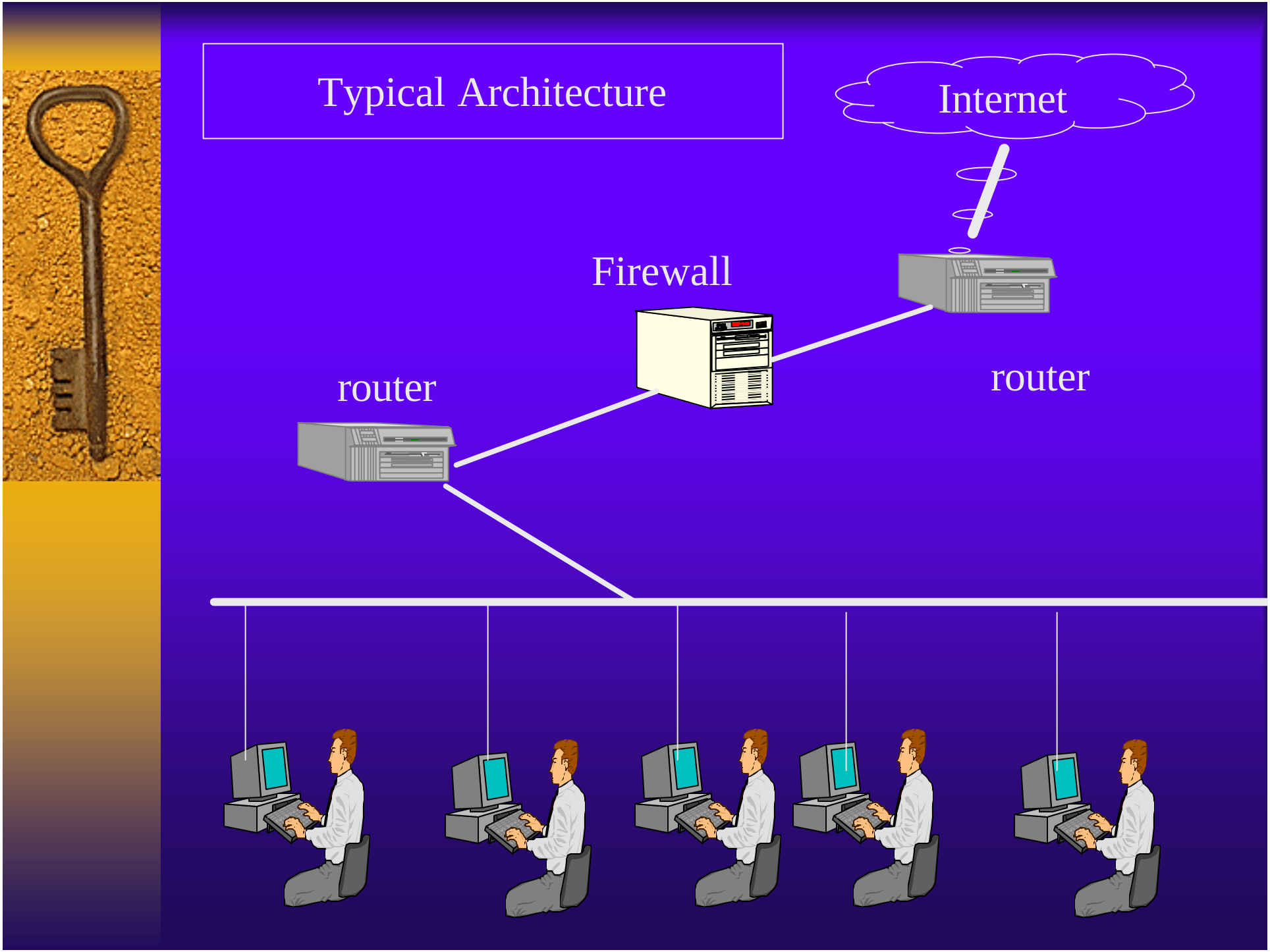
- Types
- Packet filtering gateways
  - Use routers to grant or deny access based on source address
- Application Gateway
  - Most secure type
  - Uses Proxies
- Hybrid
  - Mixture operated in series

Filtering Gateways

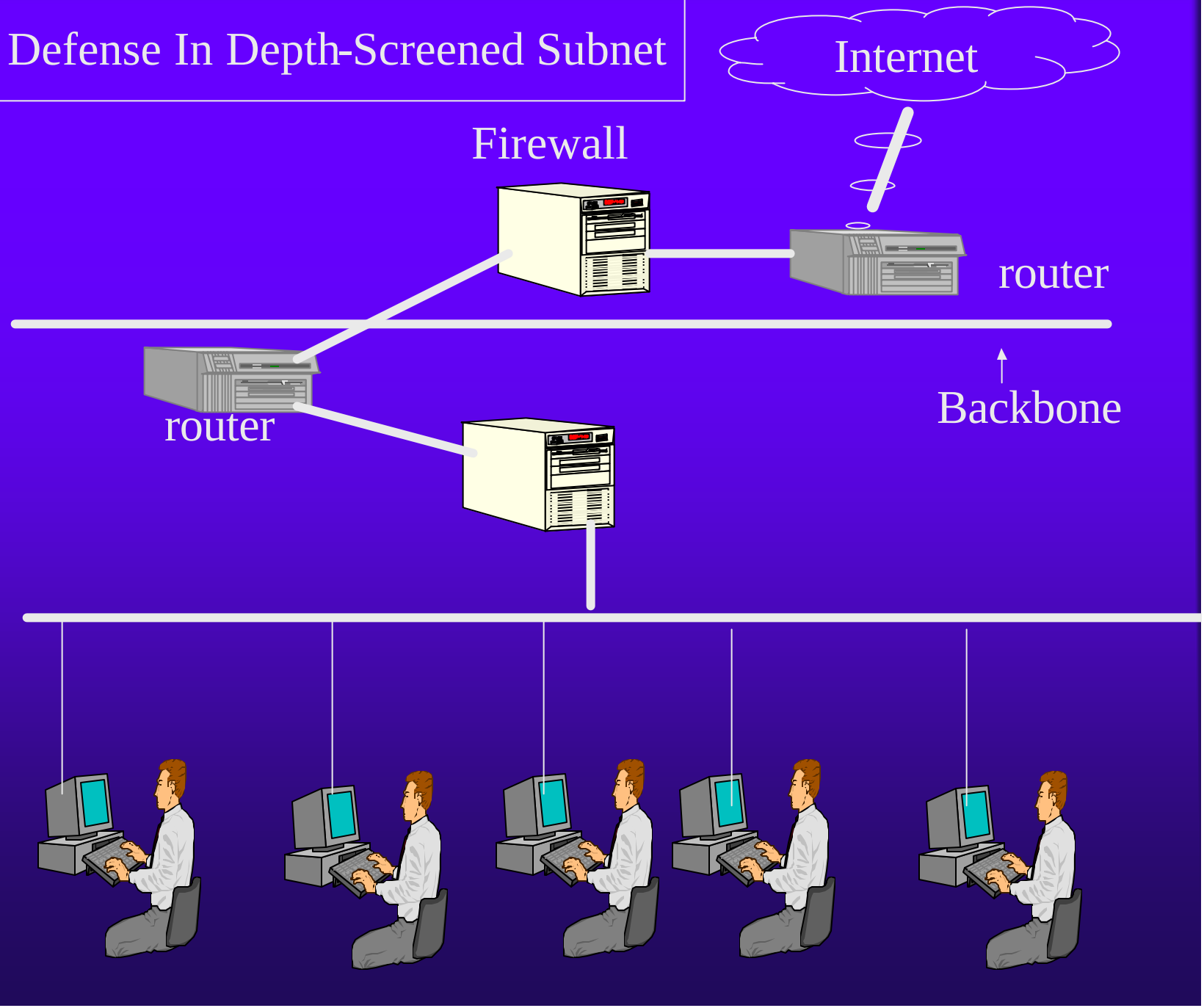
- Have inherent risks
  - Don’t protect against address spoofing
  - Attacker has direct access to the host, once he is granted access
  - Strong authentication is not supported
  - Provides little or no useful logging

Firewall Comparisons

Firewall Architecture	High Risk Environment (hospitals)	Medium Risk Environments (universities)	Low Risk Environments (florist shop)
Packet Filter Gateway	Unacceptable	Minimal security	Recommended
Applications Gateway	Effection Option	Recommended	Acceptable
Hybrid Gateway	Recommended	Effective	Acceptable


Typical Architecture
Internet
Firewall
router
router

Defense In Depth-Screened Subnet



Router vs. Firewall

Router	Firewall
♦ Filter certain packets based on criteria such as IP address	♦ Stops all packets
♦ Process up through network layer	♦ Process through the applications layer

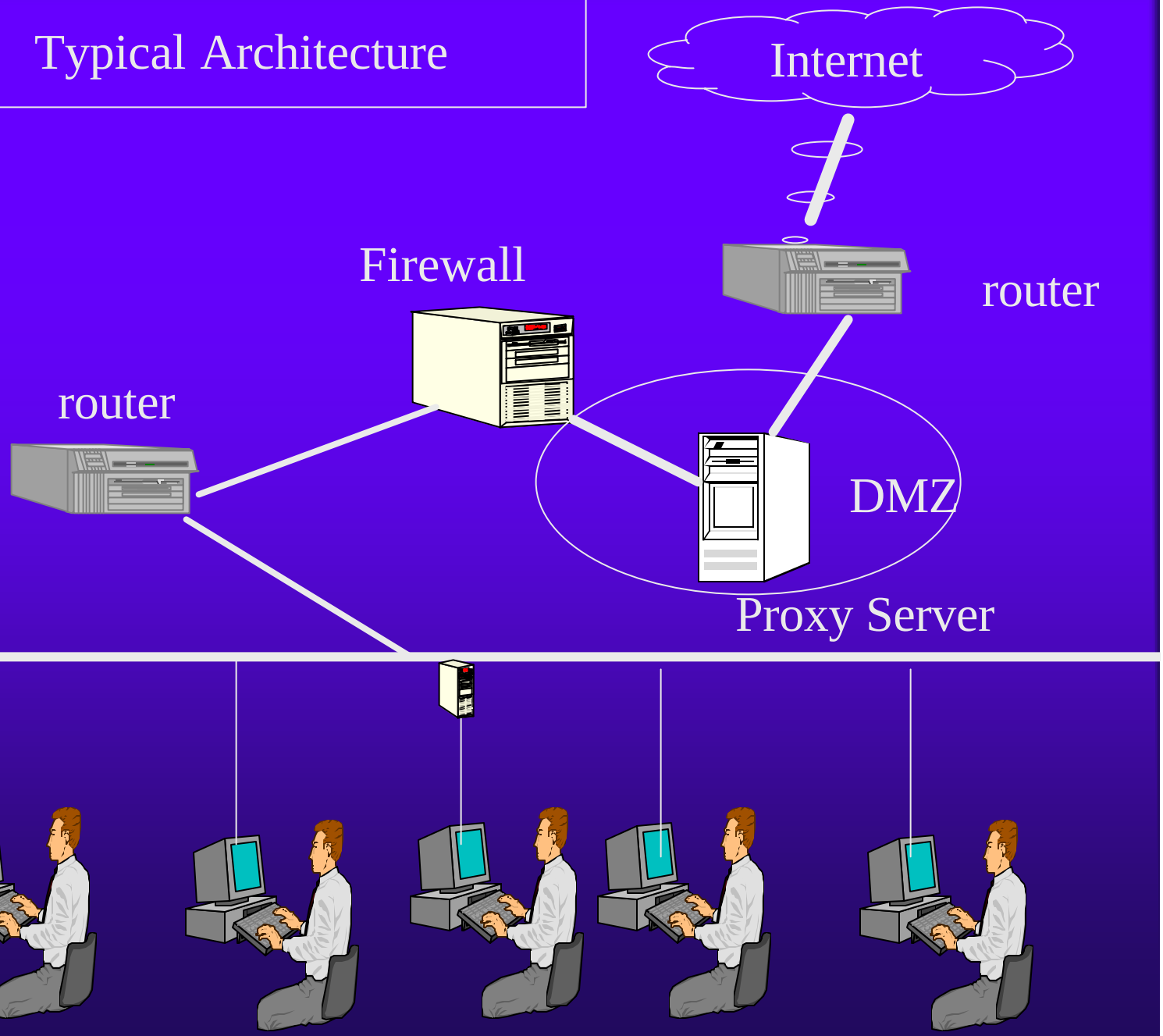
Firewall Criteria

- Only minimal services permitted (Deny all, permit by exception)
- Log everything
- Only administrators have accounts on firewall

DMZ

- Location for Proxy server
- Used if company needs web presence
- Located between the router that connects to the internet and the firewall

Typical Architecture

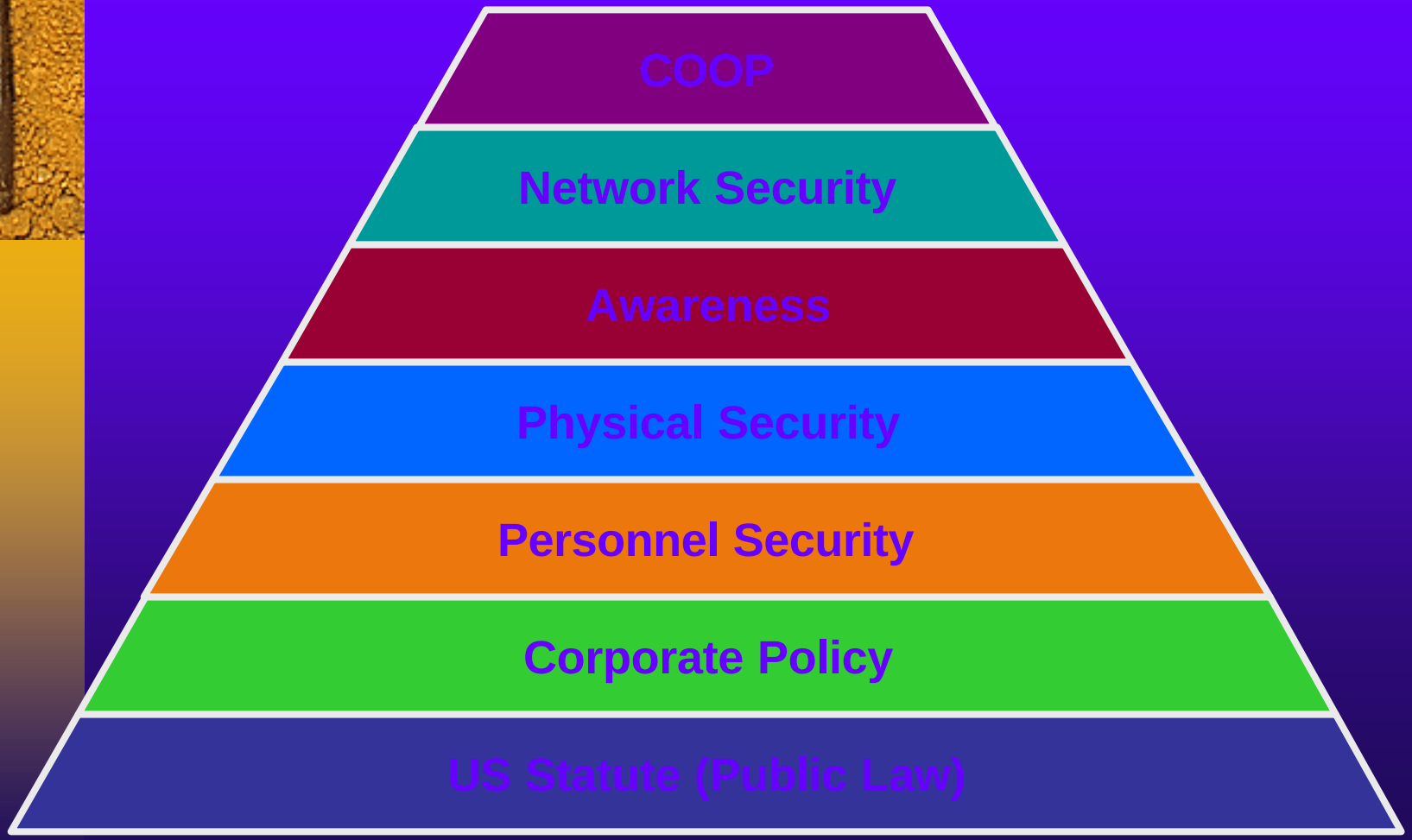


Proxy Servers

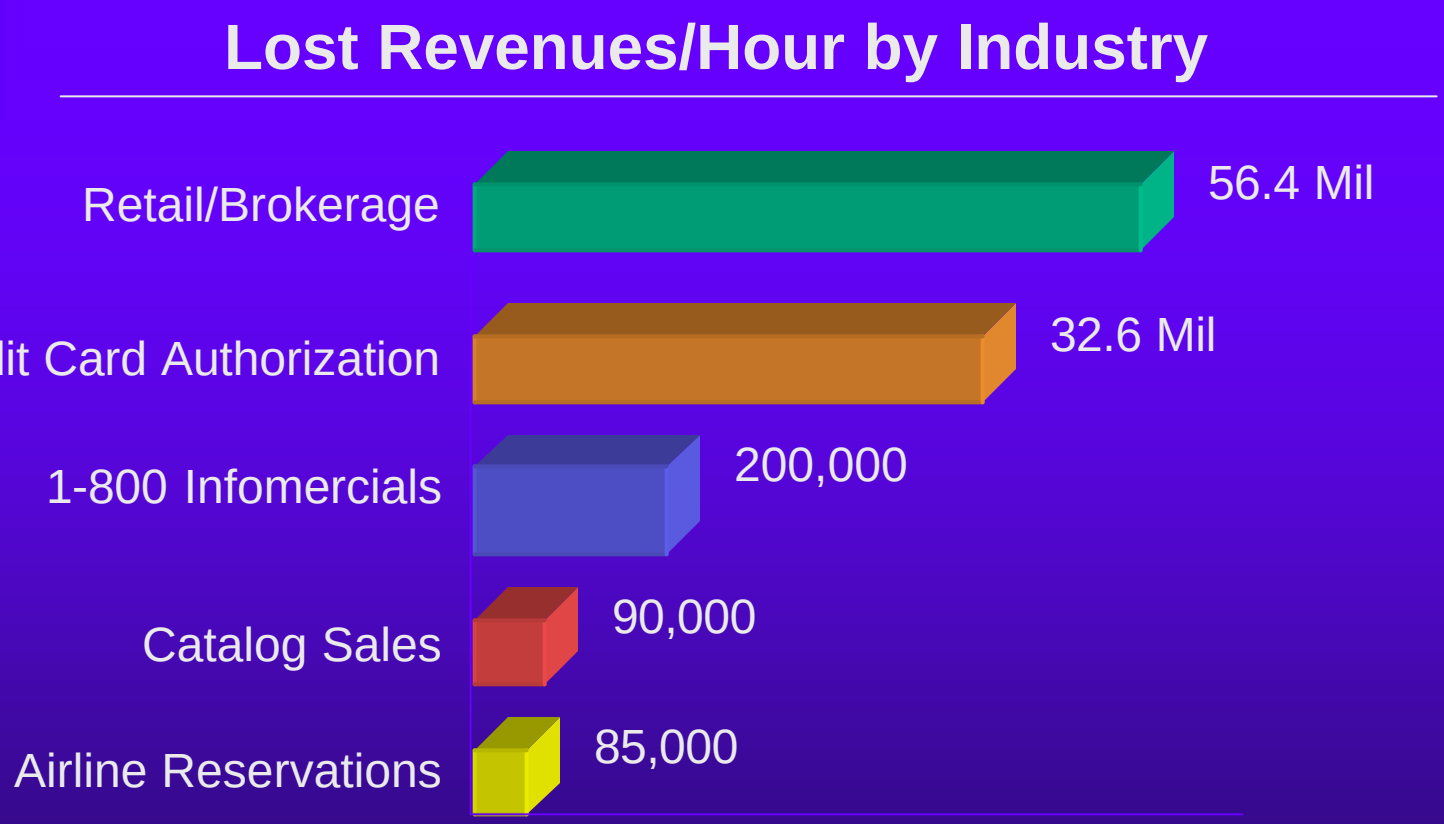
- Used as go between for external requests for services directed at the internal network
- Proxy server evaluates all requests
  - Passes it on to the internal network
  - Discards it
- Reverse is also true

Proxy Server

- Protects company from advertising internal network scheme
- Provides Network Address Translation
- Example—Mail Proxy
  - Albert_Smith @ starwars.abc.com translates to Smith@ proxy.abc.com as it goes out to the internet
- The reverse is also true


COOP
Network Security
Awareness
Physical Security
Personnel Security
Corporate Policy
US Statute (Public Law)

Not Just an IT Issue



A University of Texas study was conducted to ascertain the financial impact of long term outages. This study found that the loss of revenue varies greatly, depending on the industry

Not Just an IT Issue

- Top 10 Major Disasters ranked by FEMA Relief Costs 1987-1996

Northridge Earthquake (CA, 1994)	5.558 Billion
Hurricane Andrew (FL, LA, 1992)	1.803 Billion
Hurricane Hugo (NC, SC, PR, VI, 1989)	1.320 Billion
Midwest Floods (IL, IA, KS, MN, MO, NE, ND, SD, WI, 1993)	1.144 Billion
Loma Prieta Earthquake (CA, 1989)	836 Million
Hurricane Marilyn (PR, VI, 1995)	542 Million
Hurricane Fran (MD, NC, PA, SC, VA, WV, 1996)	496 Million
Tropical Storm Alberto (AL, FL, GA, 1994)	433 Million
Winder Storms (CA, 1995)	372 Million
Mid Atlantic/Northeast Floods (MD, ME, NY, OH, PA, VA, VT, WV, 1996)	359 Million

OK, Sometimes It is an IT Issue

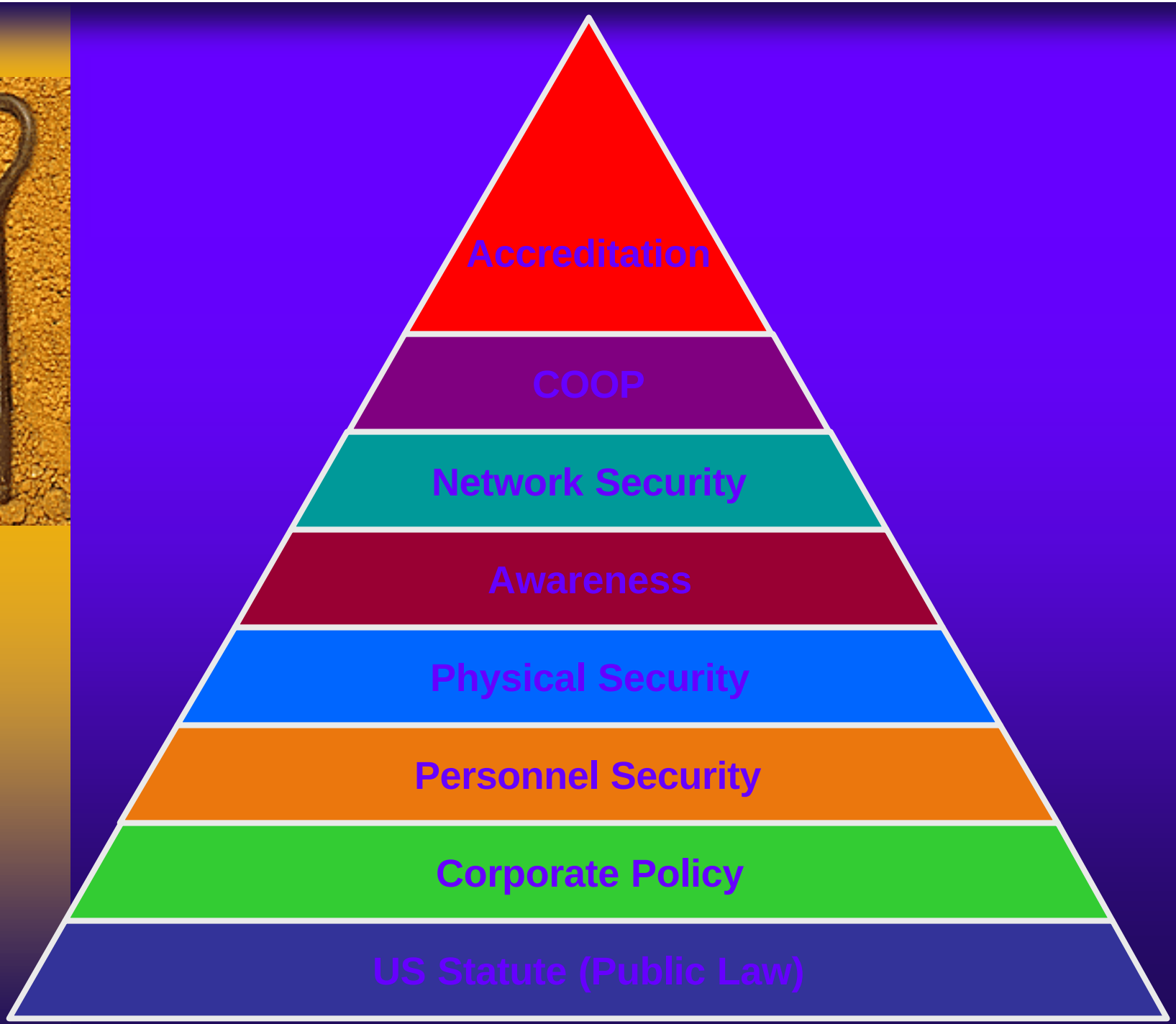
Economic impact of malicious code attacks

Year	Code Name	$ Impact
2001	Nimda	635 $M
2001	Code Red(s)	2.62 $B
2001	SirCam	1.15 $B
2000	Love Bug	8.75 $B
1999	Melissa	1.10 $B
1999	Explorer	1.02 $B

Source: www.computereconomics.com

DP Summary

- Axioms to remember
  - Business functions drive the DP plan
  - No backup -- no recovery
  - Alternate site not affected by same disaster
  - Look at worst case
  - Protect human life above all else


Accreditation
COOP
Network Security
Awareness
Physical Security
Personnel Security
Corporate Policy
US Statute (Public Law)

Accreditation

- What is it?
- Formal Declaration by a Senior Official that all actions have been taken to secure the network for the level of information being processed, that the risk is at an acceptable level and that the he/she personally accepts those risks taken in association with the operation of the network.

Accreditation

- What's involved?

- An ongoing process with IT security professionals providing certification to the accrediting authority.

Certification

Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements"*

Certification

- Certification is a security analysis in the following areas:

- Disaster Recover (Information)
- Network/Communications
- Awareness
- Physical
- Personnel
- Policy (Administrative)

Certification And Accreditation Process

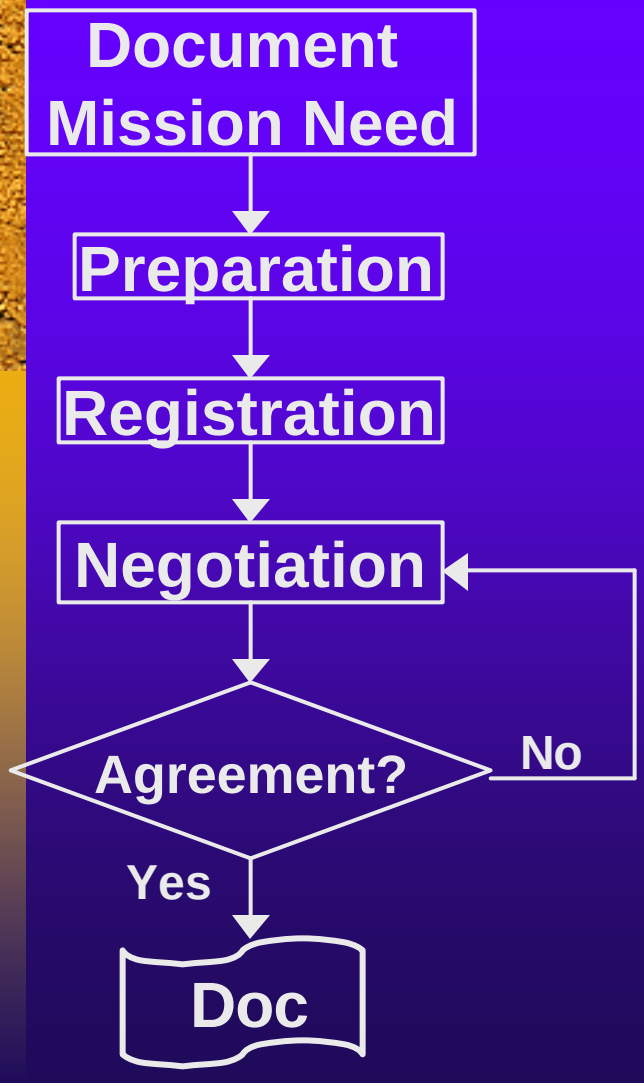
Phase 1
Definition

Phase 2
Verification

Phase 3
Validation

Phase 4
Post Accreditation

Definition Phase

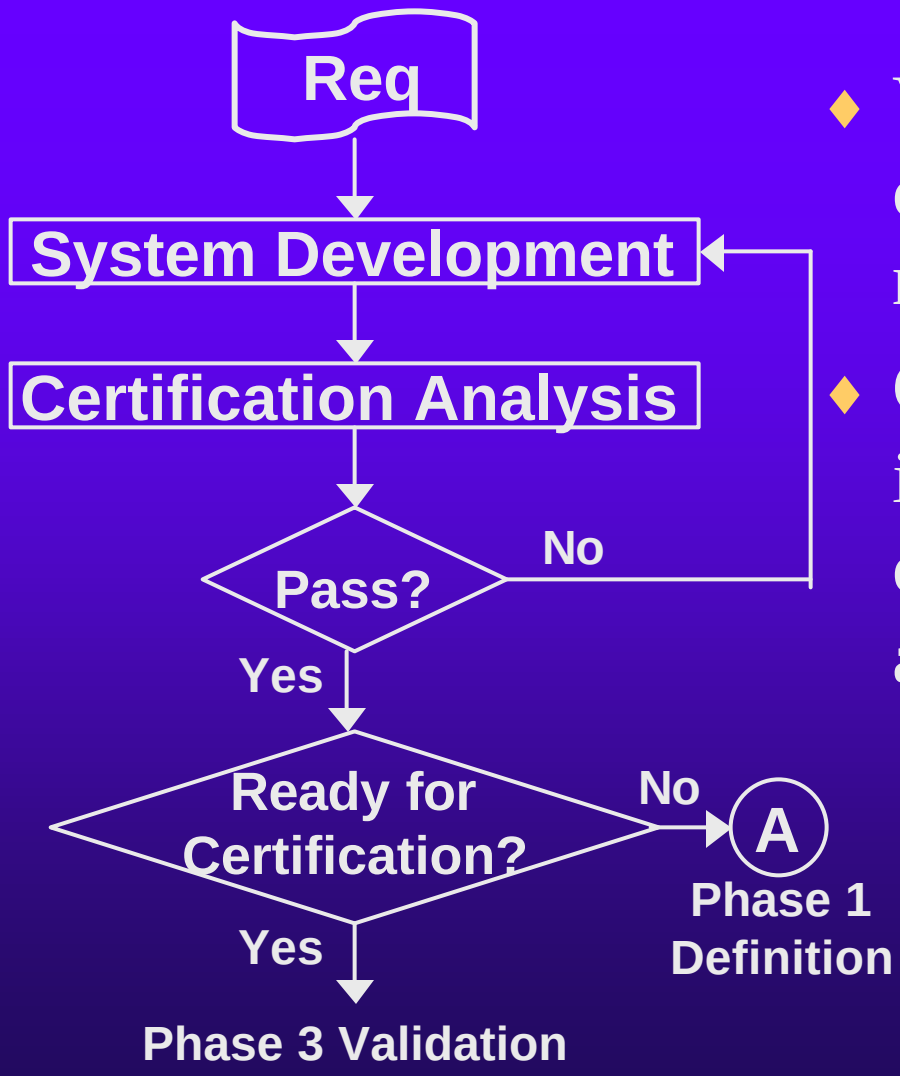


- Key players agree on the intended system mission, security reqs, C&A boundary, schedule, level of effort, and required resources
- Agreement is documented in the Basic document

Definition Phase

- Main tasks
- Define system functions, reqs, and interfaces
- Define information category and classification
- Prepare the system architecture description
- Identify principle C&A roles & responsibilities
- Define C&A level of effort
- Draft Main Document
- Agree on the method for implementing security requirements

Verification

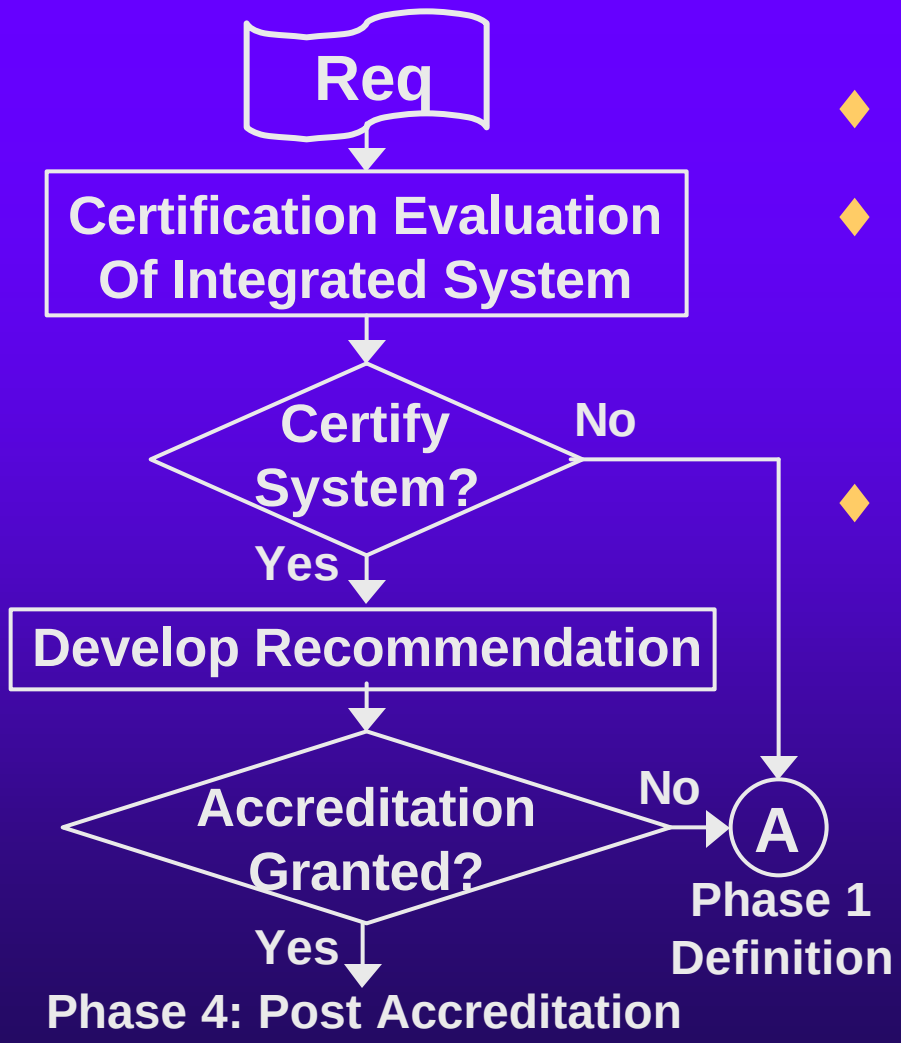


- Verify system's compliance with stated requirements
- Goal is to obtain integrated system for certification testing and accreditation

Verification Phase

- Main tasks
- System Architecture Analysis
- Software Design Analysis
- Network Connection Rule Compliance
- Integrity Analysis of Integrated Products
- Life Cycle Management Analysis
- Security Reqs Validation Procedures
- Vulnerability Evaluation

Validation



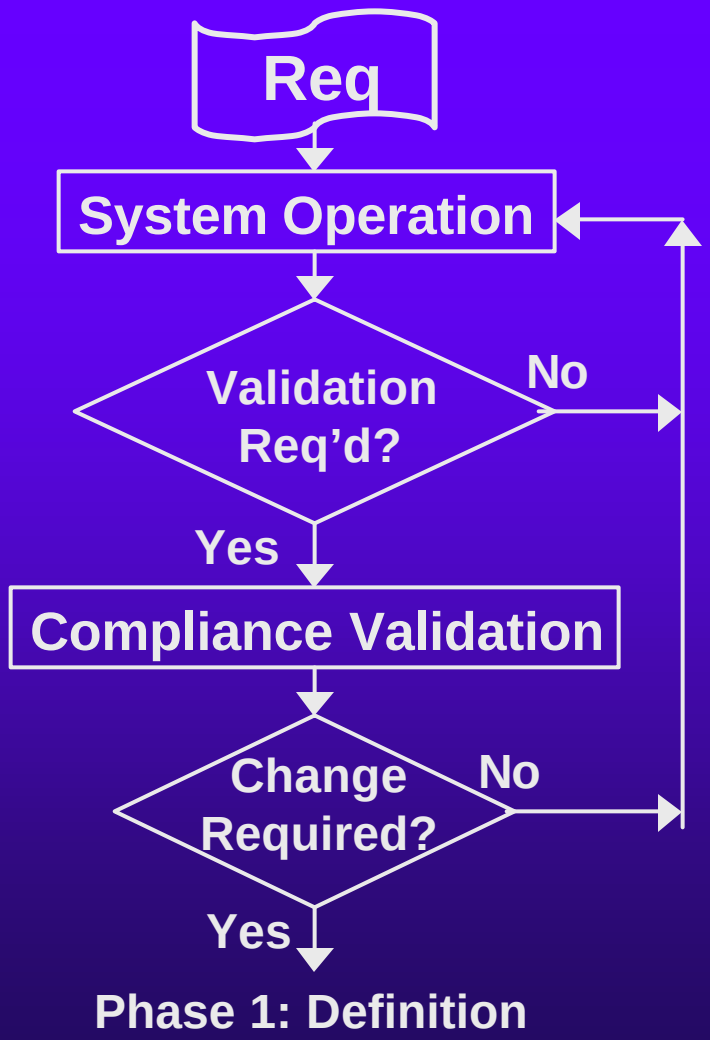
- System on-hand
- Validates system compliance with security reqs
- Goal is to obtain full approval to operate system (accreditation)

Validation

♦ Main Tasks

- ST&E
- Penetration Testing (Exploitation, Insider/Outsider)
- COMSEC Compliance Evaluation (Reqs, Integration)
- System Management Analysis (Maintain Mgmt/CM/Arch)
- Contingency Plan Evaluation (Backup, COOP…)
- Site Accreditation Survey
- Risk Management Review
- Develop Certification Report and Recommendation for Accreditation:
- Ends with accreditation decision

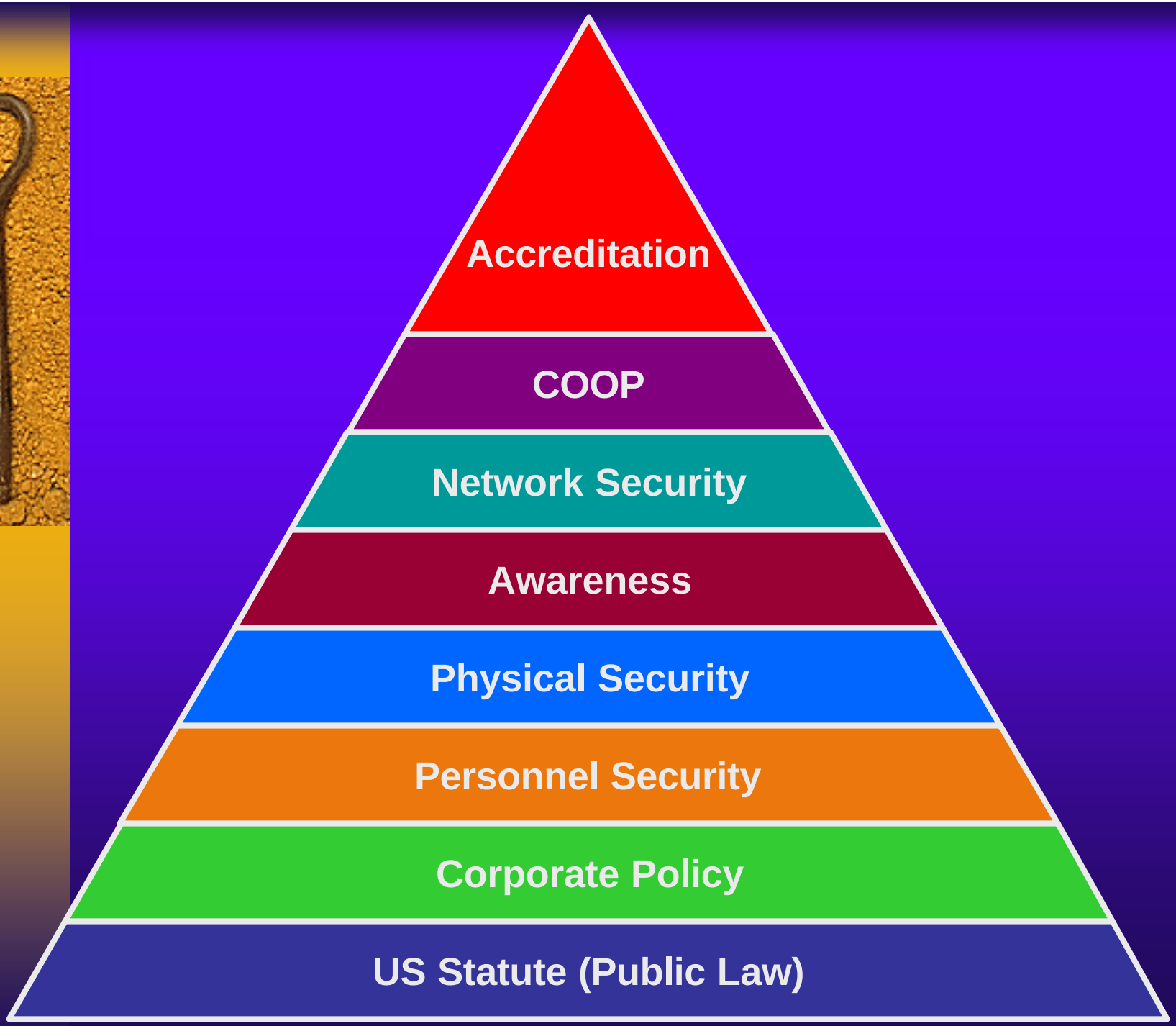
Post Accreditation



- Starts after site accreditation
- Objective is to maintain an acceptable level of residual risk
- Certification responsibilities shift to site/O&M Orgs
- Ends with system termination

Post Accreditation

- Main Tasks
- Review configuration & security Mgmt Follow change mgmt documented in basic plan
  - Determine if system security mgmt continues to support mission and architecture
- Conduct risk management review
  - Assess if risk to system is being maintained at an acceptable level
- Conduct compliance validation if needed
  - Ensure continued compliance requirements, current threat assessment, and concept of operations
- Maintain basic documentation


Accreditation
COOP
Network Security
Awareness
Physical Security
Personnel Security
Corporate Policy
US Statute (Public Law)