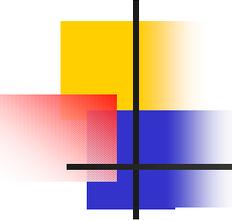


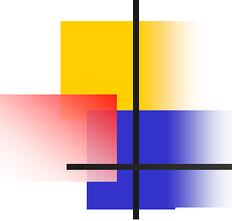
Information Security Policy

Steve R. Hutchens, CISSP
EDS, Global Leader, Homeland Security



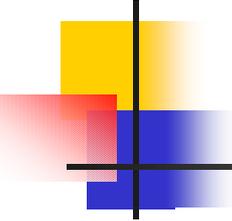
Agenda

- Security Architecture
 - Threats and Vulnerabilities
 - Design Considerations
- Information Security Policy
- Current Legislation
- Security Policy Benefits
- Questions



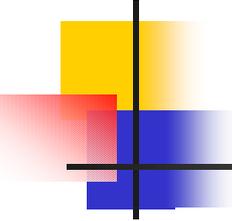
Definitions

- Threat – a possible danger to a computer system
 - Active threat – alteration, not just interception, of information (ie. Changing information in transit – authenticity)
 - Passive threat – interception, without alteration, of information (ie. Wire tap, eavesdropping, monitoring - confidentiality)
- Source: Computer Security Basics, O'Reilly & Associates



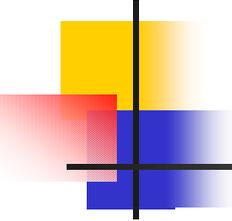
Definitions

- Vulnerability – a weakness in a computer system that may be exploited to violate system security
 - Example: software error / function
(ie. Visual Basic file execution on Microsoft e-mail message)
 - Configuration setting on a firewall
 - Undocumented features
 - Errors in software that permit access
 - Functions that are used for purposes other than intended

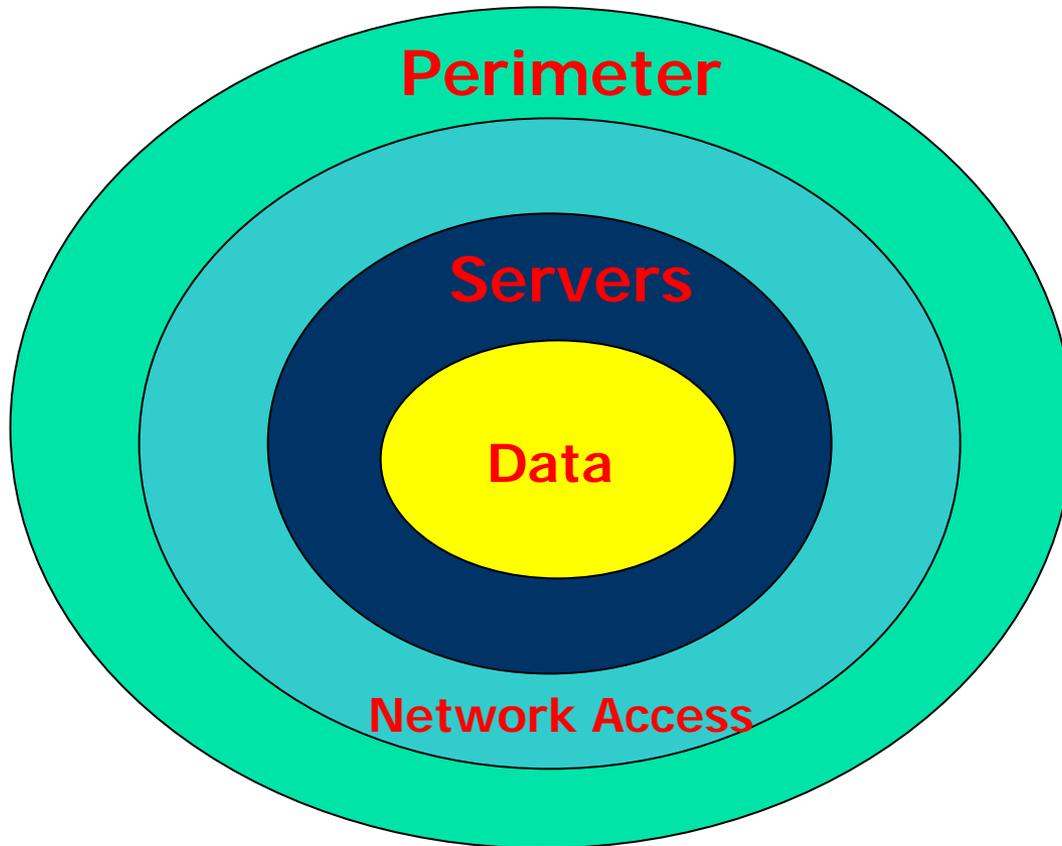


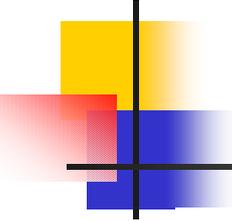
Security Architecture

- Minimize Threats to Systems
- Minimize Vulnerabilities / Exposures of Systems
- Defense in Depth Strategy
 - People
 - Technology
 - Operations
- Layers of Security Technology
 - Network Perimeter
 - Communication Technology
 - Server / Applications Technology
 - Server / Database Technology



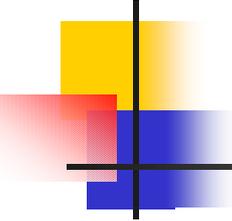
Security Architecture





Security Architecture

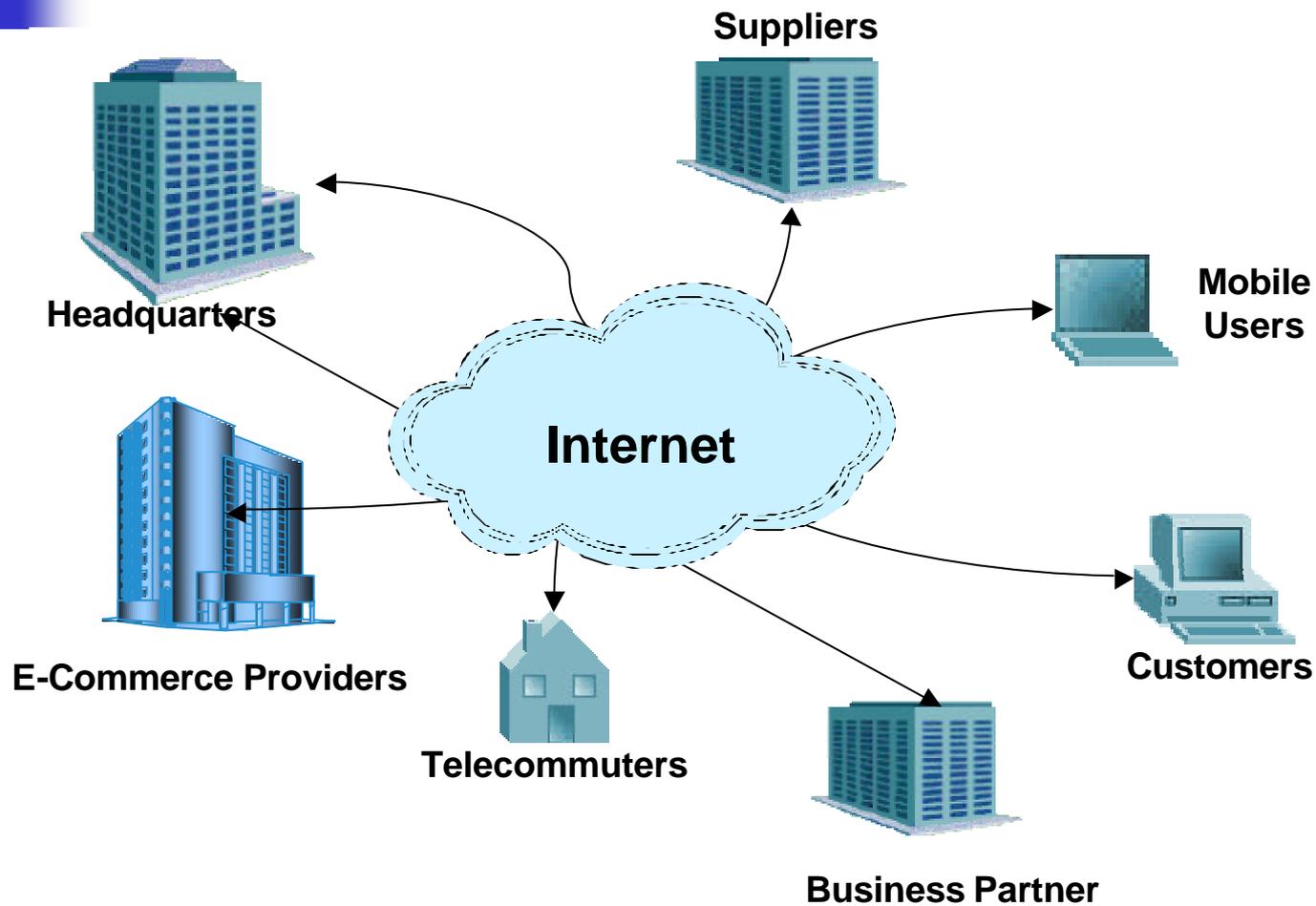
- People
 - Security Policy Support
 - Roles (Job function, Need to Know)
 - Identification and Authentication
 - Password Management
 - Biometrics / Smartcards
 - Digital Certificates
 - Access Control (Read, Write, Run Apps)



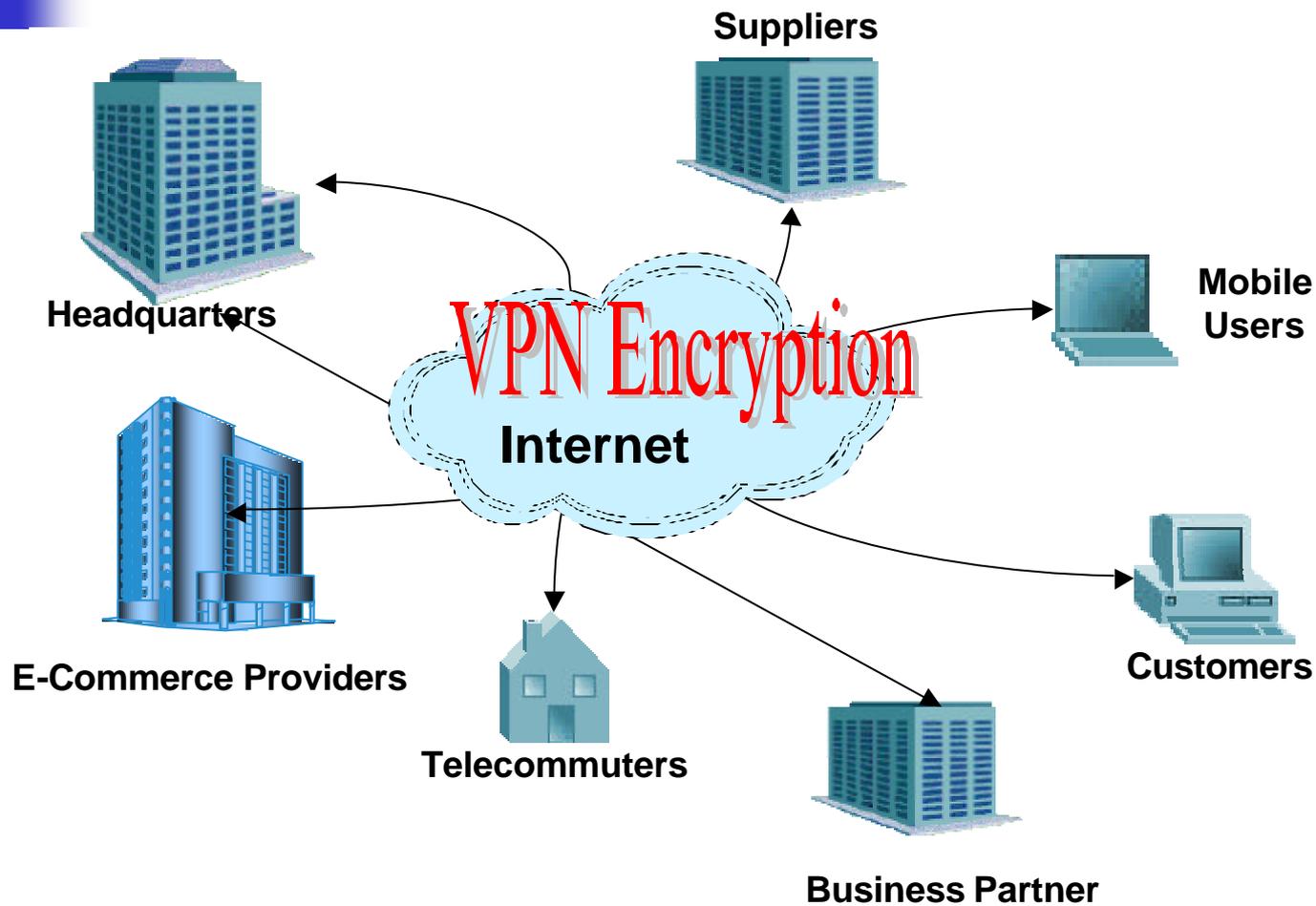
Security Architecture

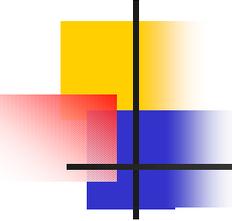
- Technology
 - Security Policy Support
 - Virus Protection
 - Firewall Systems Technology
 - Intrusion Detection
 - Host-based Intrusion Detection Systems
 - Network-based Intrusion Detection Systems
 - Virtual Private Networks
 - Encryption

Security of Connections



Security of Connections

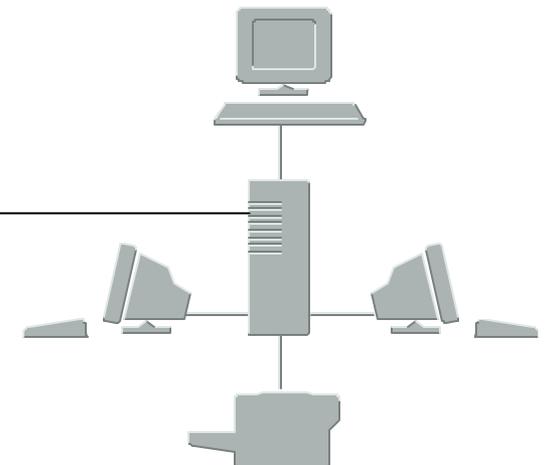
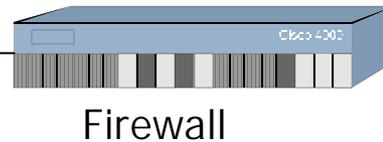
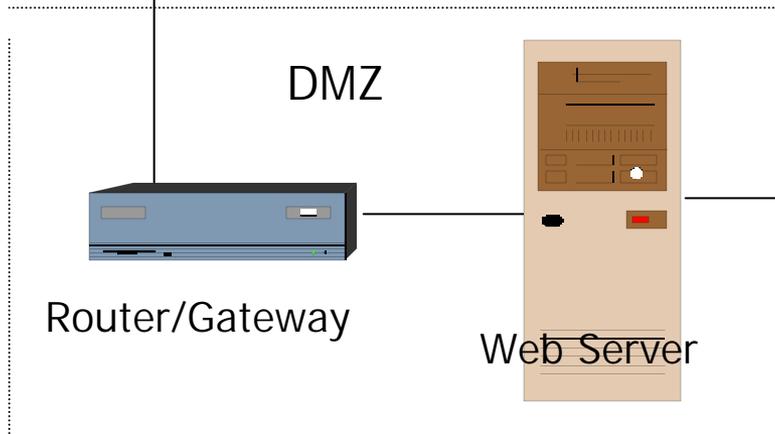
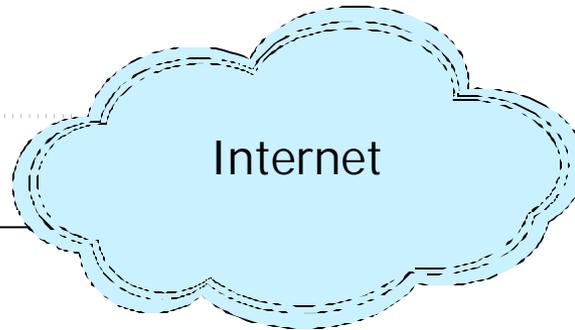


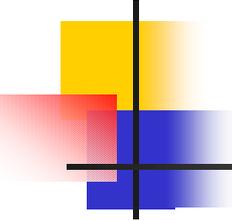


Security Architecture

- Technology
 - Network Devices (routers, switches, etc.)
 - E-mail Servers
 - Encryption (data & transport)
 - Wireless LAN (secure)
 - Demilitarized Zones

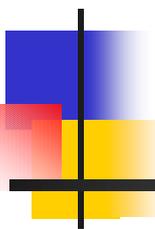
Demilitarized Zone (DMZ)





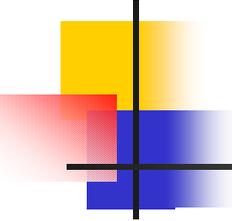
Security Architecture

- Operations
 - Operations Procedures
 - Disaster Recovery Planning & Testing
 - Security Awareness Training
 - Best-practices for Security Management
 - Patches / Updates Maintenance
 - Technology Refresh



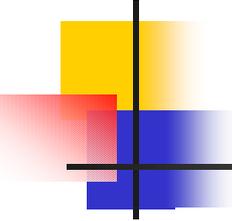
Information Security Policy

Defining Rules and Regulations



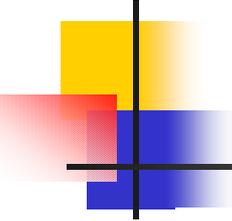
Policy Guidelines

- National Institute of Standards and Technology
- Industry Groups
 - SANS Institute – (SysAdmin, Audit, Network, Security)
- National Security Agency (NSA) for Government Systems
- Department / Agency Specific



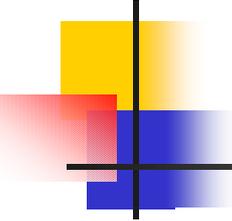
Security Policy

- Effective Policy must Support Organizational Goals and Objectives
- Policy must Support Controls Necessary to Organizational Integrity:
 - Management Controls (Risks)
 - Operational Controls (People and Procedures)
 - Technical Controls (Systems)



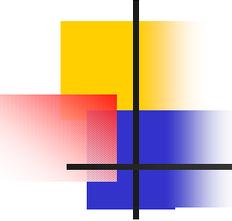
Security Policy

- Policy may address these issues:
 - Duty of Loyalty
 - Conflict of Interest
 - Duty of Care
 - Least Privilege
 - Separation of Duties / Privilege
 - Accountability
 - Management Objectives



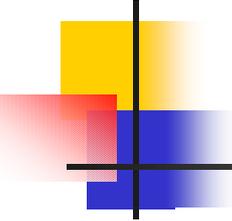
Types of Policy

- Regulatory
- Advisory
- Informative
- Corporate versus Departmental



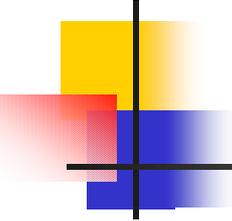
Laws, Directives and Regulations

- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Federal Information Security Management Act of 2002 (FISMA)
- Gramm-Leach-Bliley Act of 1999
- Computer Fraud and Abuse Act
- Federal Privacy Act of 1974
- European Union Principles on Privacy
- Computer Security Act of 1987
- Security and Freedom Through Encryption Act
- Economic Espionage Act of 1996



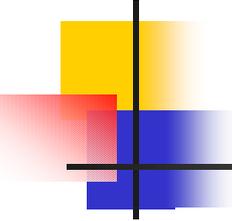
Security Policy Benefits

- Policy regarding IT refresh:
 - Old disk drives (wipe or destroy?)
 - Desktop standards enforcement
- E-mail policies
 - Warning banners
 - “Acceptable use” of e-mail systems
- Theft of IT Assets
 - Protection of stored information
- System Upgrades / Maintenance
 - Authorized individuals
 - Testing and Evaluation



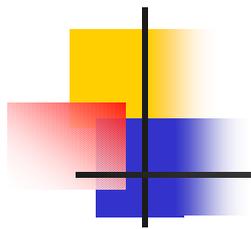
Security Policy Benefits

- User Access Control
 - Password Policy (Example)
 - Minimum length of 8 characters
 - Combination of numbers, letters and special characters (2day!sgr8)
 - Force Password Change every 30 days
 - Not a common word (Name, Date of birth, family member names, sports, etc.)
 - Biometrics
 - Strong Authentication
 - Iris, Face, Finger



Security Policy Benefits

- Computer Crime Investigations
 - Policy establishes “what’s expected” of employees
 - Policy establishes rights and privileges
- Computer Misuse
 - Violations of “acceptable use policy”
- Criminal Activities
 - Fraud
 - Espionage
 - Copyright violations (music, graphics)
- Civil activities
 - Intellectual property violations
 - Activist groups, many others...



Thank You!