Overall Network Security

Daniel J. Nealis

Overall Network Security

What does Network mean?

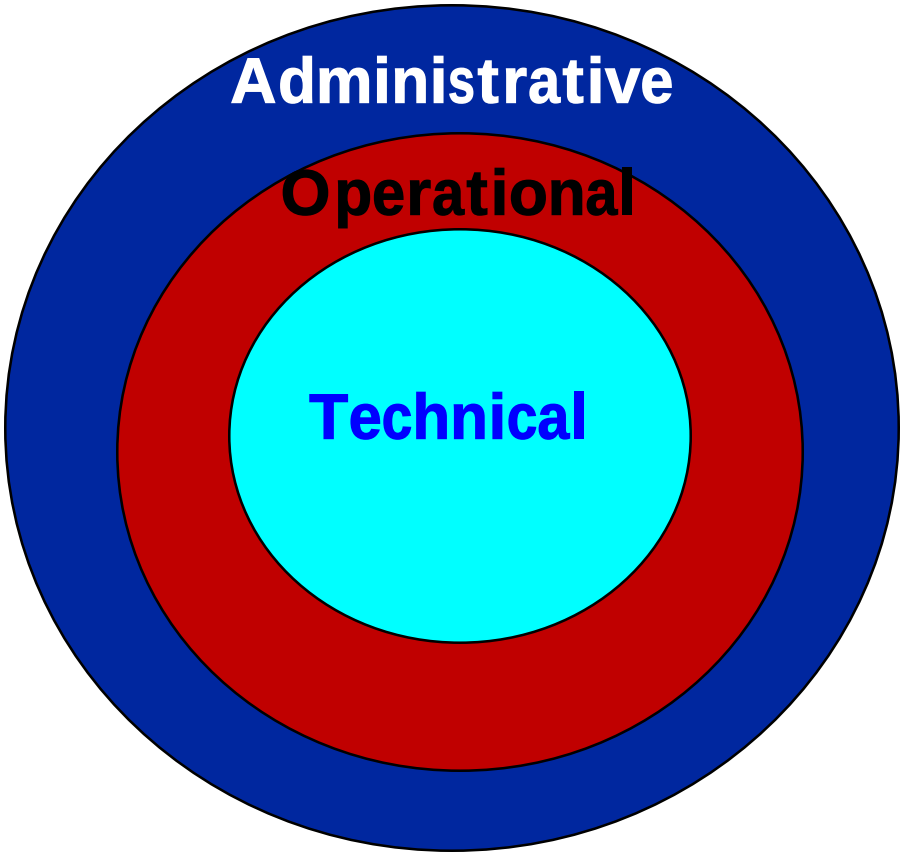
- Bridges/routers/hubs
- Firewalls
- Ethernet/Token Ring/Frame Relay/Switched Networks
- Public vs. Private Networks
- Internet/Extranet/Intra net

Or

- Broader concept of "End -to- End" Security
- Customer to institution and beyond

Overall Network Security

Needs to focus on

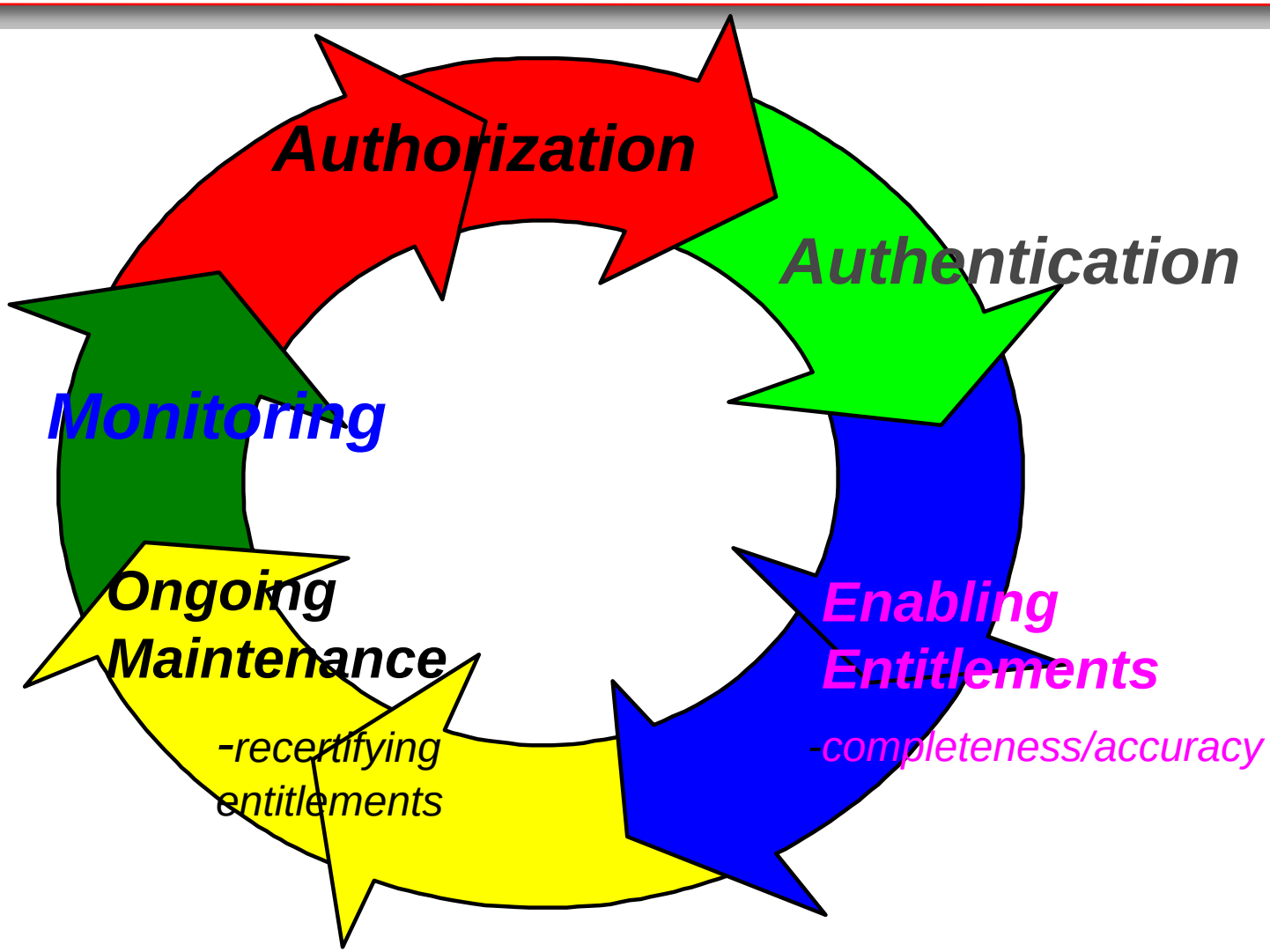


End to end perspective

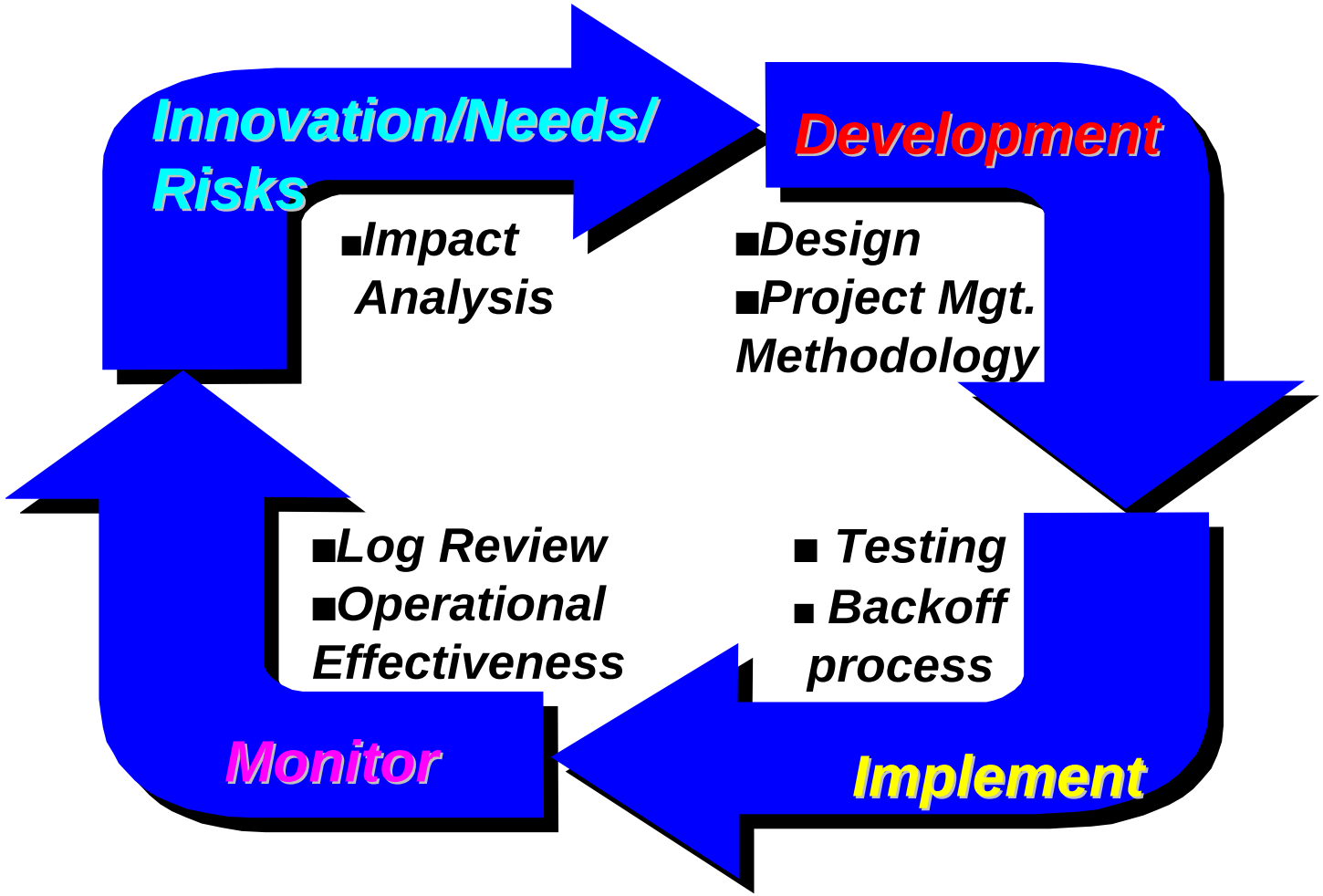
Administrative

- **Tone at the Top**
- **Culture of the Organization**
  - Security co-equal with revenue
  - Viewed from an enterprise perspective
  - Impact on Brand (Reputational risk)
- **Responsibility clearly defined**
  - Corporate
  - Line of Business
  - Users

Operational Control Cycle



Development Control Cycle

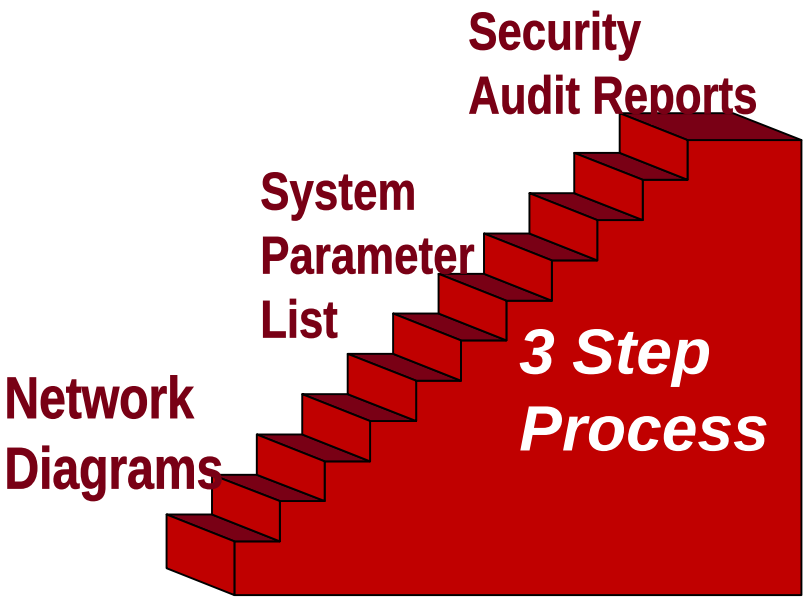


Technical Perspective

Risk Analysis

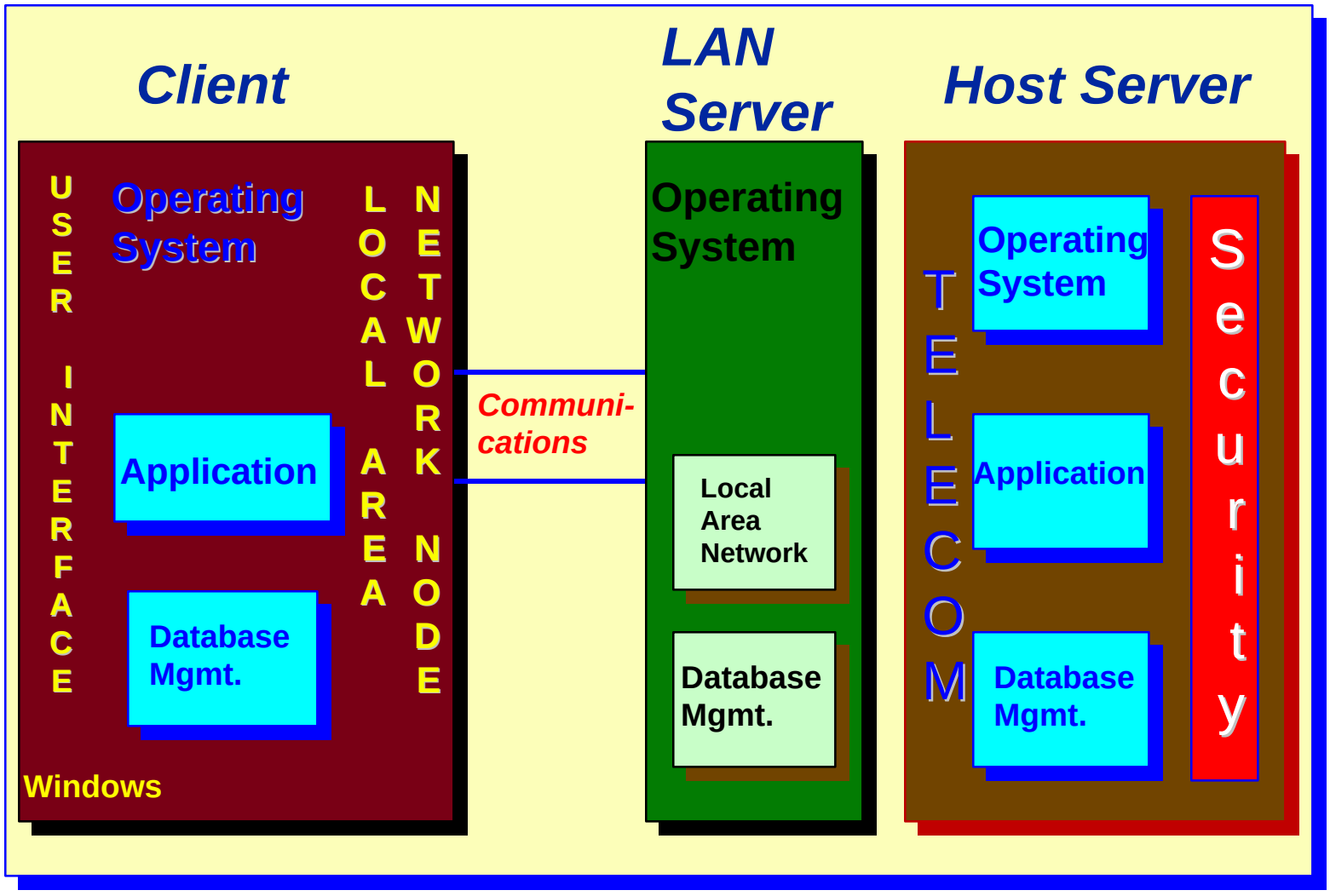
Prevent Propagation of Exposures

Address baseline requirements



- Identify points of vulnerability
- Institute appropriate controls

Managing Risk - Challenges and Opportunities



End to End Security Considerations

CUSTOMER

- Are Chase's Policies applicable?
- What layers of security are acceptable?
  - Certificate authority
  - ID/Password
  - Tokens
  - Biometric

TRANSPORT

- Encryption
- Non-repudiation/authentication/ confidentiality/integrity

NETWORK

- Internet/Extranet/Intranet
- Components
  - Router/hubs/switch/gateways
- Remote Access
- Private vs. Public
- Connectivity

HOSTS/SERVER

- Operating System
- Program Products
- Customized Code
- Security Parameters
- Virus

APPLICATION

- Design
- Functionality
- Application level security
- Interconnectivity
- Interoperability

DATABASES

- Virus
- Access
- Online
- Support processors (administration)

DESKTOP/LAPTOP

- Operating System
- Virus
- Application Software
- Connectivity
- Locally stored data
- Laptop physical vulnerability

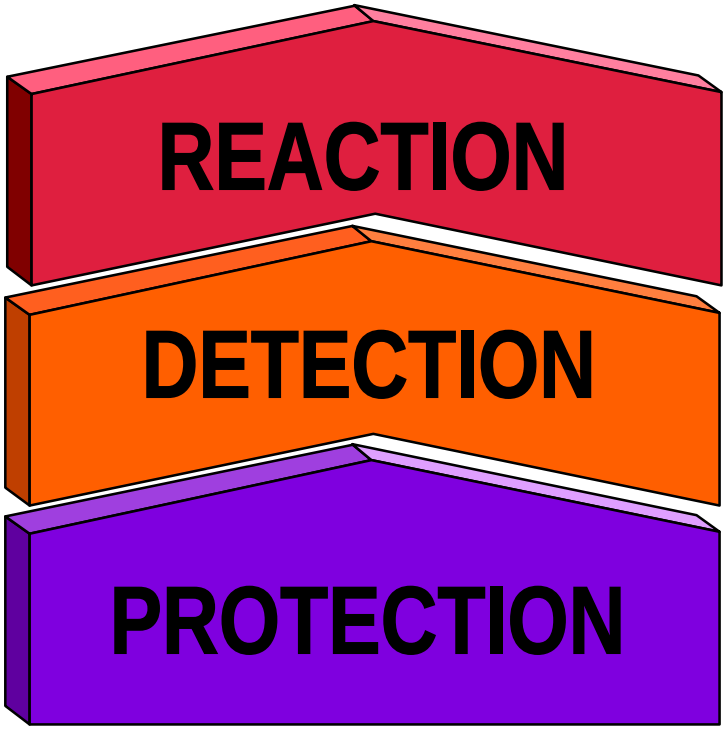
REDPLOYMENT OF ASSETS

- Data storage
- Data disposal

ARCHIVED DATA

- Physical access
- Administration
- Environmental control
- Disposal

End-to-End Security



- Customer to institution and beyond
- Monitoring of Logs
- Focus on External Exposure
- Consistent Control Practices
  - Baseline Control Paramenter Setting
  - End-to-End Security Mapping

Approach to Risk Management

Risk Management requires a comprehensive knowledge of the components of risk:

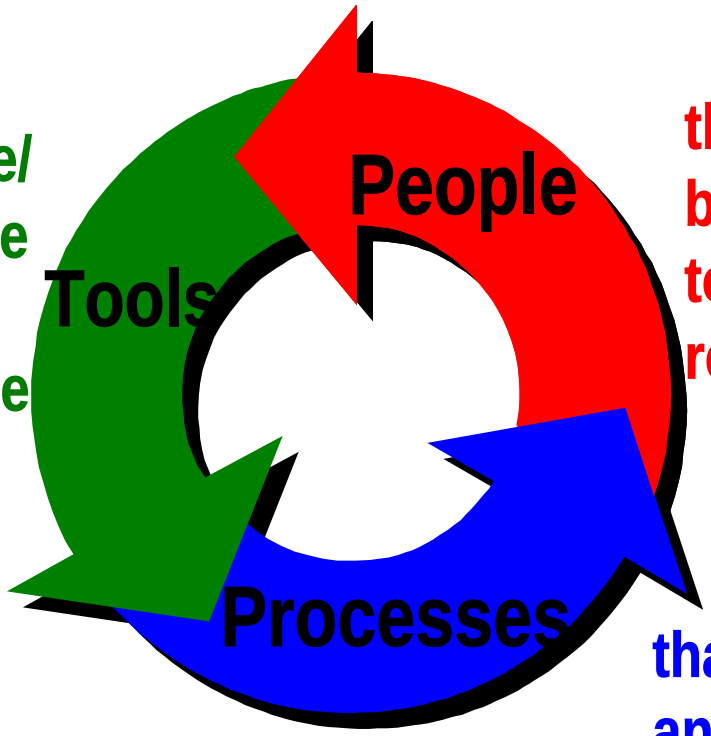
- **Where is it?**
- **What is it?**
- **Who is responsible/accountable?**
- **How is it controlled?**
- **When was it last revised/assessed?**

Security is a component of Technology Risk Management.

Security Components

To be effective, a security program needs to contain:

that enable/ support the people to execute the processes



that have the appropriate background and skill set to effect their responsibilities

that are clearly defined and consistently employed

Recent Articles Related to Security Threats

- **CIA Plans Center to Counter "Cyberwar Threat**

  N.Y. Times, June 26, 1996

- **Feeling Insecure, Are We? Hackers Are Out to Get You, So Paranoia is O.K.**

  N.Y. Times, March 17, 1997

- **Information-Warfare Defense is Urged Pentagon Panel Warns of "Electronic Pearl Harbor"**

  Wall Street Journal, April 23, 1997

- **Hacker Hits Internet Page of Malaysian Telecom**

  Reuter Information Service, February 21, 1997

Excerpts from the Articles

- **Reuters Hong Hong, November 19, 1996**

  A Reuters computer maintenance engineer deleted critical files and “crashed” the system at the Standard Chartered Bank, Jardine Fleming and Natwest, all before his lunch break.

Excerpts from the Articles

- **Business Week, April 21, 1997**

  Russia's Military leaders are shaping a strategy that one day could pose a threat to the West; **focusing its limited resources on R&D for "information warfare."**

  Western analysts say that Russia is anteing up for new generations of smart sensors and precision weapons. And it is working on viruses and other high-tech wreckers that can attack an adversary's civilian computers running everything from the financial system to telephones to utility grids.

Excerpts from the Articles

- **New York Times, March 17, 1996**

  "We're really on the cusp of this becoming a major problem." said **James Kallstrom, head of the FBI** office in New York. "As more and more of the **economy goes digital, there are huge incentives for criminal attacks on American corporations."**

  Today there are an estimated 440 hacker bulletin boards, 1900 Web sites purveying hacking tips and tools, and 30 hacker publications like "Phrack" and "2600: The Hacker Quarterly." These are readily available software programs for hacking tactics like "war dialing", and "sniffing"--all used to exploit security weaknesses in computer systems.

Distribution of Sources of Risk

- Disgruntled Employee or Contract Workers
- Organized Crime
- Cyber Criminal
- Competitors
- Graffiti Artists
- Nation State

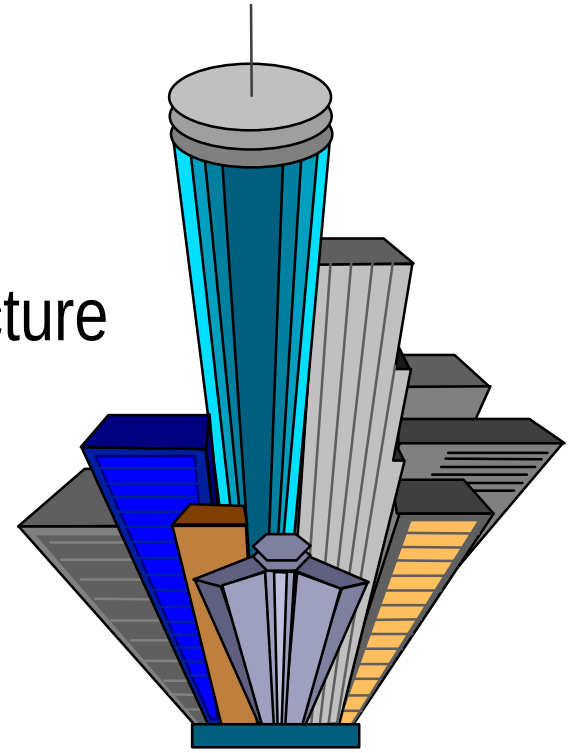
Concerns

- Technology/Automation wave moving faster than control tools and user awareness.
- Legal/law enforcement infrastructure poorly suited for virtual world.

Challenges of Leadership

Large financial institutions have good reason to be a leader in managing its security risks:

- Market visibility
- Financial volume
- Component of national infrastructure
- Global reach
- Vendor dependencies
- Customer data
- Constant change



Network Security

Concerns

- **Security/Confidentiality**
- **Integrity**
- **Operability/Availability**
- **Recoverability**
- **Administrative Issues**
  - Integrity/audit trail of usage
  - Segregation of Duties
- **Software Implementation**
  - Table Maintenance
  - Protocol Management
- **Security**
  - Open vs. Closed

Risks

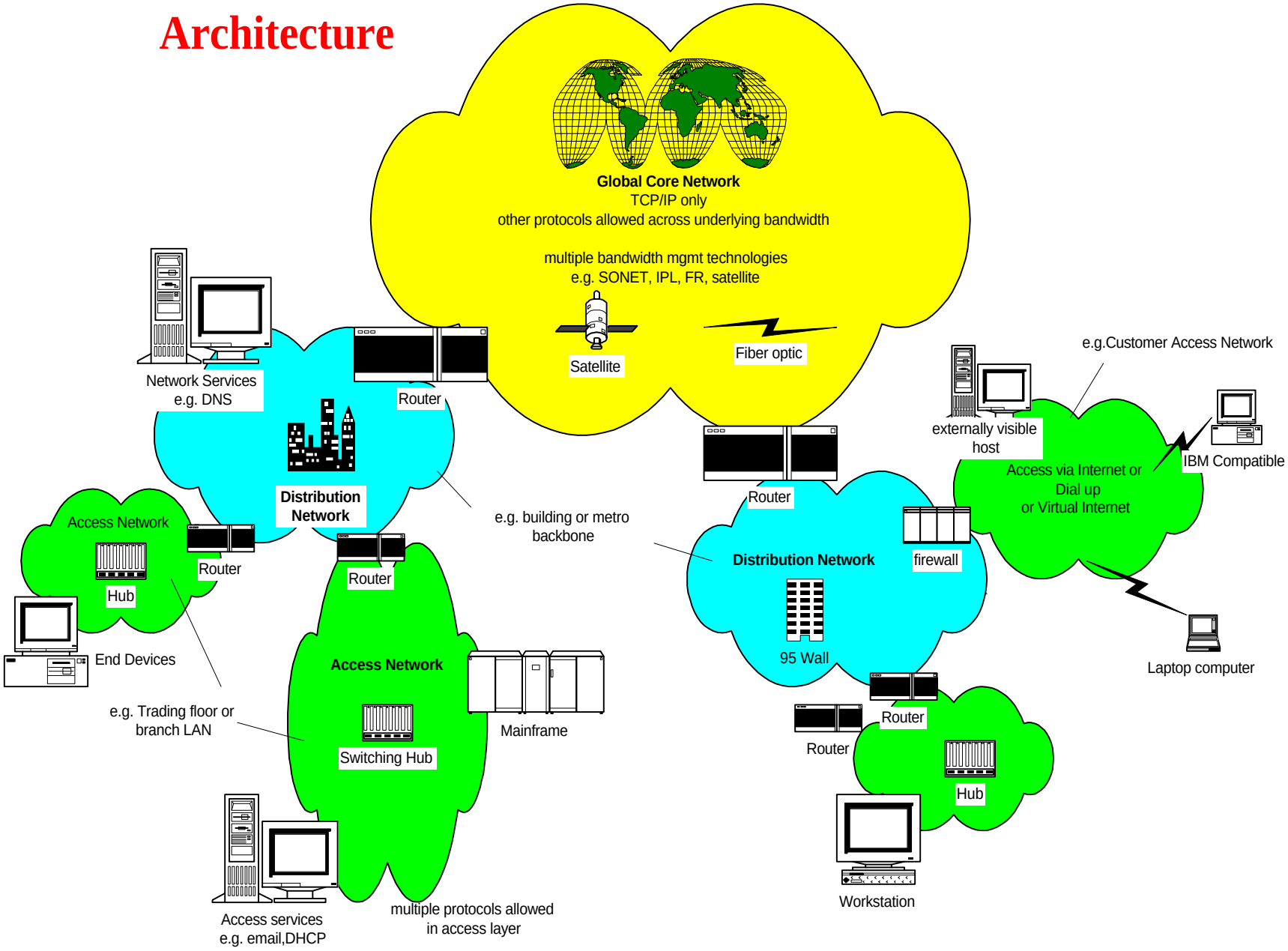
- Interconnectivity of Networks
  - Internal / External
  - Customers (trusted environments)
  - Intra /Extra / Inter Net
  - Outside Service Providers
  - Maintenance of Network Components
    - Routers/Switches/Hubs/Firewalls

Network Security

Architectural Approaches

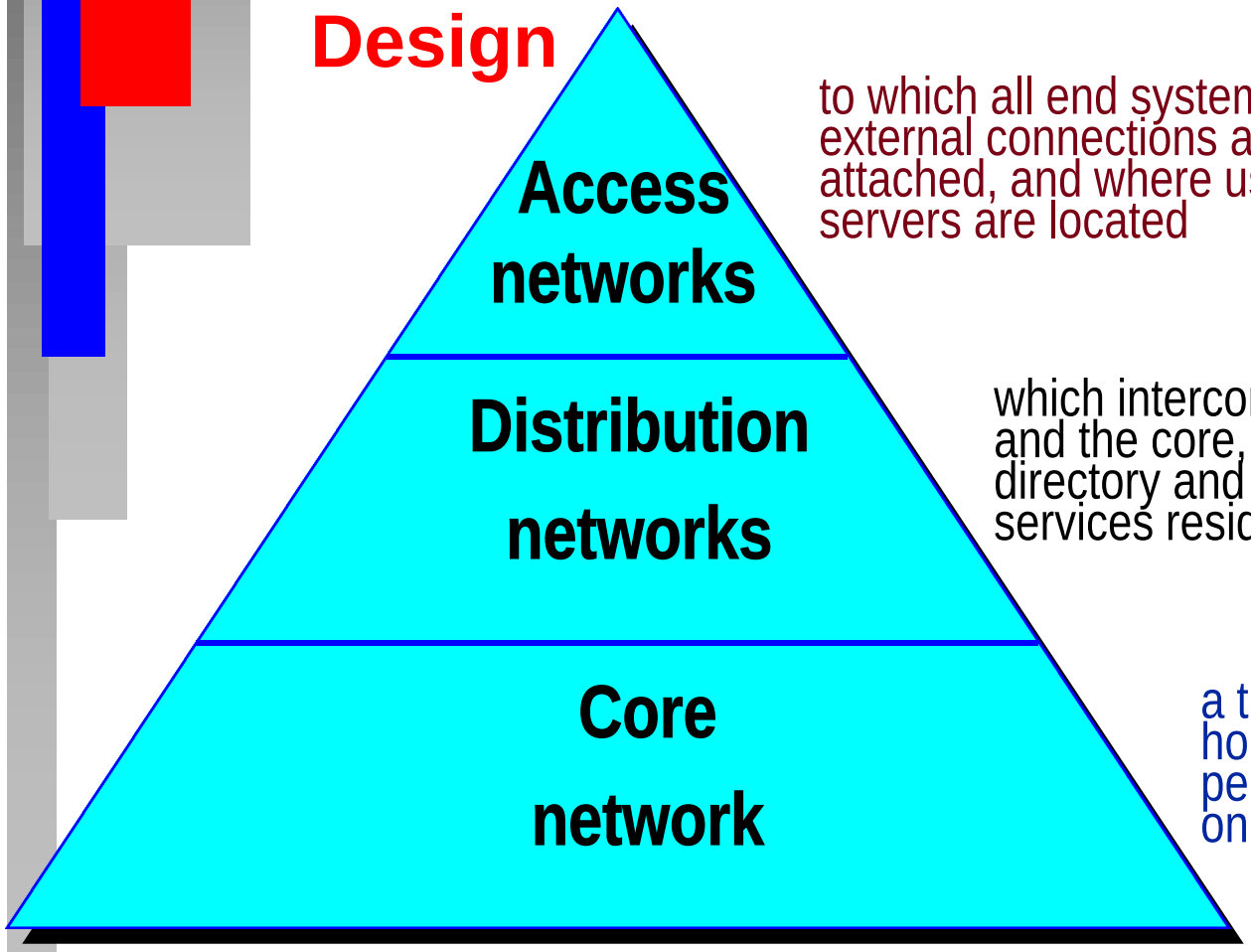
- **Front-End**
  - Prevents access to network
- **Back-End**
  - Burden on each individual host processor
- **Centralized**
  - Common “authentication Server”
- **Centralized Session Control**
  - Divides resources by groups according to security requirements
- **Firewalling**
  - Processor accepts risk
  - User locked in cannot use processor to gain access path to another processor

3 Tier Hierarchical Network Architecture



The Internetwork

Three Tier Hierarchial Design



to which all end systems and external connections are attached, and where user-related servers are located

which interconnect access networks and the core, and where only directory and enterprise-wide services reside

a tightly controlled, global, homogeneous, reliable, high-performance backbone using only IP routing

The Network Security Model

External Network Perimeter

- **Protect the Network from unauthorized external access**
  - All External Connections must pass through a limited number of carefully managed perimeter Firewalls
  - All Dial-up Access must be made through a Secure Gateway
  - All External Access will be controlled by “strong” authentication procedures

The Network Security Model

Internal Network Perimeter

- **Protect sensitive information assets**
  - Three tier hierarchy facilitates internal access control
  - Network Security implementation is based on the risk level of the business application
  - Complementary Network and Application Level Security mechanisms must be employed

The Network Security Model

Ensure Privacy

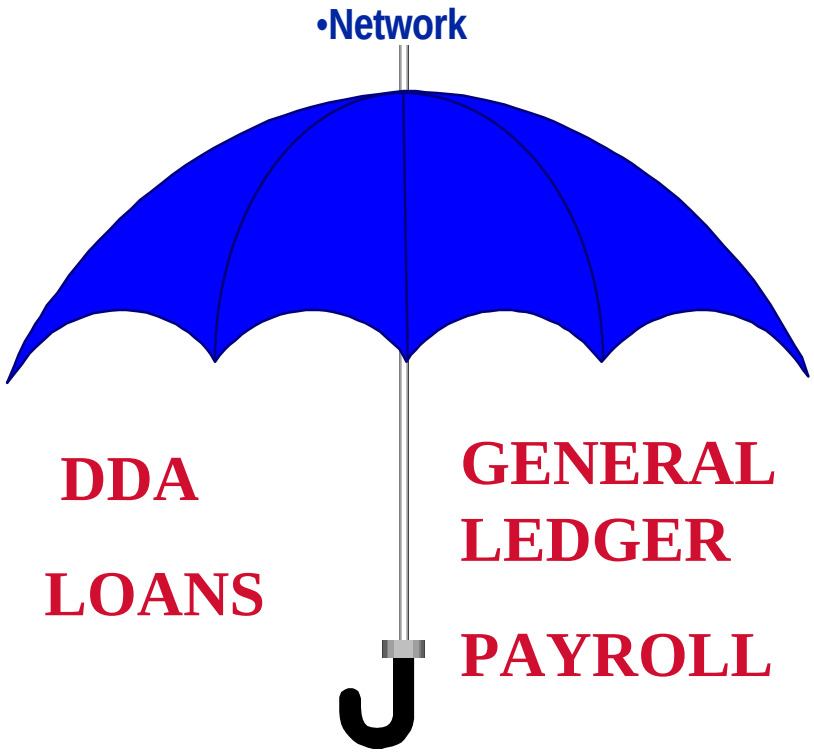
- **Protect sensitive information assets**
  - All Levels of encryption should be supported
    - Link
    - Network
    - Application
    - File Level
- **Risk Assessment to determine need for encryption**

Network Security Goals

- Apply access controls appropriate to the risk exposure
- Provide appropriate level of confidentiality and integrity of data transmission
- Prevent unauthorized activity from interfering with the integrity and availability of the network
- Physical access - To hardware and line connection points
- Implementation and use of logical access controls for network devices
- Controlled implementation of modifications to network software and table maintenance
- Vital Records Management for network devices
- Disaster Recovery Program for network services

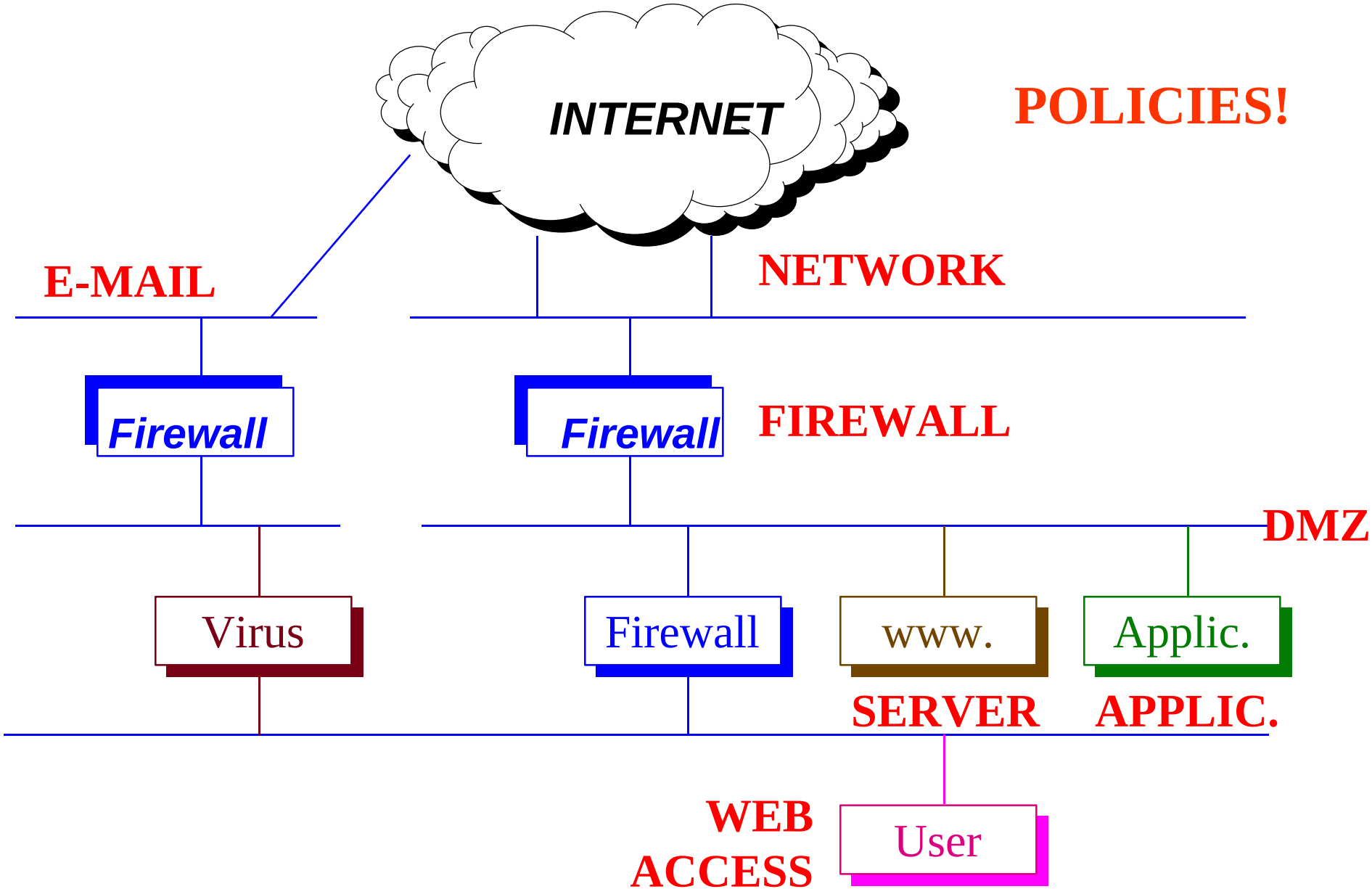
Control Feature

INTEGRITY CONTROLS



APPLICATION CONTROLS

- User
- Program


INTERNET
POLICIES!
E-MAIL
NETWORK
Firewall
Firewall
FIREWALL
DMZ
Virus
Firewall
www.
Applic.
SERVER
APPLIC.
WEB
ACCESS
User

The Risks

- **The Enterprise is exposed to the "World".**
- **Some old challenges**
  - Operating System Security
  - Network Security
  - Data Integrity
  - Social Engineering
  - Viruses

The Risks (Cont'd)

- **Some new challenges**
  - Denial of Service Attacks
  - TCP/IP Spoofing
  - Session Hijacking
  - Confidentiality
  - Operational Risk

Meeting the Challenge

- Perform a network security review.
- Carefully select and implement a firewall system.
- MONITOR! MONITOR! MONITOR!
- Form a tiger team to test your defenses.
- Be prepared for the WORST!

Going Forward

- Focus on end-to-end security.
- Connecting existing applications to the Net is not a simple change.
- Partner with the business units during the development process.
- Risk management is a value added service.

The Future

- Technology is getting better
  - Firewalls
  - Encryption and key management
  - Authentication and non-repudiation
  - Monitoring

Conclusion

- Active Risk Management Program
- Dedicated Resources
- Defined Metrics
- Management Commitment
- Risks are growing