How to Implement a Secure Campus

EDUCATION SERVICE CENTER, REGION 20

Serving the Educational Community

Agenda

Five Strategic Objectives for Comprehensive Security

Strategy – Doing the right things

- Risk Management
- Infrastructure
- People and Processes
- Effective Security Mechanisms
- Awareness

Three Tactical Objectives to Meet Strategic Goals

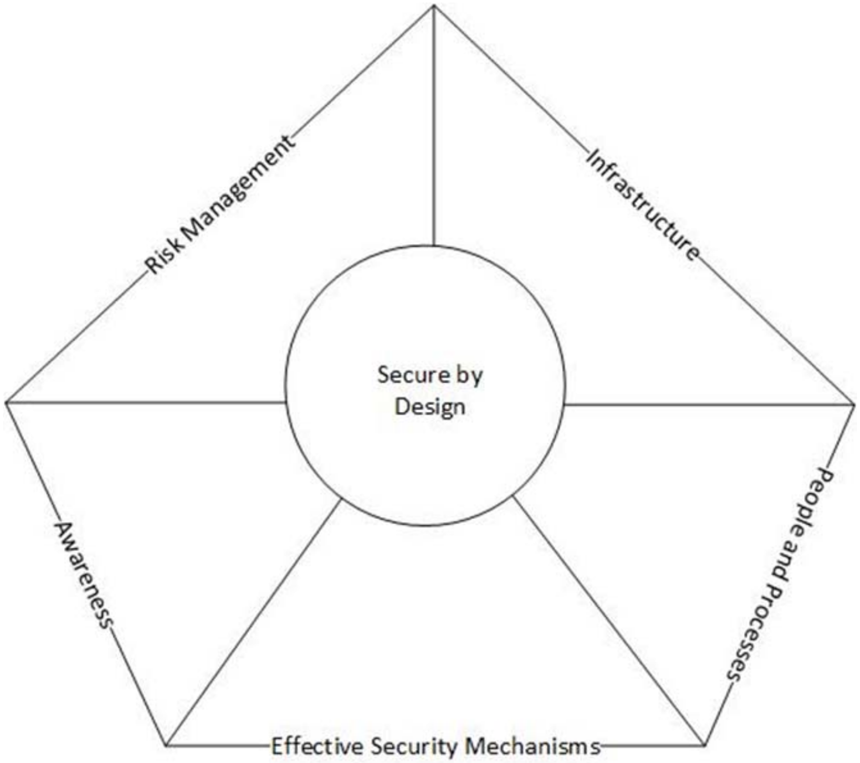
Tactical – Doing things right

- Technical
- Administrative
- Physical

Secure by Design

Comprehensive Security is the sum of its parts.
The objective is to be secure by design.

Secure by Design



360 degree field of view

Identify – Protect – Detect – Respond – Recover

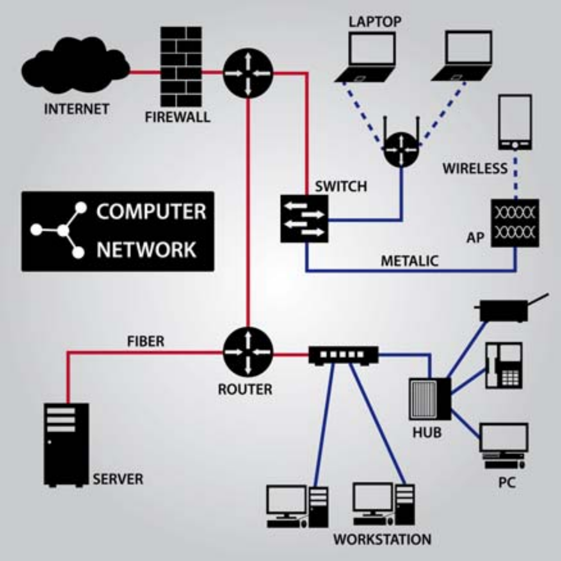
What is at Risk

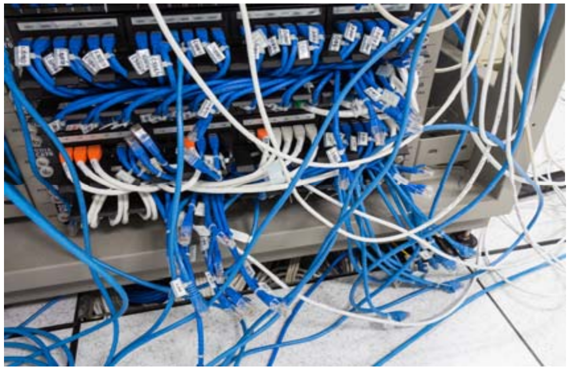
Security objective #1: Enterprise Risk Management

- What needs protecting and how much protection is needed?
- Cost benefit/Total Cost of Ownership
- Protect the brand
- Protect customers/students/staff
- Avoid legal and financial problems

Devil in the Details

Security objective #2: Infrastructure





- Physical and logical design.
- The simpler the better. Complexity adds risk.
- Simple but allows for efficient application of security controls, management, and the effective application of security tools.
- What needs protecting and how much protection is needed?
- Detailed diagrams and maps.
- Environmental and Physical controls
- Cable Plant

Culture

Security objective #3: People and Processes that Oversee the Network.

- Develop cybersecurity culture
- Train techs, admins, and users to recognize threats
- Response plans
- Continuity of operations
- Change Management
- Backup/restoration/failover/patching/updates

Be Proactive

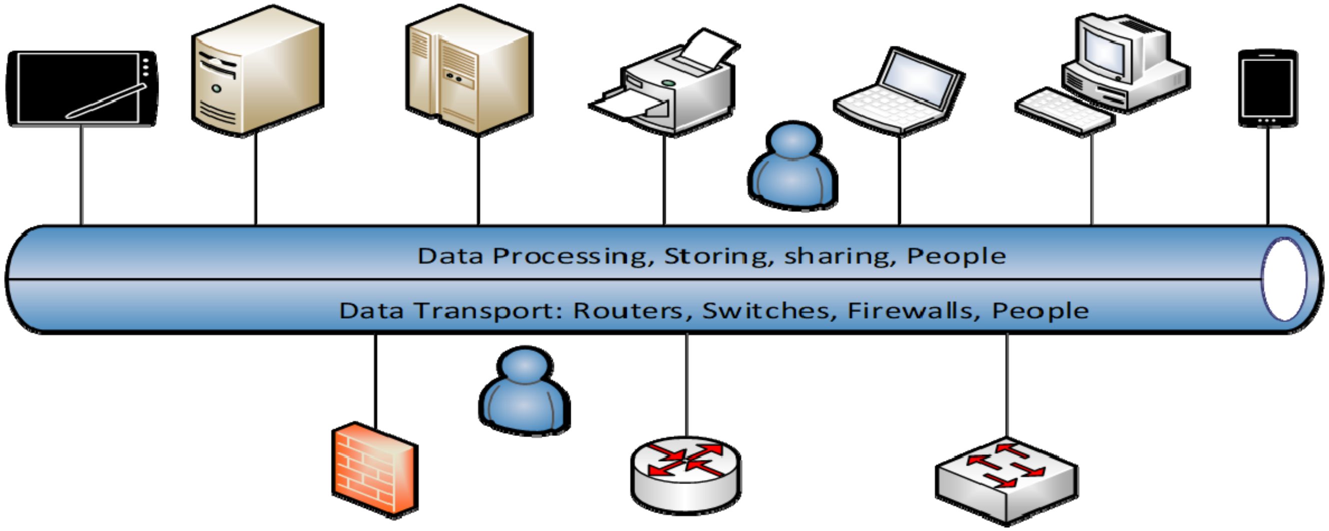
Security Objective #4: Effective Use of Network Security Mechanisms

- Are security tools being fully utilized?
- No point in scanning if actions aren't being taken.
- What data points can be used as indicators (trend analysis/baselining)
- Protect outside in and inside out.

Situational Awareness

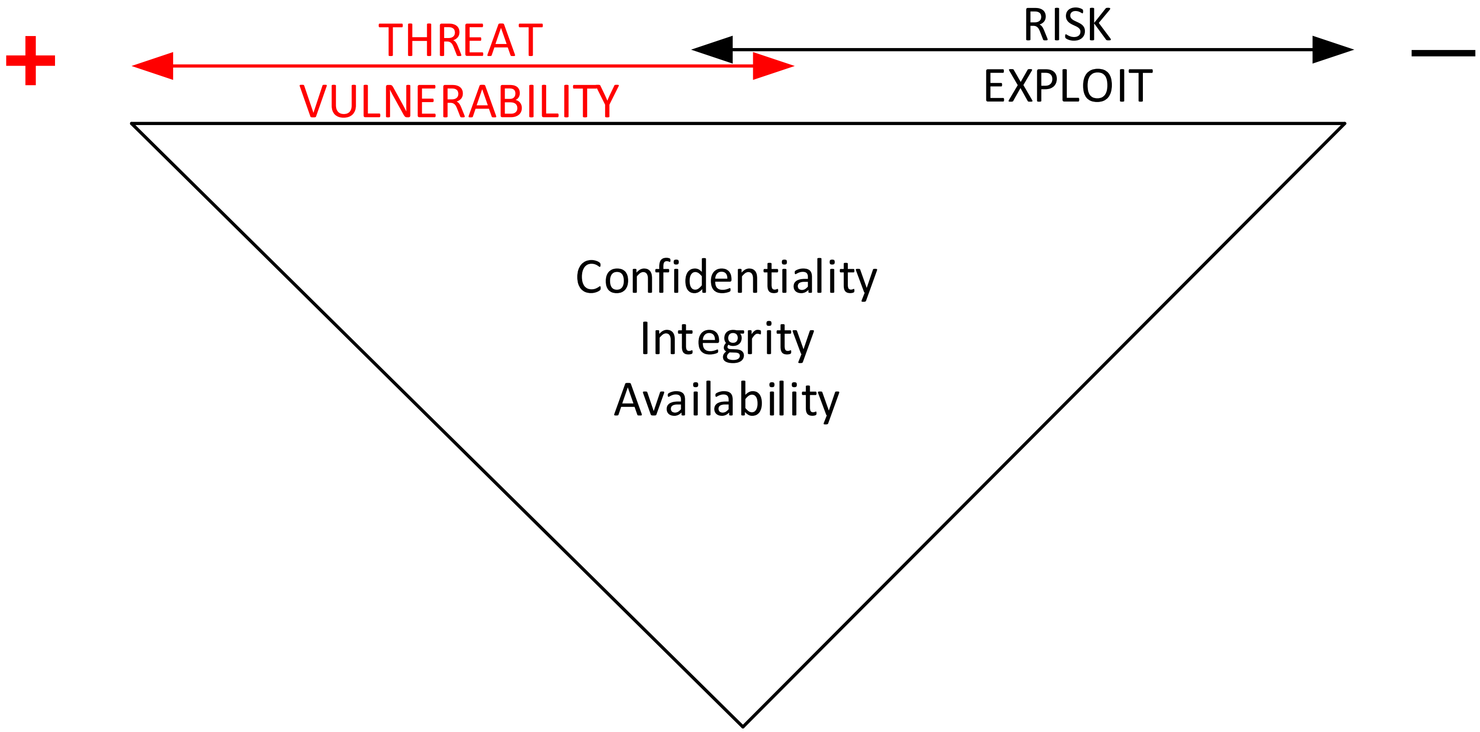
Security Objective #5: Awareness

- As part of the "system" general user awareness is an important component of information security.
- Be aware of threat vectors.
- Be aware of potential vulnerabilities.
- Social engineering education.


Data Processing, Storing, sharing, People
Data Transport: Routers, Switches, Firewalls, People

Achieve Balance

Balance



How Do I Implement A Secure Campus

Achieve strategic objectives through relevant tactics.

- Technical
- Administrative
- Physical

Technical

You can have a well designed network and poor security but you cannot have a poorly designed network and good security.

Design

- Poor design equals poor security
- Marginalizes the effectiveness of security investments

Routers/Switches

- IOS Security
- Access Security
- Network Services
- ACLs, Filtering, and Rate Limiting
- Routing Protocols
- Audit and Management

Technical

"Prevention is ideal, but detection is a must. However, detection without response has little value"

Servers

- Operating Systems
- Patches
- Disk Space
- Services
- Accounts
- Logging
- Software/Hardware Inventory
- Backups

PCs

- Operating Systems
- Patches
- Anti-Virus Protection

Management

- Active Directory Structure
- Group Policy
- Passwords

Administrative

Administrative controls are the policies, procedures, guidelines, and mechanisms in place to enforce and control the human side of things.

- Develop enforceable policies
- Document Processes and procedures
- Document network and system changes
- Separation of duties
- Applicant Screening, Employee Controls, Termination procedures
- User awareness training
- Security training for admins

Physical

Collect as much information as you can so that you can establish event correlation.

- Guards, gates
- Locked doors
- Controlled access to equipment rooms
- Surveillance
- Fences
- HVAC

In closing

If I was a bad guy, what would I want and how would I get it?

Common sense is relative, develop security sense.

Plan to be impacted by an incident.

Can you spot the hacker?