The Security Matrix

	People	Physical	Networks	Computer Equipment
Prevention				
Detection				
Reaction				

The Security Matrix: uses

- Use the matrix to focus measures where they are needed, and to be aware of what measures are being (purposely) neglected.
- Drawing a threat/risk landscape. What areas are most at risk? Acceptable downtime.
- Define future measures, baselines, or project specific security
- Relating security topics.
- Dept & diversity of defence
- List/audit current measures
- Follow changes in focus over time
- Divide “Computer Equipment” according to your needs, e.g. : OS, DBs, Middleware, Applications

Examples

	People	Physical	Networks	Computer Equipment
	Users, managers, admins	Buildings, server rooms, laptops, diskettes, backups..	Telephone, fax, voicemail, IP tel., Internet , Intranet, VPN, SNA, Novel,I Dialup	Servers, workstations, laptops, routers, hubs, switches,

General measures

Prevention	Physical, technical, continual re-assessment, resource isolation, ...
Detection	Audits, looking for unusual behaviour
Reaction	Panic? .. disciplinary action, forensics/detective work

Measures

	People	Physical	Networks	Computers (OS + Applications)
Prevention	Policy, processes, responsibility, roles, education, goodwill.. Documentation: architecture/ services/ changelog. Good Programming. Continual re-assessment. Release mgt	Locks (several layers), logging.. cameras, security guards,	Network firewall, switches not hubs anti-spoofing content filtering strong authentication resource isolation encryption	Hardening local/personal firewall log analysis anti-virus & updates redundancy & backups resource isolation encryption
Detection	audits	Cameras, alarms Security guards	NIDS, logs, traffic changes Scanning	Log analysis integrity checker local/personal IDS
Reaction	Discipline Incident Response Team		Firewall rules Unplug networks	Unplug from network, shutdown, Reinstall, fix, ignore, Forensics

Security Mechanisms

Organisational aspects

- Process security
- Clear policies, known, enforced.
- Security process: manage risk.
- Only expose necessary systems.
- Education of the users and admins.
- Clear roles & responsibilities

Physical security

Legal threat

Audit & review

Technical countermeasures

- System hardening (services, config, patches, accounts)
- Access control: local & network (packet screening, switched networks)
- content filtering (HTTP/Email/ftp)
- Encryption
- Resource isolation
- Strong authentication (VPN, RAS & FW)
- Good password management or tokens
- Intrusion detection networks/hosts (passive)
- Scanning networks/hosts (active)
- Traffic/statistics monitoring
- Correctly program/review/test code
- Backup/Restore procedures/processes

Trade-offs

- Complexity
- time / skills
- rate of change
- Performance
- ease of use
- cost