Control categories

Control categories

Controls within cybersecurity are grouped into three main categories:

- Administrative/Managerial controls
- Technical controls
- Physical/Operational controls

Administrative/Managerial controls address the human component of cybersecurity. These controls include policies and procedures that define how an organization manages data and clearly defines employee responsibilities, including their role in protecting the organization. While administrative controls are typically policy based, the enforcement of those policies may require the use of technical or physical controls.

Technical controls consist of solutions such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus (AV) products, encryption, etc. Technical controls can be used in a number of ways to meet organizational goals and objectives.

Physical/Operational controls include door locks, cabinet locks, surveillance cameras, badge readers, etc. They are used to limit physical access to physical assets by unauthorized personnel.

Control types

Control types include, but are not limited to:

1. Preventative
2. Corrective
3. Detective
4. Deterrent

These controls work together to provide defense in depth and protect assets. **Preventative controls** are designed to prevent an incident from occurring in the first place. **Corrective controls** are used to restore an asset after an incident. **Detective controls** are implemented to determine whether an incident has occurred or is in progress. **Deterrent controls** are designed to discourage attacks.

Review the following charts for specific details about each type of control and its purpose.

Administrative/Managerial Controls		
Control Name	**Control Type**	**Control Purpose**
Least Privilege	Preventative (should be Preventative/Deterrent)	Reduce risk and overall impact of malicious insider or compromised accounts
Disaster recovery plans	Corrective	Provide business continuity (with additional: Restore business behavior after the disaster)
Password policies	Preventative (should be Preventative/Deterrent)	Reduce likelihood of account compromise through brute force or dictionary attack techniques
Access control policies	Preventative	Bolster confidentiality and integrity by defining which groups can access or modify data
Account management policies	Preventative	Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage
Separation of duties	Preventative	Reduce risk and overall

Administrative/Managerial Controls		
		impact of malicious insider or compromised accounts

Technical Controls		
Control Name	**Control Type**	**Control Purpose**
Firewall	Preventative	To filter unwanted or malicious traffic from entering the network
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule
Encryption	Deterrent	Provide confidentiality to sensitive information
Backups	Corrective	Restore/recover from an event
Password management	Preventative	Reduce password fatigue
Antivirus (AV) software	Preventative (should be Preventative/Detective)	Scans to detect and quarantine known threats
Manual monitoring, maintenance, and intervention	Preventative (should be Preventative/Detective)	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems

Physical/Operational Controls		
Control Name	**Control Type**	**Control Purpose**

Time-controlled safe	Deterrent (should be Preventative)	Reduce attack surface and overall impact from physical threats
Adequate lighting	Deterrent	Deter threats by limiting “hiding” places
Closed-circuit television (CCTV)	Preventative/Detective	Closed circuit television is both a preventative and detective control because its presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions
Locking cabinets (for network gear)	Preventative	Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear
Signage indicating alarm service provider	Deterrent	Deter certain types of threats by making the likelihood of a successful attack seem low
Locks	Deterrent/Preventative	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative	Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc.