Rebecca Dias
BEA (19)
182027

MIS IAT-1

Q3]

Physical controls

(1) Physical controls prevent unauthorized individuals from gaining access to a company's facilities
(2) common physical control include walls, doors, fencing, gates, locks, badges, guards and alarm systems
(3) more sophisticated physical controls include pressure sensors and temperature sensors
(4) organisations also implement physical security measures that limit computer users to acceptable login times and locations

eg:- Home automation system with motion sensors

Access controls

(1) Access controls restrict unauthorized individuals from using information resources
(2) The controls involve two major functions
   - authentication
   - authorization
(3) Authentication confirms the identity of the person requiring access. After the person is identified, the next step is authorization
(4) Authorization determines which actions, rights or privileges the person has based his/her verified identity

eg:- authority checks to enter a particular office building/ house Id code checking.

Rebecca Dias
BE A (19)

Communication Controls

(1) Also called as network controls
(2) Firewalls, anti-malware system, black listing, encryption virtual private networks (VPNs) secure socket layer (SSL)
(3) eg:- firewall is a system that prevents a specific type of information from moving between untrusted networks such as Internet
(4) Anti-malware systems also called antivirus or AV software are software packages that attempt to identify and eliminate viruses and worms
(5) A third party called a certificate authority acts as a trusted + intermediary between the companies
(6) VPN's is a private network that uses a public network to connect users
(7) eg:- employee monitoring systems, monitors their employees computers email activities and internet surfing activities.