Protecting Information Assets

- Unit#2c -

Physical and Environmental Security

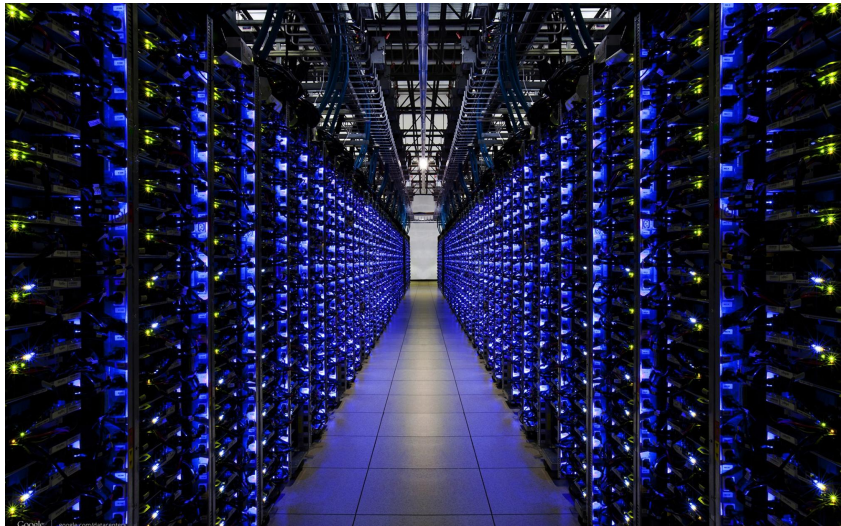
Agenda

- Physical and Environmental Security
- Physical Security
- Environmental Security
- Test Taking Tip
- Quiz

Physical and Environmental (PE) Security

…encompasses protection of physical assets from damage, misuse, or theft

- **Physical security addresses**
  - **…mechanisms used to create secure areas around hardware**
- **Environmental security addresses**
  - **…safety of assets from damage from environmental concerns**



Physical and Environmental (PE) Security

Focuses on controlling the **impact of hazardous energies and materials** on Information Systems

- Addresses physical protection of the organization's resources, including:
  1. *People*
  2. *IT Equipment and facilities*
  3. *Information systems*
  4. *Data*
- *Concerns:*
  - *People safety*
  - *Environmental issues can affect equipment and systems*
  - *People (as threats) can affect physically enter an environment*

Saving human lives is the first priority in any life-threatening situation

People safety always takes precedence over the other security factors

Physical and Environmental sources of threats…

Human *– vandalism, sabotage, theft, terrorism, war*

- *…*

Materials

- ***Water*** *– floods, leaks*
- ***Chemicals and particulates -*** *smoke, toxic materials, industrial pollution*
- ***Organism*** *- virus, bacteria, animal, insect*
- *…*

Energy

- ***Wind***
- ***Fire***
- ***Explosion***
- ***Electricity***, ***magnetism, radio wave*** *anomalies*

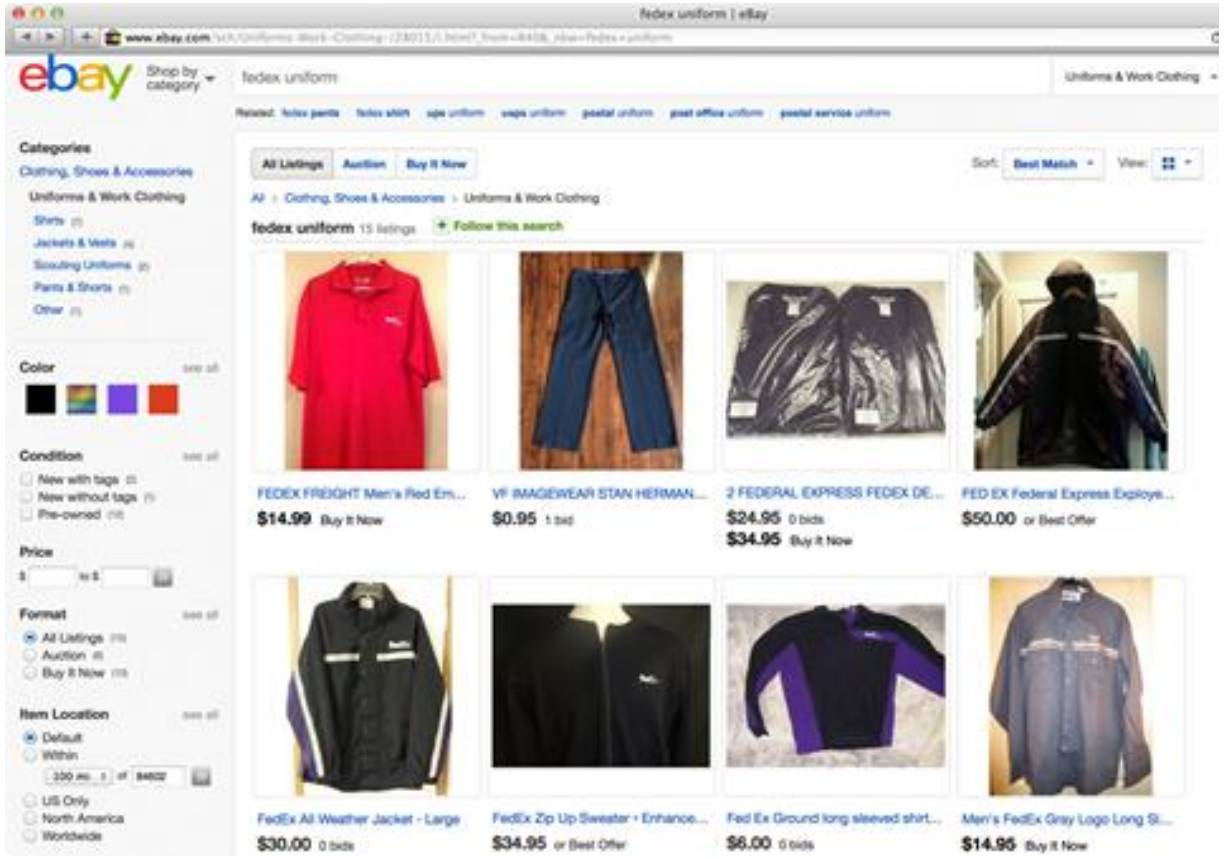

HOW ARE YOU

“Tailgating”, “Piggybacking” and Social Engineering

Social engineering

Are receptionists good at preventative security?

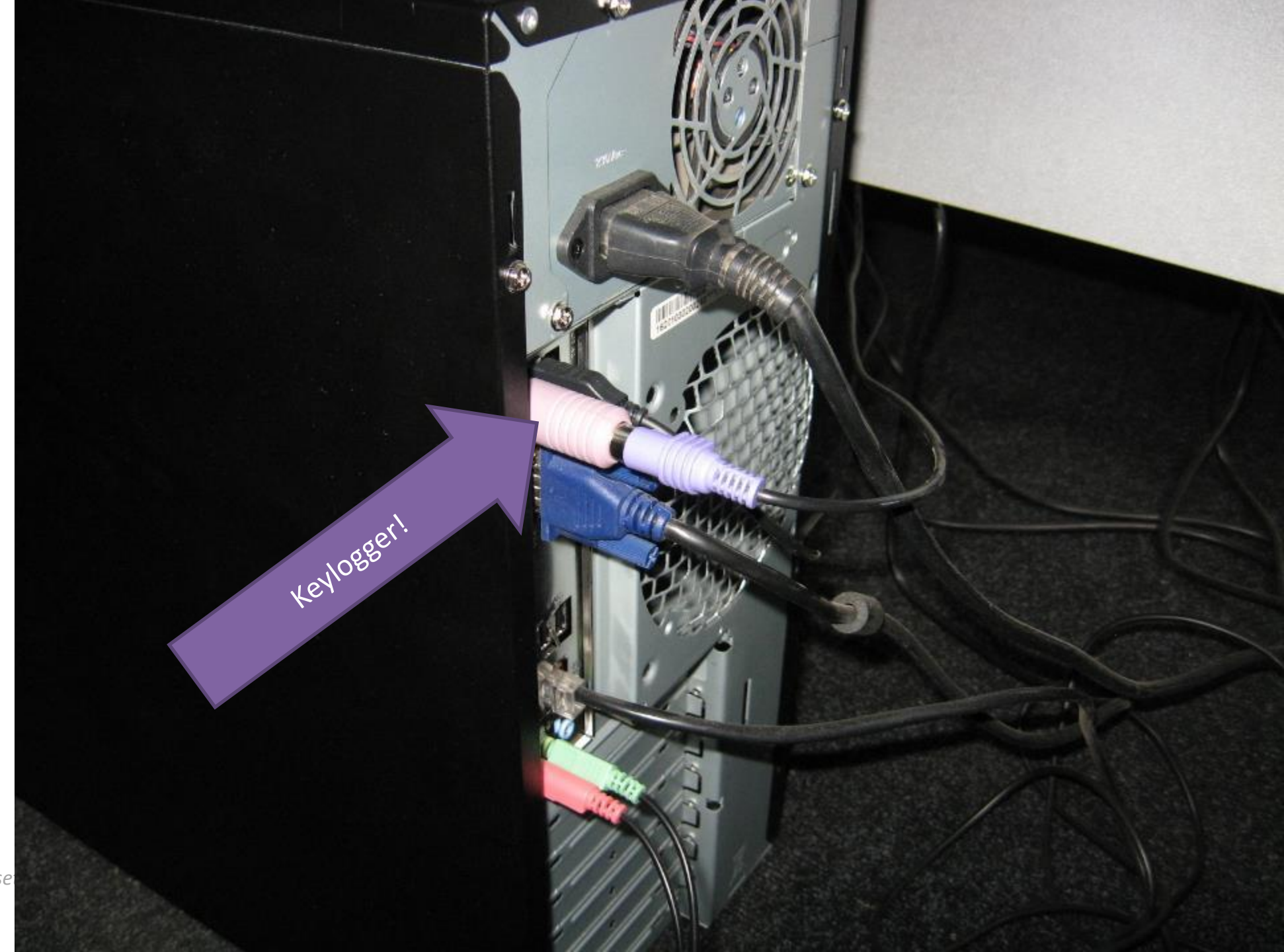
- **No,** their job is to help people feel welcome and guide them through the organization in an efficient way
- But intruders can get past guards with social engineering…




What could a hacker do, once in a server room?
Physical access to an unlocked, running system usually means “game over!”
Google
google.com/datacenters


TrueCrypt Boot Loader 7.1
Keyboard Controls:
[Esc] Skip Authentication (Boot Manager)
Enter password: _

What's wrong in this photo?



Keyloggers violate federal wiretapping laws

Keystroke injector

MENU HAK5 0

USB RUBBER DUCKY

$49.99

Imagine you could walk up to a computer, plug in a seemingly innocent USB drive, and have it install a backdoor, exfiltrate documents, steal passwords or any number of pentest tasks.

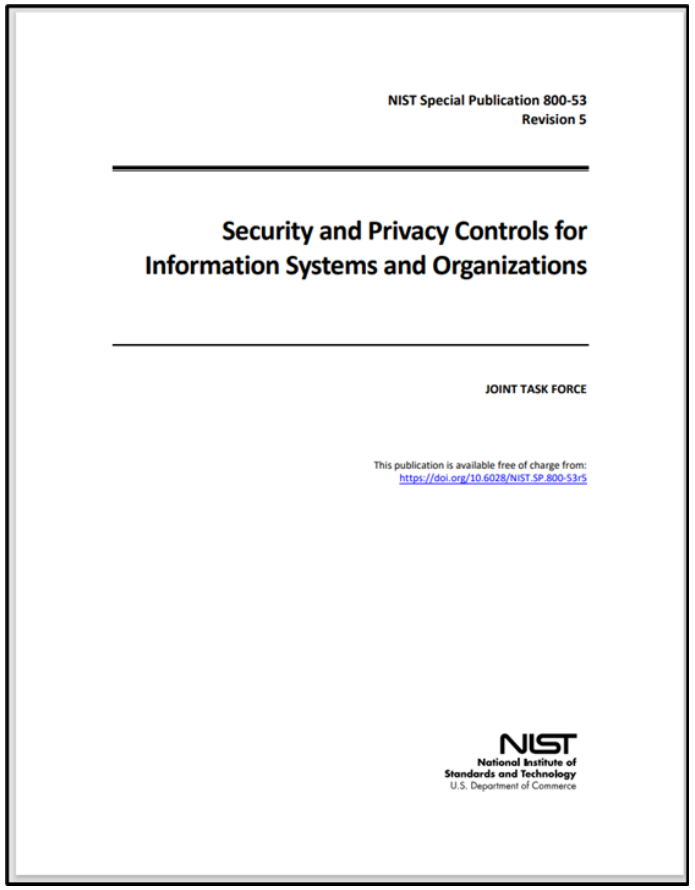
All of these things can be done with many well crafted keystrokes. If you could just sit in front of this computer, with photographic memory and perfect typing accuracy, you could do all of these things in just a few minutes.

The USB Rubber Ducky does this in seconds. It violates the inherent trust computers have in humans by posing as a keyboard - and injecting keystrokes at superhuman speeds.

Since 2010 the USB Rubber Ducky has been a favorite among

“Dumpster diving”

Physical and Environmental control baselines


NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

TABLE 3-11: PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PE-1	Policy and Procedures		x	x	x
PE-2	Physical Access Authorizations		x	x	x
PE-2(1)	ACCESS BY POSITION AND ROLE				
PE-2(2)	TWO FORMS OF IDENTIFICATION				
PE-2(3)	RESTRICT UNESCORTED ACCESS				
PE-3	Physical Access Control		x	x	x
PE-3(1)	SYSTEM ACCESS				x
PE-3(2)	FACILITY AND SYSTEMS				
PE-3(3)	CONTINUOUS GUARDS				
PE-3(4)	LOCKABLE CASINGS				
PE-3(5)	TAMPER PROTECTION				
PE-3(6)	FACILITY PENETRATION TESTING	W: Incorporated into CA-8.			
PE-3(7)	PHYSICAL BARRIERS				
PE-3(8)	ACCESS CONTROL VESTIBULES				
PE-4	Access Control for Transmission			x	x
PE-5	Access Control for Output Devices			x	x
PE-5(1)	ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS	W: Incorporated into PE-5.			
PE-5(2)	LINK TO INDIVIDUAL IDENTITY				
PE-5(3)	MARKING OUTPUT DEVICES	W: Incorporated into PE-22.			
PE-6	Monitoring Physical Access		x	x	x
PE-6(1)	INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT			x	x
PE-6(2)	AUTOMATED INTRUSION RECOGNITION AND RESPONSES				
PE-6(3)	VIDEO SURVEILLANCE				
PE-6(4)	MONITORING PHYSICAL ACCESS TO SYSTEMS				x
PE-7	Visitor Control	W: Incorporated into PE-2 and PE-3.			
PE-8	Visitor Access Records		x	x	x
PE-8(1)	AUTOMATED RECORDS MAINTENANCE AND REVIEW				x
PE-8(2)	PHYSICAL ACCESS RECORDS	W: Incorporated into PE-2.			
PE-8(3)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	x			
PE-9	Power Equipment and Cabling			x	x
PE-9(1)	REDUNDANT CABLING				
PE-9(2)	AUTOMATIC VOLTAGE CONTROLS				
PE-10	Emergency Shutoff			x	x
PE-10(1)	ACCIDENTAL AND UNAUTHORIZED ACTIVATION	W: Incorporated into PE-10.			
PE-11	Emergency Power			x	x
PE-11(1)	ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY				x
PE-11(2)	ALTERNATE POWER SUPPLY — SELF-CONTAINED				
PE-12	Emergency Lighting		x	x	x
PE-12(1)	ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS				
PE-13	Fire Protection		x	x	x
PE-13(1)	DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION			x	x
PE-13(2)	SUPPRESSION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION				x
PE-13(3)	AUTOMATIC FIRE SUPPRESSION	W: Incorporated into PE-13(2).			
PE-13(4)	INSPECTIONS				
PE-14	Environmental Controls		x	x	x
PE-14(1)	AUTOMATIC CONTROLS				
PE-14(2)	MONITORING WITH ALARMS AND NOTIFICATIONS				
PE-15	Water Damage Protection		x	x	x
PE-15(1)	AUTOMATION SUPPORT				x
PE-16	Delivery and Removal		x	x	x
PE-17	Alternate Work Site			x	x
PE-18	Location of System Components				x
PE-18(1)	FACILITY SITE	W: Moved to PE-23.			
PE-19	Information Leakage				
PE-19(1)	NATIONAL EMISSIONS POLICIES AND PROCEDURES				
PE-20	Asset Monitoring and Tracking				
PE-21	Electromagnetic Pulse Protection				
PE-22	Component Marking				
PE-23	Facility Location				

PE-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-01_ODP[01]	***personnel or roles to whom the physical and environmental protection policy is to be disseminated is/are defined;***
	PE-01_ODP[02]	***personnel or roles to whom the physical and environmental protection procedures are to be disseminated is/are defined;***
	PE-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	PE-01_ODP[04]	***an official to manage the physical and environmental protection policy and procedures is defined;***
	PE-01_ODP[05]	***the frequency at which the current physical and environmental protection policy is reviewed and updated is defined;***
	PE-01_ODP[06]	***events that would require the current physical and environmental protection policy to be reviewed and updated are defined;***
	PE-01_ODP[07]	***the frequency at which the current physical and environmental protection procedures are reviewed and updated is defined;***
	PE-01_ODP[08]	***events that would require the physical and environmental protection procedures to be reviewed and updated are defined;***
	PE-01a.[01]	a physical and environmental protection policy is developed and documented;
	PE-01a.[02]	the physical and environmental protection policy is disseminated to ***<PE-01_ODP[01] personnel or roles>***;
	PE-01a.[03]	physical and environmental protection procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls are developed and documented;
	PE-01a.[04]	the physical and environmental protection procedures are disseminated to ***<PE-01_ODP[02] personnel or roles>***;
	PE-01a.01(a)[01]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses purpose;
	PE-01a.01(a)[02]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses scope;
	PE-01a.01(a)[03]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses roles;
	PE-01a.01(a)[04]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses responsibilities;
	PE-01a.01(a)[05]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses management commitment;
	PE-01a.01(a)[06]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses coordination among organizational entities;

Example of guidance for auditing a PE control

PE-01	POLICY AND PROCEDURES	
	PE-01a.01(a)[07]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses compliance;
	PE-01a.01(b)	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	PE-01b.	the ***<PE-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures;
	PE-01c.01[01]	the current physical and environmental protection policy is reviewed and updated ***<PE-01_ODP[05] frequency>***;
	PE-01c.01[02]	the current physical and environmental protection policy is reviewed and updated following ***<PE-01_ODP[06] events>***;
	PE-01c.02[01]	the current physical and environmental protection procedures are reviewed and updated ***<PE-01_ODP[07] frequency>***;
	PE-01c.02[02]	the current physical and environmental protection procedures are reviewed and updated following ***<PE-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-01-Examine	[SELECT FROM: Physical and environmental protection policy and procedures; system security plan; privacy plan; organizational risk management strategy; other relevant documents or records].
	PE-01-Interview	[SELECT FROM: Organizational personnel with physical and environmental protection responsibilities; organizational personnel with information security and privacy responsibilities].

How would you audit the existence and strength of the PE-3 Control ?

PE-03	PHYSICAL ACCESS CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-03_ODP[01] PE-03_ODP[02]	***entry and exit points to the facility in which the system resides are defined;*** ***one or more of the following PARAMETER VALUES is/are selected: {<PE-03_ODP[03] systems or devices>; guards};***
	PE-03_ODP[03]	***physical access control systems or devices used to control ingress and egress to the facility are defined (if selected);***
	PE-03_ODP[04]	***entry or exit points for which physical access logs are maintained are defined;***
	PE-03_ODP[05]	***physical access controls to control access to areas within the facility designated as publicly accessible are defined;***
	PE-03_ODP[06]	***circumstances requiring visitor escorts and control of visitor activity are defined;***
	PE-03_ODP[07]	***physical access devices to be inventoried are defined;***
	PE-03_ODP[08]	***frequency at which to inventory physical access devices is defined;***
	PE-03_ODP[09]	***frequency at which to change combinations is defined;***
	PE-03_ODP[10]	***frequency at which to change keys is defined;***
	PE-03a.01	physical access authorizations are enforced at ***<PE-03_ODP[01] entry and exit points>*** by verifying individual access authorizations before granting access to the facility;
	PE-03a.02	physical access authorizations are enforced at ***<PE-03_ODP[01] entry and exit points>*** by controlling ingress and egress to the facility using ***<PE-03_ODP[02] SELECTED PARAMETER VALUE(S)>***;
	PE-03b.	physical access audit logs are maintained for ***<PE-03_ODP[04] entry or exit points>***;
	PE-03c.	access to areas within the facility designated as publicly accessible are maintained by implementing ***<PE-03_ODP[05] physical access controls>***;
	PE-03d.[01]	visitors are escorted;
	PE-03d.[02]	visitor activity is controlled ***<PE-03_ODP[06] circumstances>***;
	PE-03e.[01]	keys are secured;
	PE-03e.[02]	combinations are secured;
	PE-03e.[03]	other physical access devices are secured;
	PE-03f.	***<PE-03_ODP[07] physical access devices>*** are inventoried ***<PE-03_ODP[08] frequency>***;
	PE-03g.[01]	combinations are changed ***<PE-03_ODP[09] frequency>*** , when combinations are compromised, or when individuals possessing the combinations are transferred or terminated;
	PE-03g.[02]	keys are changed ***<PE-03_ODP[10] frequency>*** , when keys are lost, or when individuals possessing the keys are transferred or terminated.

TABLE 3-11: PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PE-1	Policy and Procedures		X	X	X
PE-2	Physical Access Authorizations		X	X	X
PE-2(1)	ACCESS BY POSITION AND ROLE				
PE-2(2)	TWO FORMS OF IDENTIFICATION				
PE-2(3)	RESTRICT UNESCORTED ACCESS				
PE-3	Physical Access Control		X	X	X
PE-3(1)	SYSTEM ACCESS				X
PE-3(2)	FACILITY AND SYSTEMS				
PE-3(3)	CONTINUOUS GUARDS				
PE-3(4)	LOCKABLE CASINGS				
PE-3(5)	TAMPER PROTECTION				
PE-3(6)	FACILITY PENETRATION TESTING	W: Incorporated into CA-8.			
PE-3(7)	PHYSICAL BARRIERS				
PE-3(8)	ACCESS CONTROL VESTIBULES				
PE-4	Access Control for Transmission			X	X
PE-5	Access Control for Output Devices			X	X
PE-5(1)	ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS	W: Incorporated into PE-5.			
PE-5(2)	LINK TO INDIVIDUAL IDENTITY				
PE-5(3)	MARKING OUTPUT DEVICES	W: Incorporated into PE-22.			
PE-6	Monitoring Physical Access		X	X	X
PE-6(1)	INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT			X	X
PE-6(2)	AUTOMATED INTRUSION RECOGNITION AND RESPONSES				
PE-6(3)	VIDEO SURVEILLANCE				
PE-6(4)	MONITORING PHYSICAL ACCESS TO SYSTEMS				X
PE-7	Visitor Control	W: Incorporated into PE-2 and PE-3.			
PE-8	Visitor Access Records		X	X	X
PE-8(1)	AUTOMATED RECORDS MAINTENANCE AND REVIEW				X
PE-8(2)	PHYSICAL ACCESS RECORDS	W: Incorporated into PE-2.			
PE-8(3)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	X			
PE-9	Power Equipment and Cabling			X	X
PE-9(1)	REDUNDANT CABLING				
PE-9(2)	AUTOMATIC VOLTAGE CONTROLS				

Physical Control Elements

Physical Controls	Perimeter security, fences, lighting, facility construction, keys and locks, access card and readers, …
Administrative Controls	Facility selection, facility construction and management, personnel identity badges and controls, evacuation procedures, system shutdown procedures, fire suppression procedures, hardware failure procedures, bomb threat and lock down procedures,…
Technical Controls	Physical access control and monitoring system, intrusion detection and alarm system, fire detection and suppression system, uninterrupted power supply, heating / ventilation / air conditioning system (HVAC), disk mirroring, data backup,…

Perimeter Security

Perimeter security controls are used to prevent, detect and respond to unauthorized access to a facility

Fire suppression system

Perimeter Control example…

Perimeter Control

Fencing – different heights serve different purposes:

- 3 – 4 feet – deter casual trespassers
- 6 – 7 feet – deter general intruders
- 8 feet with barbed wire slanted at a 45º angle – deter more determined intruders

PIDAS – Perimeter Intrusion and Detection Assessment System

- Fencing system with mesh wire and passive cable vibration sensors
- Detects intruder approaching and damaging the fence (may generate many false alarms)

Bollards – Small round concrete pillars placed around a building

- Protects from damage by someone running a vehicle into the side of the building or getting too close for car-bomb

Lighting – Streetlights, floodlights or searchlights

- Good deterrents for unauthorized access and personnel safety
- National Institute of Standards and Technology (NIST) standard requires critical areas to be illuminated 8 feet in height with 2-foot candle power

Perimeter Security - *physical control for facilities*

Natural access control to limit opportunities for crime

- Uses security zones to restrict movement and differentiate between areas
- Requiring different levels of protection
  - Public areas
  - Semi-private area
  - Private areas
- Limiting points of entry into a building, using structures (e.g. sidewalks & lights) to guide visitors to main entrances and reception areas

www.pinterest.com

Target Hardening

– Complements natural access controls by using mechanical and/or operational controls:
  - e.g. door and window locks
  - alarms, guards and receptionists
  - visitor sign-in/sign-out procedures
  - picture identification requirements,…

Facilities – Data Center

- Should not be located on the top floor because of risk of fire
- Should not be in the basement nor underneath bathrooms - flooding risk
- Ideally in the core of a building - provides protection from natural disasters and intrusion
- Should not be close to a public area – to ease security

Technical Controls for Physical Access Monitoring

Dry contact switch - uses metallic foil tape as a contact detector to detect whether a door or window is opened

Electro-mechanical detection system - detects a change or break in a circuit. It can be used as a contact detector to detect whether a door or window is opened

Vibration detection system - detects movement on walls, ceiling, floors by vibration

Pressure mat - detects whether there is someone stepping on the mat

Visual recording device - Camera and Closed Circuit TV (CCTV), records the activities taking place in a particular area. It should be used together with security guards to detect for anomalies

Technical Controls for Physical Access Monitoring

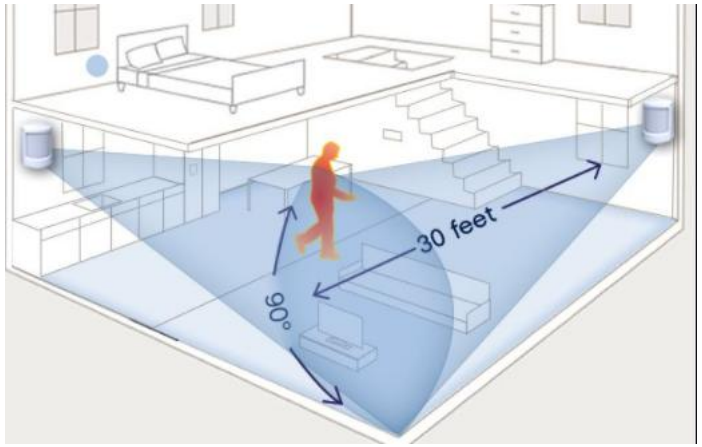
Photoelectric or photometric detection system - emits a beam of light and monitors the beam to detect for motion and break-in

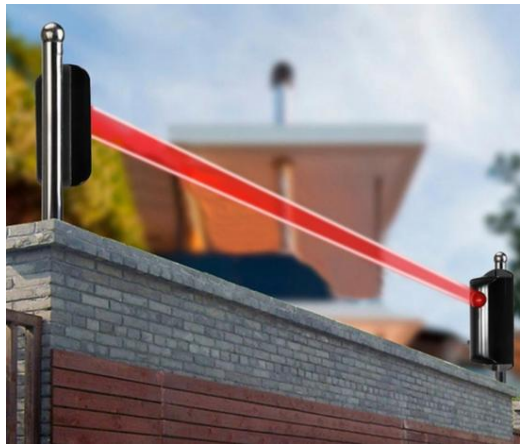
Wave pattern motion detector - generates microwave or ultrasonic wave, and monitors the emitted wave to detect for motion

Passive infrared detection system - detects for changes of heat wave generated by an intruder

Audio or Acoustical-seismic detection system - listens for changes in noise level

Proximity detector or capacitance detector - emits magnetic field and monitors the field to detect for any interruption. It is especially useful for protecting specific objects





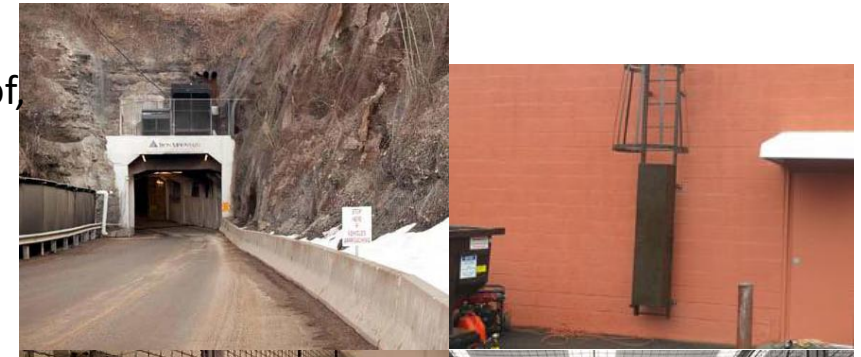
Construction design considerations

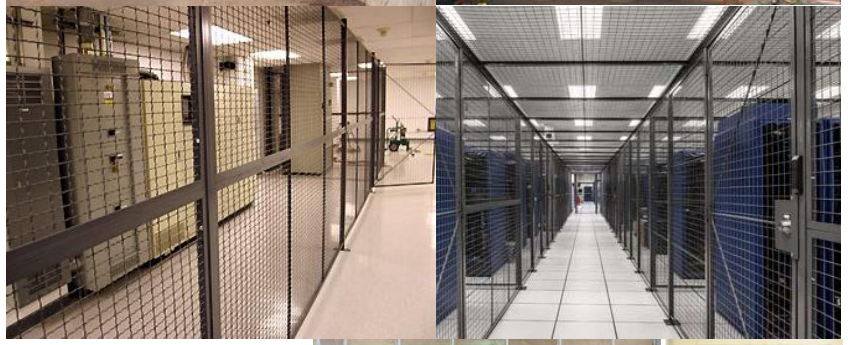
Exterior Walls – Able to withstand high winds, reduce electronic emanations (when needed), avoid windows at lower levels – otherwise fixed, shatterproof, opaque to conceal inside activities, and reinforced with bars at lower levels (when needed)…

Interior Walls – Must extend from floor to ceiling (through dropped ceilings and raised floors to stop intruders) if adjacent to restricted or secure areas, meet building and fire ratings (flammable material storage ratings), reinforced (Kevlar) to protect sensitive areas…

Doors – Resistant to forcible entry, fire rating equal to surrounding walls, unlocked from inside with emergency marking, electronic locks and access controls should "fail-soft" (unlocked during power outage) or "fail-safe" (locked during power outage) intrusion detection alarm, doors that swing out to facilitate emergency existing have hinges on the outside which must be secured so hinge pins are not easily lifted by placement of doors…

Windows – characteristics of windows material (opaque, translucent, transparent, shatterproof, bulletproof), intrusion detection alarms, placement of windows…





Construction design considerations

Ceilings – Consider fire and weigh-bearing building codes, waterproofing to prevent water leakage from upper floors.

- Drop-ceiling may temporarily hide intruders and small water leaks; conversely
- Stained ceiling tiles can reveal leaks while temporarily impeding water damage

Floors – Consider fire and weight-bearing building codes

- Raised floors require electrical grounding and non-conducting material to prevent safety risks

Wiring – All conduits, cable runs and wiring must be protected and comply with building and fire codes

- Special plenum cabling must be used because PVC-clad cabling releases toxic chemicals when it burns

Lighting – Exterior lighting for all physical spaces

- All conduits, cable runs and wiring must be protected and comply with building and fire codes

A plenum is the vacant area below a raised floor or above a drop ceiling. Fire in these areas can spread rapidly carrying smoke and noxious fumes o other areas of a burning building

Server rooms, wiring closets, media and evidence storage facilities

contain high-value equipment and media critical to:

- ***Ongoing business operations***
- ***Supporting investigations***

<u>Physical security controls</u> for these locations can include:

- **Strong access control**
  - Bi-factor (or tri-factor): key cards, PIN pad or biometric
- **Fire suppression**
  - Inert gas fire suppression is more common than water sprinklers
    - ***Water damages computer equipment***
- ***Video surveillance***
  - Cameras focused to observe on goings of both intruders and authorized personnel
- ***Visitor log***
  - Signed by all visitors classified as needing a continuous escort
- ***Asset check-in / check-out log***
  - All personnel are required to log introduction and removal of any equipment and media

Restricted and work area security often

receive additional physical security controls beyond:

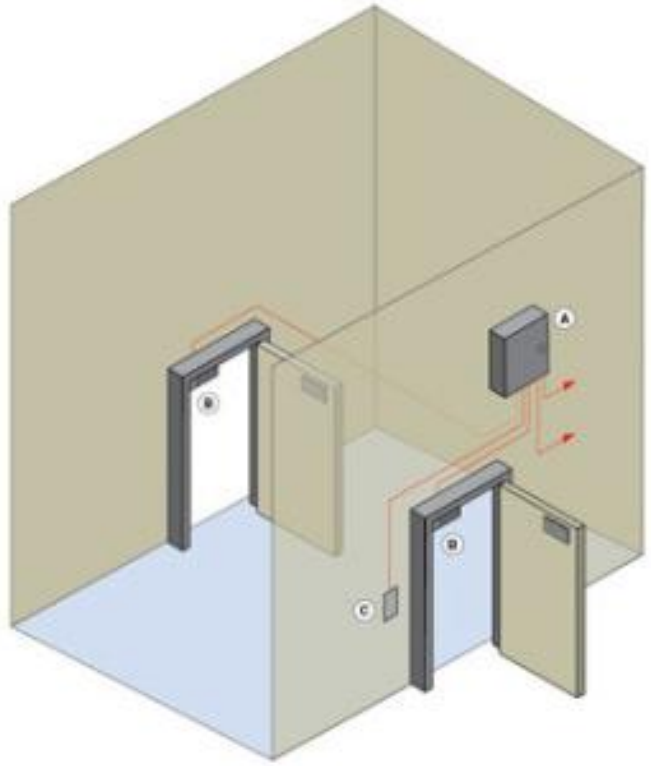
- ***Key card access control systems***
- ***Video surveillance***

<u>Physical security controls</u> for secure locations may also include:

- **Multi-factor key card entry**
  - Bi-factor (or tri-factor): Key cards + PIN pad or biometric
- **Security guards and guard dogs**
  - At ingress/egress points to prevent unauthorized access, roaming facility alert for unauthorized personnel or activities, involved in capture of unauthorized personnel in a facility
- ***Security wall and fences***
  - 1 or more to keep authorized personnel away from facilities
- ***Security lighting***
  - Additional lighting to expose and deter would-be intruders
- ***Security gates, crash gates, and bollards***
  - Limit the movement of vehicles near a facility to reduce vehicle-borne threats

<u>Physical security controls</u> for secure locations may also include:

- ***Mantrap***
  - is made of two doors, one for entry, one for exit from the booth/ mantrap. When the first door is open, the second remains locked until the first one is closed and the individual inside the booth is cleared by a security operator monitoring this interlocking system



- Examples of physical security attacks
  - "Piggybacking"
  - "Tailgating"
  - "Shoulder surfing" (Note: Not thwarted by a mantrap)

Utilities and heating, ventilation, and air conditioning (HVAC)

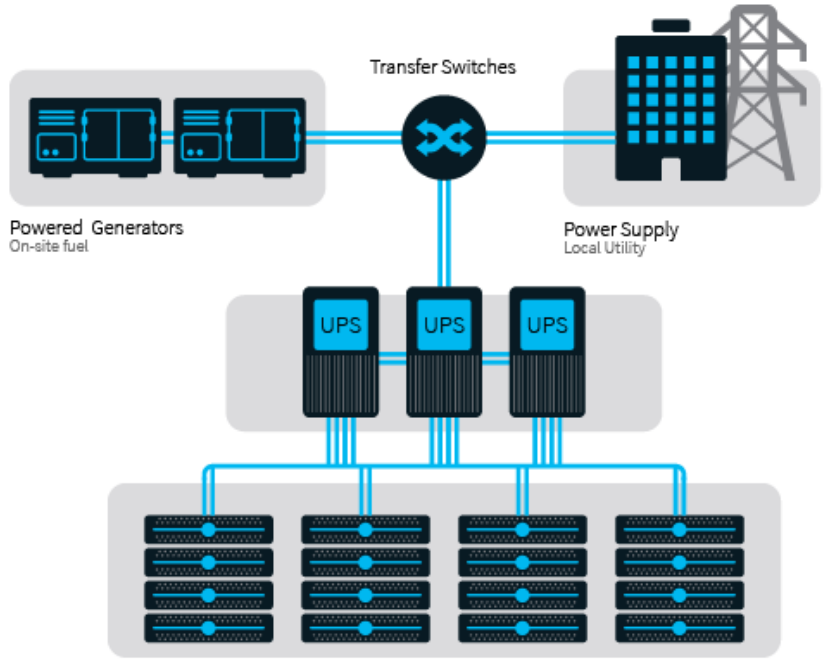
…are Environmental and life safety controls necessary for maintaining safe and acceptable operating environment for computers and humans

- **Electrical power**
  - **1+ dedicated feeders from 1+ utility substations or power grids**
  - Adequate physical access controls to circuit breakers and distribution panels
  - **Emergency Power Off (EPO) switch** installed near major systems and exit doors
    - ***To shut down power in response to fire or electrical shock***
  - **Backup power**

    Only for critical facilities and systems

    Source: Diesel or natural gas

    Fuel source must be locally stored for emergency life systems (such as emergency lighting and fire protection systems) – this often rules out natural gas pipelines



Electrical power continued…

- ***Controls for electrostatic discharge (ESD)***
  - ***Ideal humidity level for computer equipment is 40% - 60%***
    - ***Higher causes condensation and corrosion***
    - ***Lower increases potential for static electricity (ESD)***
      - » ***Static charge of 40V (volts) can damage circuits and 2,000V can shutdown a system***
      - » ***Minimum discharge felt by humans is 3,000V (if you feel it there's a problem)***
  - ***Proper grounding in-place***
  - ***Antistatic flooring, carpeting, and floor mats***
- ***Controls for electrical noise – a "transient" is a momentary line-noise disturbance***
  - ***Power line conditioners installed***
  - ***Proper grounding in place***
  - ***Shielded cables used***
- ***Electric anomalies include:***
  - Any amount of current over 0.01 amp is capable of producing painful to severe shock
  - Currents between **0.1** to **0.2** amp are lethal

It is not the volts that kill – it's the amps!

Electrical Event	Anomalie Definition
Surge	Prolonged rush of power
Spike	Momentary rush of power
Inrush	Initial power rush
Sag	Short drop in voltage
Brownout	Prolonged drop in voltage
Fault	Momentary loss of power
Blackout	Total loss of power

Electrical power continued…

Electrical Event	Anomalie Definition
Surge	Prolonged rush of power
Spike	Momentary rush of power
Inrush	Initial power rush
Sag	Short grop in voltage
Brownout	Prolonged drop in voltage
Fault	Momentary loss of power
Blackout	Total loss of power

- Uninterruptible Power Supply (UPS)
  - Is the most important protection against electrical anomalies
  - Is not a backup power source!
  - Is a temporary source of clean power for sensitive systems during electrical outages (sag, brownout, blackout)
  - Must be sufficient to provide 5 to 30 minutes of temporary power to support a proper controlled shutting down of protected systems and starting and bringing up a backup generator online
- Surge protectors and suppressors only provide minimal spike protection – not a substitute for a UPS

Power Protection

Uninterrupted Power Supply (UPS) to protect against a short duration power failure

There are **two types of UPS**:

1. **Online UPS** – It is in continual use because the primary power source goes through it to the equipment. It uses AC (alternating current) line voltage to charge a bank of batteries. When the primary power source fails, an inverter in the UPS will change DC (direct current) of the batteries into AC

2. **Standby UPS** – It has sensors to detect for power failures. If there is a power failure, the load will be switched to the UPS. It stays inactive before a power failure, and takes more time than online UPS to provide power when the primary source fails.

Power Protection

Backup/alternate power source to protect against a long duration power failure, e.g. uninterruptible power supply (UPS), motor generator, another electrical substation, etc.

Power line monitor to detect for changes in frequency and voltage amplitude

Voltage regulator and power line conditioner to protect against unstable power supply

- Used to compensate for peaks and valleys in the power supply and reduce peaks in the power flow to what is needed by the machine.
- Any valleys are removed by power stored in the equipment

Surge protectors protect against high-voltage bursts

Power Protection

Proper grounding for all electrical devices to protect against short circuit and static electricity, e.g. by using 3-prong outlets

Cable shielding to avoid interference

Emergency power off (EPO) switch to shut down the power quickly when required

Electrical cables should be:

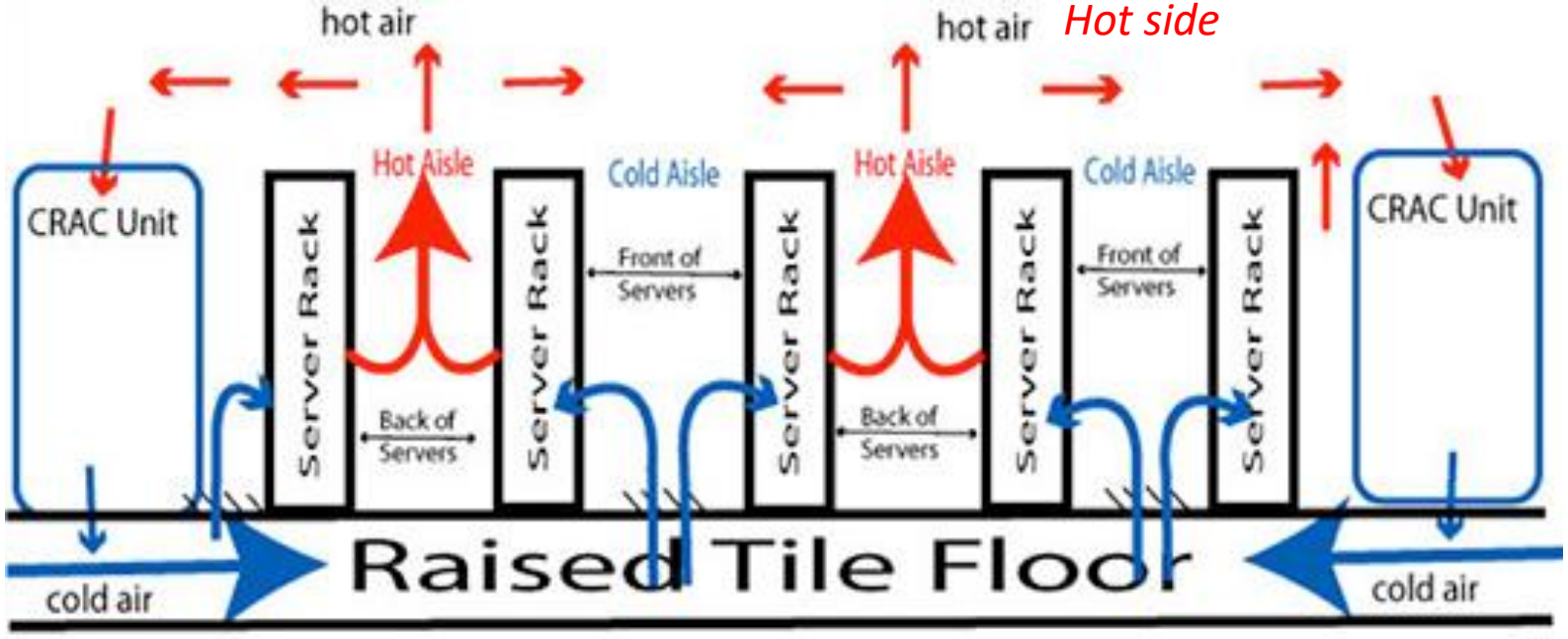
- placed away from powerful electrical motors and lighting to avoid electromagnetic interference.
- placed away from powerful electrical cables and fluorescent lighting to avoid radio frequency interference.

Heating, ventilation, and air conditioning (HVAC)

- Ideal temperature range for computer equipment is between 50°F and 80°F (10°C – 26°C)
  - Magnetic storage can be damaged at 100°F (38°C)

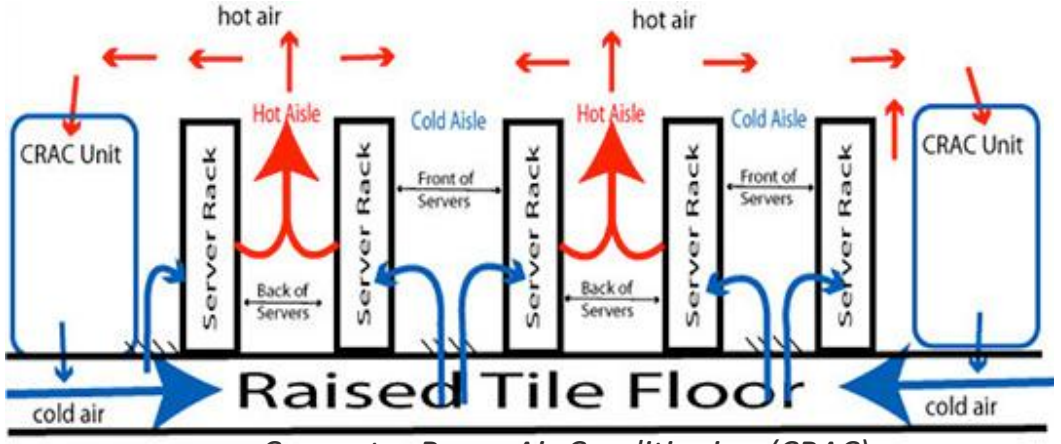
- Ideal humidity range for computer equipment is between 40% - 60 %
  - Higher humidity causes condensation and corrosion
  - Lower humidity increases potential for ESD (static electricity)

Power supplies are on the Hot side



Computer Room Air Conditioning (CRAC)

Heating, ventilation, and air conditioning (HVAC)



Computer Room Air Conditioning (CRAC)

Computer side panels of racks kept…

- Closed to ensure proper airflow for cooling and ventilation
- Locked for physical access control
- Blocked by blanking panels in place of gaps in half-filled racks to reduce hot and cold air mixing which reduces cooling system efficiency

- Emergency Power Off (EPO) switch should be installed near exists for manual emergency shutdown
- HVAC is shutdown automatically by most gas-discharged fire suppression systems
- HVAC should be dedicated, controlled and monitored to notify appropriate personnel when problems detected
  - If not need proper liaison with building manager to ensure everyone knows who to contact in case of emergency

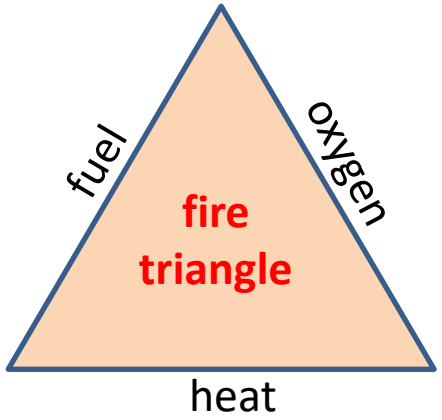
Water damage

- Damage from liquids (in general) can occur from many sources including:
  - Leaking roofs
  - Pipe breakage
  - Firefighting efforts
  - Spilled drinks
  - Flooding
  - Tsunamis

- Wet electrical equipment and computers are a lethal hazard
- **Preventative and detective controls** are necessary to make sure uncontrolled water does not destroy expensive assets or disrupt business operations
  - **Water diversion** barriers to prevent water from entering sensitive areas
  - **Water detection sensors and alarms** to detect presence of water and alert personnel in-time to prevent damage

Fire prevention, detection, & suppression

- Hazards associated with fires include:
  - Smoke,
  - Toxic vapors and materials
  - Water damage
  - Building collapse
- For a fire to burn it requires: fuel, oxygen and heat
  - *Fire extinguishing and suppression systems remove one of these or break up the chemical reaction of among the three to fight fires*



- Fires are classified by the type of fuel burned:

Class A, B, and C fires and primary extinguishing methods are covered on the CISSP exam!

D, K and F are not covered (Asia uses F not K)

Class	Fuel Description	Extinguishing Method
A	Common combustables: E.g. paper, wood, furnature, clothing…	Water or soda acid
B	Burnable fuels: E.g. gasoline or oil	CO_2, soda acid or Halon substitutes
C	Electrical fires: E.g. computers or electronics	CO2, or Halon substitutes - *Turn off electricity first!*
D	*Special fires: E.g. combustable metals*	*Special techniques, total immersion,…*
K (or F)	*Cooking oils or fats*	*Water mist or fire blankets*

Fire detection & suppression

3 main types of fire detection systems

1. **Heat-sensing**
2. **Flame-sensing**
3. **Smoke-sensing**

Modern detectors sense multiple indicators of fire

1. Heat-sensing fire detection systems

- Sense temperatures either
  - Exceeding a predetermined threshold level ("**Fixed-temperature** detectors")
    - *Associated with lower false-alarm rate - preferred*
  - Rapidly rising ("**Rate-of-rise** detectors")

2. Flame-sensing fire detection systems

- *Sense either **flicker** (pulsing) or **infrared** energy of flames*
  - *More expensive but provide rapid fire detection*

3. Smoke-sensing fire detection systems (smoke is a byproduct of fire)

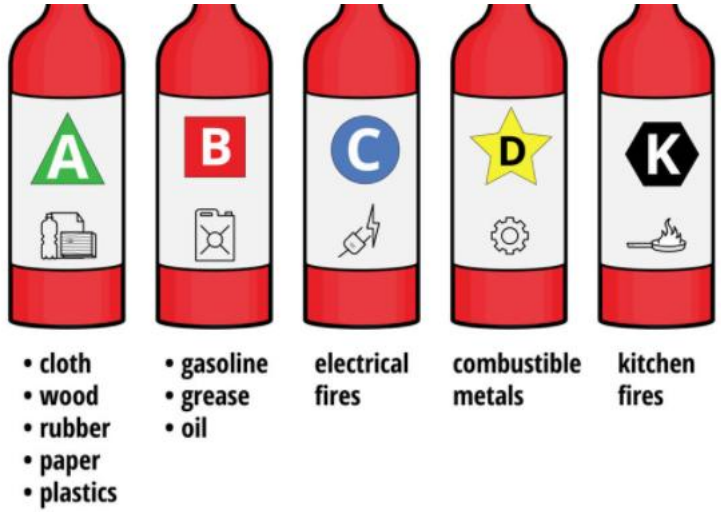
1. *Photoelectric: Senses variations in light intensity*
2. *Beam: Senses when smoke interrupts beams of light (similar to photoelectric)*
3. *Ionizing: Detects disturbances in normal ionization current of radioactive materials*
4. *Aspirating: Detects minute amount of smoke in air drawn into sample chamber*

Fire detection & suppression

2 main types of fire suppression (extinguishing) systems

1. **Water-sprinkler systems (Class A, D, K fires)**
    1. Wet-pipe (or closed-head)
    2. Dry-pipe
    3. Pre-action
    4. Deluge
2. **Gas discharge systems (Class B and C fires)**
    1. CO_2 Carbon dioxide (Class B and C fires)
    2. Soda acid (Class A and B fires)
    3. Gas-discharge (Class B and C fires)

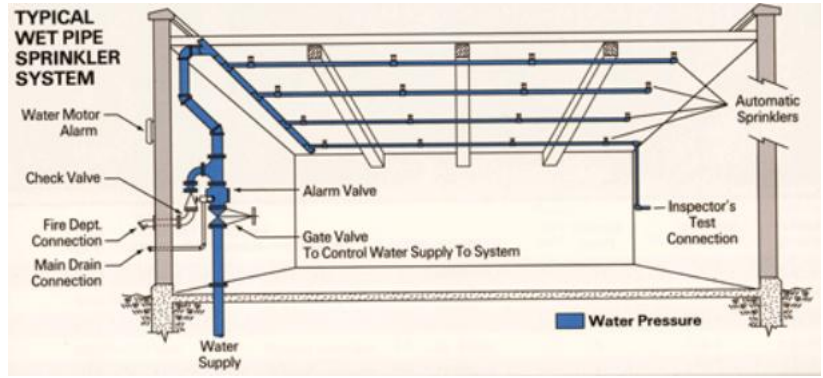
Class	Fuel Description
A	Common combustables: E.g. paper, wood, furnature, clothing…
B	Burnable fuels: E.g. gasoline or oil
C	Electrical fires: E.g. computers or electronics
D	*Special fires: E.g. combustable metals*
K (or F)	*Cooking oils or fats*



Extinguisher type and fire classes it is for should be clearly marked on the extinguisher!

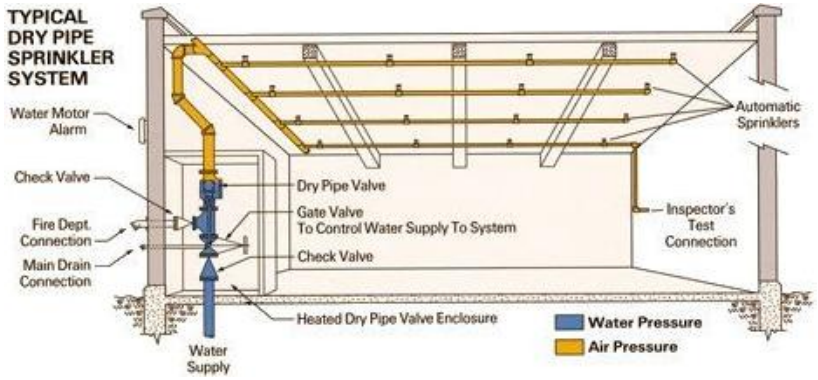
Fire detection & suppression

Water-sprinkler fire suppression systems (4 main types)



1. Wet-pipe (or closed-head)

- Most common and reliable
- Pipes always charged with water under pressure and ready for activation
- Fuse in nozzle melts or ruptures opening gate valve and releasing water
- Disadvantages: Flooding due to pipe failure (e.g. due to freezing in cold weather) or nozzle/fuse failures



2. Dry-pipe

- No standing water in the pipes
- Activation opens clapper valve, water flows in the pipe as air is blown out
- Helps protect from accidental flooding, provides time delay to (possibly) shutdown computer systems and/or power
- Less efficient than wet-pipe system

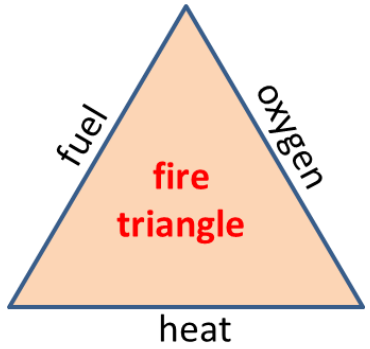
3. Pre-action – *Combines dry-pipe and wet-pipe systems*

- Pipes are initially dry. Triggering of heat sensor charges pipes with water (but does not discharge) and activates an alarm. When fusible link melts water is discharged, as in wet-pipe systems
- Reduces risk of accidental discharge and enables manual intervention
- Recommended systems for computer-equipment areas

4. Deluge – *Not typically used for computer-equipment areas*

- Quickly delivers large volumes of water while operating like a dry-pipe system

Fire detection & suppression



Gas fire suppression systems (3 main types)

1. Carbon dioxide (CO_2)

- Extinguishes fire by removing oxygen (from fire triangle)
- Most effective against Class B and C fires
- Removing oxygen makes it lethal and best suited for unmanned areas or with a delayed action with manual override in manned areas
- Used in portable extinguishers – keep within 50ft of electrical equipment and near all exits

2. Soda acid

- Suppresses flammable components with a chemical compound removing the fuel from the fire triangle
- Most effective against Class A and B fires
- NOT to be used for Class C fires because it is highly corrosive

3. Gas-discharge

- Creates a chemical reaction that separates elements of the fire triangle
- Most effective against Class B and C fires
- Uses inert gases that mixes thoroughly with the air, spreads extremely quickly and will not damage computer equipment, nor leave a liquid nor solid residue
- At concentrations of >10% these gases are harmful if inhaled
- Degrades into toxic chemicals when used on fires that burn at temperatures >900°F (482°C)
- Halon (which depleted ozone) was the preferred for gas-discharge fire suppression systems until 1994 when it was replaced with
  - FM-200 (the most effective), CEA-401 and CEA308, NAF-S-III, FE-13, Intergen, Argon or Argonite

Sources of environmental threats

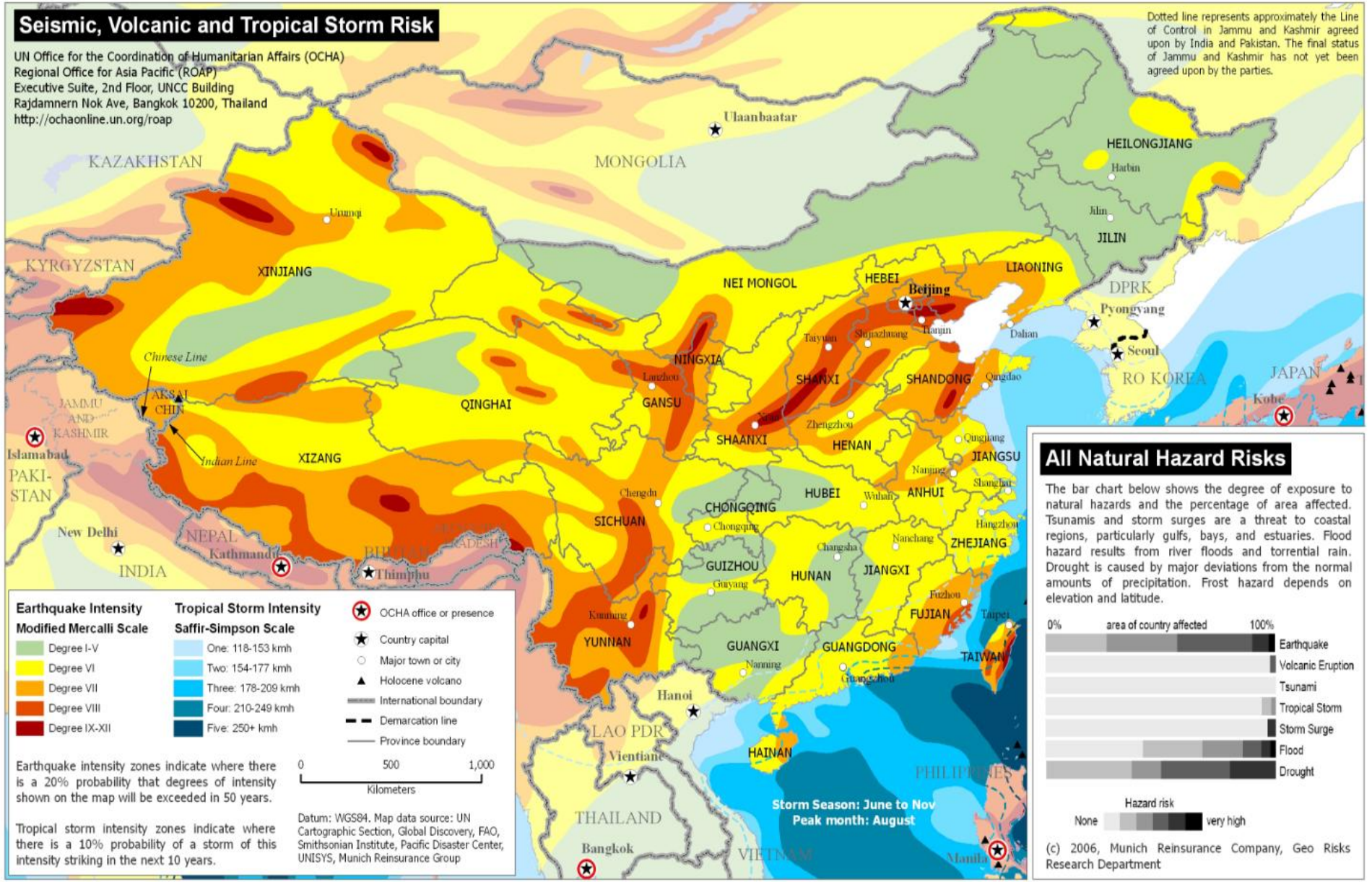
- **Severe weather**
  - Likelihoods of hurricanes, tornadoes, high winds, severe thunderstorms, rain, snow, sleet and ice
    - Causing fires, flooding/water damage, structural damage, loss of utilities and communications, and hazards to personnel
  - Lightening strikes can discharge 100,000 amperes of electric current and heat the air to 54,000^{o}F (30,000^{o}C), in US starts ~10,000 fires/year
- **Earthquakes and landslides**
  - Can generate vibration, movement, falling objects
  - May weaken structural integrity and cause unstable buildings to collapse

OCHA Regional Office for Asia Pacific

CHINA: Natural Hazard Risks

Issued: 29 June 2007

Where is a good place for a backup data center?



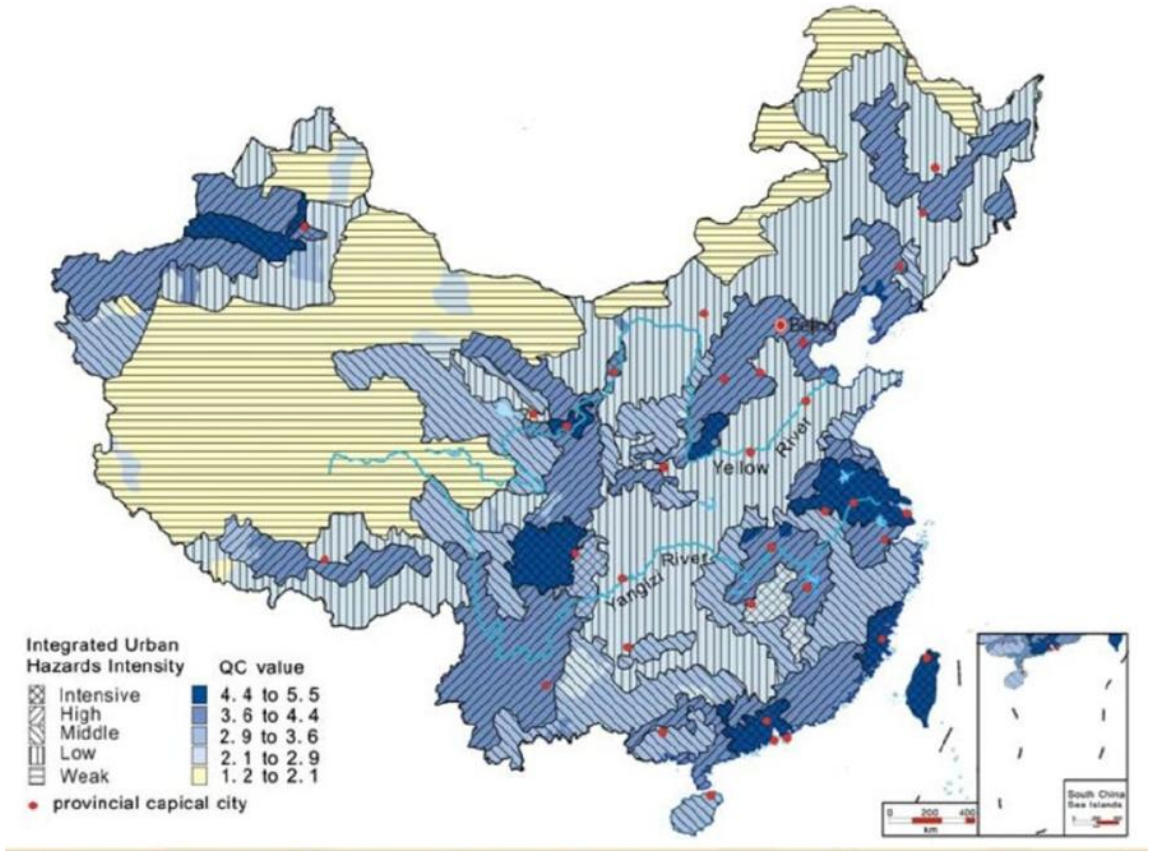
The names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations

Map Ref: OCHA_CHN_Hazard_v1_070629

Example of a multi-hazard map

Outdated maps, shown as examples

High speed internet locations (outdated map)



Multi-hazard map

Examples of information needed to plan location of a data center disaster recovery site

Site selection criteria…

- **Climactic disasters**
  - Is it in a high likelihood area for hurricanes, earthquakes, flood plains, tornadoes or other natural threats?
  - Are evacuation routes available and what is the level of emergency preparedness?
- **Visibility**
  - Is it an easy target for crime, terrorism or vandalism? (adjacent to high-profile organization, government or military target?)
  - Does it have a low profile for avoiding unneeded attention? Is it possible to avoid external markings?
- **Accessibility**
  - Is it convenience to travel: airports and/or railroads? What are the local traffic patterns?
  - Is it close to emergency services: police stations, fire stations and hospitals
- **Utilities**
  - Does location in the power grid provide clean/stable power?
  - Are telecommunications supported by sufficient high-speed fiber optic network connections?
  - Are there multiple provides to provide redundant utilities?
- **Local Considerations**
  - What are the crime rates and adjacent neighborhoods?
  - Is it near hazard materials storage? Railroad freight lines? Airport flight paths?
- **Joint tenants**
  - Are they serious enough about security?
  - Should/would they share physical security responsibilities and costs?

Test Taking Tip

Keep track of your guesses

- OK to guess and move on if you don't know answer
- Often in a standardized test, later questions on the same topic appear
- Remembering where you saw that topic earlier and if you guessed at the answer can make that information valuable

Quiz

1. What type of glass is much stronger than standard window glass and breaks into smaller fragments when shattered?

A. Plate glass
B. Enforced glass
C. Stain glass
D. Tempered glass

1. What type of glass is much stronger than standard window glass and breaks into smaller fragments when shattered?

A. Plate glass
B. Enforced glass
C. Stain glass
D. Tempered glass

2. Which of the following intrusion detection controls may have potential legal and privacy implications?

A. Motion detectors
B. CCTV
C. Mantraps
D. Dry contact switches

2. Which of the following intrusion detection controls may have potential legal and privacy implications?

A. Motion detectors
B. CCTV
C. Mantraps
D. Dry contact switches

3. What type of lock provides additional strength to prevent physical attack to doors?

A. Smart locks
B. Deadbolt locks
C. Key locks
D. Pushbutton locks

3. What type of lock provides additional strength to prevent physical attack to doors?

A. Smart locks
B. Deadbolt locks
C. Key locks
D. Pushbutton locks

4. What type of smoke detector triggers on changes in light caused by smoke?
   A. Infrared
   B. Heat
   C. Ionization
   D. Photoelectric

4. What type of smoke detector triggers on changes in light caused by smoke?
   A. Infrared
   B. Heat
   C. Ionization
   D. Photoelectric

Fire detection & suppression

3 main types of fire detection systems

1. **Heat-sensing**
2. **Flame-sensing**
3. **Smoke-sensing**

Modern detectors sense multiple indicators of fire

1. Heat-sensing fire detection systems

- Sense temperatures either
  - Exceeding a predetermined threshold level ("**Fixed-temperature** detectors")
    - *Associated with lower false-alarm rate - preferred*
  - Rapidly rising ("**Rate-of-rise** detectors")

2. Flame-sensing fire detection systems

- *Sense either **flicker** (pulsing) or **infrared** energy of flames*
  - *More expensive but provide rapid fire detection*

3. Smoke-sensing fire detection systems (smoke is a byproduct of fire)

1. *Photoelectric: Senses variations in light intensity*
2. *Beam: Senses when smoke interrupts beams of light (similar to photoelectric)*
3. *Ionizing: Detects disturbances in normal ionization current of radioactive materials*
4. *Aspirating: Detects minute amount of smoke in air drawn into sample chamber*

5. Which of the following is a problems with using dogs for perimeter control?
   A. Reliability
   B. Availability
   C. Training
   D. No judgment ability

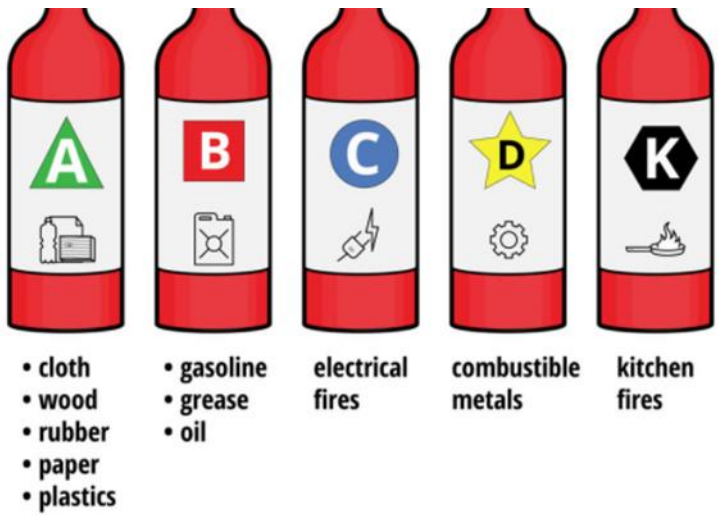
5. Which of the following is a problems with using dogs for perimeter control?
   A. Reliability
   B. Availability
   C. Training
   D. No judgment ability

6. HVAC falls under which set of controls?
   A. Administrative controls
   B. Physical and technical controls
   C. Environmental and life safety controls
   D. None of the above

6. HVAC falls under which set of controls?
   A. Administrative controls
   B. Physical and technical controls
   C. Environmental and life safety controls
   D. None of the above

7. Wood, paper, rubber, and plastics are classified as which class of combustibles?
   A. C
   B. B
   C. A
   D. D

7. Wood, paper, rubber, and plastics are classified as which class of combustibles?
   A. C
   B. B
   C. A
   D. D



8. Temperatures above what can damage magnetic storage?

A. 100 F or 38 C
B. 90 F or 32 C
C. 120 F or 49 C
D. 150 F or 66 C

8. Temperatures above what can damage magnetic storage?

A. 100 F or 38 C
B. 90 F or 32 C
C. 120 F or 49 C
D. 150 F or 66 C

9. Which of the following are NOT components of HVAC?

A. Air conditioning
B. Heating
C. Ventilation
D. Fire detection

9. Which of the following are NOT components of HVAC?

A. Air conditioning
B. Heating
C. Ventilation
D. Fire detection

10. Which of the following is true of bollards?
    A. Used to block automobile access
    B. Used to control crowds
    C. Used as a personnel barrier
    D. Used for entrance surveillance

10. Which of the following is true of bollards?
    A. Used to block automobile access
    B. Used to control crowds
    C. Used as a personnel barrier
    D. Used for entrance surveillance

11. Secure facility management is an example of which controls?
    A. Physical and technical controls
    B. Administrative controls
    C. Environmental and life safety controls
    D. None of the above

11. Secure facility management is an example of which controls?
    A. Physical and technical controls
    B. Administrative controls
    C. Environmental and life safety controls
    D. None of the above

12. What type of smoke detector is flame activated?
    A. Ionization
    B. Photoelectric
    C. Heat
    D. Infrared

12. What type of smoke detector is flame activated?
    A. Ionization
    B. Photoelectric
    C. Heat
    D. Infrared

Agenda

- ✓ Physical and Environmental Security
- ✓ Physical Security
- ✓ Environmental Security
- ✓ Test Taking Tip
- ✓ Quiz

Protecting Information Assets

- Unit#2c -

Physical and Environmental Security