Protecting Information Assets

- Week 7 -

Physical and Environmental Security
MIS5206 Week 7

- InTheNews
- Team project presentation
- Mid-term review
- Physical and Environmental Security
- Test Taking Tip
- Quiz
Mid-term exam review
Question 30

30. Who are responsible for ensuring that the information security policies and procedures have been adhered to?
   a. Information owners (2)
   b. Information systems auditors (3)
   c. Security officers (1)
   d. Executive management (2)
   e. All of the above (23)

Information System Auditor

Information system auditors are responsible for ensuring that the information security policies and procedures have been adhered to. They are also responsible for establishing the baseline, architecture, management direction, and compliance on a continuous basis. They are an essential part of unbiased information about the state of information security in the organization.

Vacca, page 452
12. The GREATEST benefit of having well-defined data classification policies and procedures is:
   a. A more accurate inventory of information assets (5)
   b. **A decreased cost of controls** (6)
   c. A reduced risk of inappropriate system access (17)
   d. An improved regulatory compliance (3)

**Explanation:**
A more accurate inventory of information assets is a benefit but would not be the greatest benefit of the choices listed.

An **important benefit of a well-defined data classification process** would be to lower the cost of protecting data by ensuring that the appropriate controls are applied with respect to the sensitivity of the data. Without a proper classification framework, some security controls may be greater and, therefore, more costly than is required based on the data classification.

Classifying the data may assist in reducing the risk of inappropriate system access, but that would not be the greatest benefit.

Improved regulatory compliance would be a benefit; however, achieving a cost reduction would be a greater benefit.
Question 31

31. Organizations can identify Personally Identifiable Information (PII) under their control using:

a. Privacy Threshold Analyses (7)

b. Privacy Impact Assessments (15)

c. De-identified information (8)

d. System or Records Notice (1)

GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Organizations are required to identify all PII residing within their organization or under the control of their organization through a third party (e.g., a system being developed and tested by a contractor). Organizations should use a variety of methods to identify PII. Privacy threshold analyses (PTAs), also referred to as initial privacy assessments (IPAs), are often used to identify PII. Some organizations require a PTA to be completed before the development or acquisition of a new information system and when a substantial change is made to an existing system. PTAs are used to determine if a system contains PII, whether a Privacy Impact Assessment (PIA) is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. PTAs are

NIST 800-122
Question 20

20. While auditing an e-commerce architecture, an IS auditor notes that customer master data are stored on the web server for six months after the transaction date and then purged due to inactivity. Which of the following should be the PRIMARY concern for the IS auditor?
   a. Availability of customer data (1)
   b. Integrity of customer data (7)
   c. **Confidentiality of customer data (14)**
   d. System storage performance

While auditing an e-commerce architecture, an IS auditor notes that customer master data are stored on the web server for six months after the transaction date and then purged due to inactivity. Which of the following should be the PRIMARY concern for the IS auditor?

A. Availability of customer data
B. Integrity of customer data
C. Confidentiality of customer data
D. System storage performance

C is the correct answer.

**Justification:**
A. Availability of customer data may be affected during an Internet connection outage, but this is of a lower concern than confidentiality.
B. Integrity of customer data is affected only if security controls are weak enough to permit unauthorized modifications to the data, and it may be tracked by logging of changes. Confidentiality of data is a larger concern.
C. **Due to its exposure to the Internet, storing customer data for six months raises concerns regarding confidentiality of customer data.**
D. System storage performance may be a concern due to the volume of data. However, the bigger issue is that the information is protected.
Question 19

19. The risk of dumpster diving is BEST mitigated by:
   a. Implementing security awareness training (15)
   b. Placing shred bins in copy rooms (2)
   c. Developing a media disposal policy (10)
   d. Placing shredders in individual offices (4)
Question 32

32. Linkable personally identifiable information (PII):
   a. Is used to distinguish an individual (2)
   b. Is information which is logically associated with other information about the individual (13)
   c. Is used trace an individual’s activities or status
   d. **Offers a possibility of logical association with other information about the individual** (16)

2.1 Identifying PII

PII is “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”

*Linked* information is information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable.
Question 8

8. Which of the following choices BEST helps information owners to properly classify data?
   a. Understanding the technical controls that protect data (1)
   b. **Training on organizational policies and standards** (18)
   c. Use of an automated data leak prevention (DLP) tool (1)
   d. Understanding which people need to access the data (11)
Physical and Environmental Security

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

• **Physical security addresses**
  – *mechanisms used to create secure areas around hardware*
  – Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorized personnel are allowed to access control system equipment

• **Environmental security addresses**
  – *safety of assets from damage from environmental concerns*
  – Control system equipment can be very expensive and may ensure human safety; therefore, protection is important from fire, water, and other possible environmental threats
Physical and Environmental 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
  – How the environmental issues affect equipment and systems
  – How people (as threats) can 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*
Sources of Physical Threats...

- **Water** – floods, leaks

- **Fire and chemicals** - explosion, smoke, toxic materials, industrial pollution

- **Energy** - electricity, magnetism, radio wave anomalies

- **Equipment** - mechanical or electronic component failure

- **Organism** - virus, bacteria, animal, insect

- **Human** – vandalism, sabotage, theft, terrorism, war
  - Consider both internal and external threats
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°F (30,000°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
Physical Control Types

**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, ...

**Physical Controls**

Perimeter security, fences, lighting, facility construction, keys and locks, access card and readers, ...

**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, ...
Site selection...

**An administrative control for facilities**

- **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?
- **Local Considerations**
  - What are the crime rates and adjacent neighborhoods?
  - Is it near hazard materials storage? Railroad freight lines? Airport flight paths?
- **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?
- **Joint tenants**
  - Are they serious enough about security?
  - Should/would they share physical security responsibilities and costs?
Perimeter Security - *physical control for facilities*

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

**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
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
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 45° 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
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 Physical Access Monitoring Controls

**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 Physical Access Monitoring Controls

**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 exiting 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*

**Physical security controls** 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

Physical security controls 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 unauthorized 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
Physical security controls 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.
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:**

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

<table>
<thead>
<tr>
<th>Electrical Event</th>
<th>Anomalie Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surge</td>
<td>Prolonged rush of power</td>
</tr>
<tr>
<td>Spike</td>
<td>Momentary rush of power</td>
</tr>
<tr>
<td>Inrush</td>
<td>Initial power rush</td>
</tr>
<tr>
<td>Sag</td>
<td>Short drop in voltage</td>
</tr>
<tr>
<td>Brownout</td>
<td>Prolonged drop in voltage</td>
</tr>
<tr>
<td>Fault</td>
<td>Momentary loss of power</td>
</tr>
<tr>
<td>Blackout</td>
<td>Total loss of power</td>
</tr>
</tbody>
</table>
Electrical power continued...

- **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:

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

- **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 power source** to protect against a long duration power failure, e.g. motor generator, another electrical substation, etc.

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

**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.

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

**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 – 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 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

- And 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:

<table>
<thead>
<tr>
<th>Class</th>
<th>Fuel Description</th>
<th>Extinguishing Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Common combustables: E.g. paper, wood, furniture, clothing...</td>
<td>Water or soda acid</td>
</tr>
<tr>
<td>B</td>
<td>Burnable fuels: E.g. gasoline or oil</td>
<td>CO2, soda acid or Halon substitutes</td>
</tr>
<tr>
<td>C</td>
<td>Electrical fires: E.g. computers or electronics</td>
<td>CO2, or Halon substitutes - <em>Turn off electricity first!</em></td>
</tr>
<tr>
<td>D</td>
<td>Special fires: E.g. combustable metals</td>
<td>Special techniques, total immersion,...</td>
</tr>
<tr>
<td>K (or F)</td>
<td>Cooking oils or fats</td>
<td>Water mist or fire blankets</td>
</tr>
</tbody>
</table>

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

*D, K and F are not covered*
Fire detection & suppression

3 main types of fire detection systems

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

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. Preaction
   4. Deluge

2. Gas discharge systems (Class B and C fires)
   1. CO\textsubscript{2} Carbon dioxide (Class B and C fires)
   2. Soda acid (Class A and B fires)
   3. Gas-discharge (Class B and C fires)

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. Preaction – 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 (CO₂)
   - 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
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. Which type of access control suffers from problems with false-positives and false-negatives?
   A. RFID (Radio Frequency Identification)
   B. Biometrics
   C. Smart locks
   D. Smart cards

2. 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

3. 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

4. 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

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

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

7. 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

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

9. Temperatures above what can damage magnetic storage?
   A. 100 F
   B. 90 F
   C. 120 F
   D. 150 F

10. Which of the following are NOT components of HVAC?
    A. Air conditioning
    B. Heating
    C. Ventilation
    D. Fire detection

11. 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

12. 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

13. What type of smoke detector is flame activated?
    A. Ionization
    B. Photoelectric
    C. Heat
    D. Infrared
1. Which type of access control suffers from problems with false-positives and false-negatives?
A. RFID
B. Biometrics
C. Smart locks
D. Smart cards

2. 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

3. 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

4. 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

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

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

7. 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

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

9. Temperatures above what can damage magnetic storage?
A. 100 F
B. 90 F
C. 120 F
D. 150 F

10. Which of the following are NOT components of HVAC?
A. Air conditioning
B. Heating
C. Ventilation
D. Fire detection

11. 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

12. 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

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