Physical Security Requirements

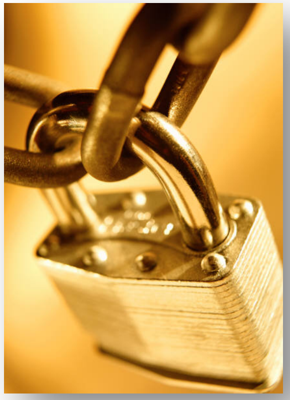
Marcus Bendtsen
Institutionen för Datavetenskap (IDA)
Avdelningen för Databas- och Informationsteknik (ADIT)

Physical Security Requirements

- Protect against physical threats:
  - Fire, smoke, water, earth movements, storms, sabotage/vandalism, explosion/destruction, toxic materials, equipment failure, theft, etc.
- Agenda:
  - Site and facility design considerations
  - Forms of physical access controls
  - Environment and life safety

Site and Facility Design Considerations

- There are several questions one should ask when building new or looking to buy facilities.
- These questions should be answered by technical and security professionals.
- The BCP team + security staff (e.g. guards, experts) is a good starting point.



Site and Facility Design Considerations

Site Selection

- **Cost**, **location** and **size** are all important when selecting a site, but the **security requirements** must take precedence.

- Susceptibility to **riots**, **looting**, **break-ins** - areas with high crime-rate should be avoided.

- Environmental threats - fault lines, hurricanes regions, etc. should also be avoided.

Site and Facility Design Considerations

Site Selection

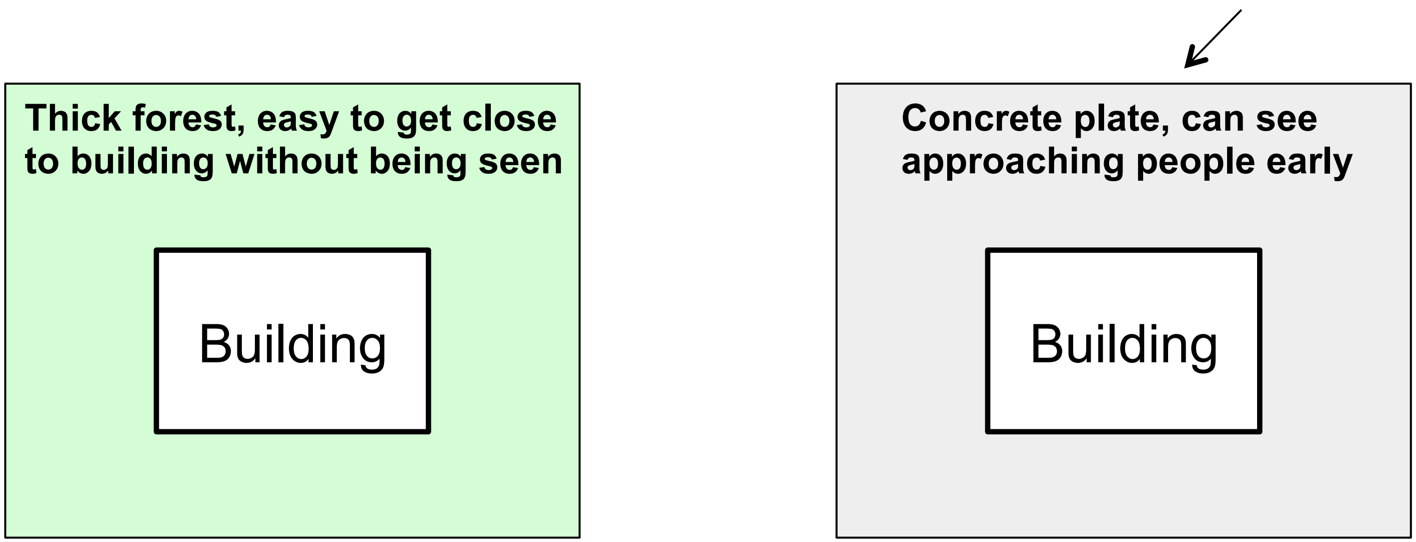
- Proximity to other buildings and businesses – what kind of attention do they draw?
- Proximity to emergency-response?
- Unique hazards in the area? – Chemical plants, construction sites, etc.
- Is it nearby residential, business or industrial areas?

Site and Facility Design Considerations

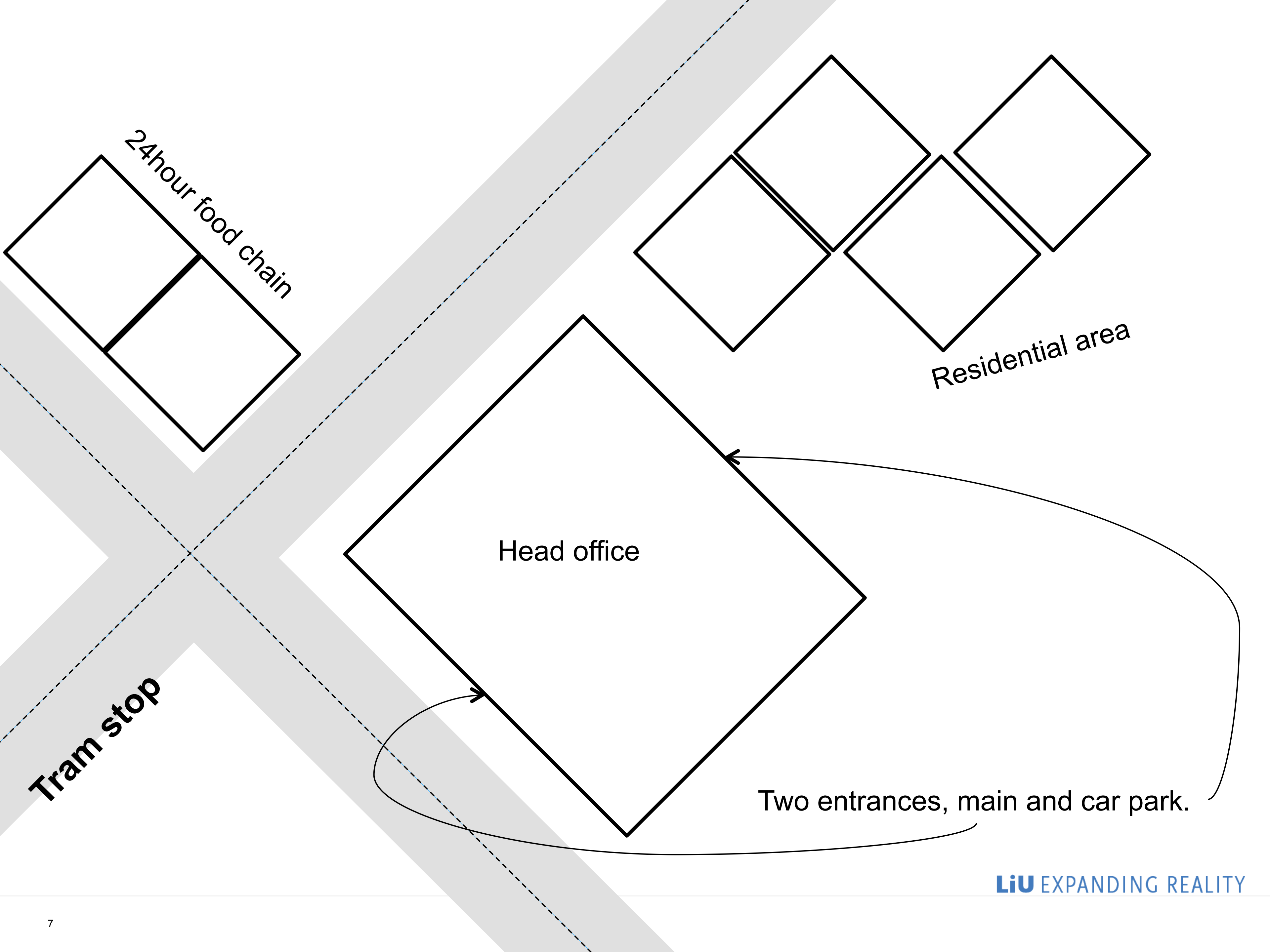
Site Selection

- What is the surrounding terrain? Would it be easy to approach the facility by vehicle or on foot without being seen?
- Single entrances are great for providing security, but multiple entrances are better for emergencies.

Large corporations can afford to build campuses to control the surrounding area.



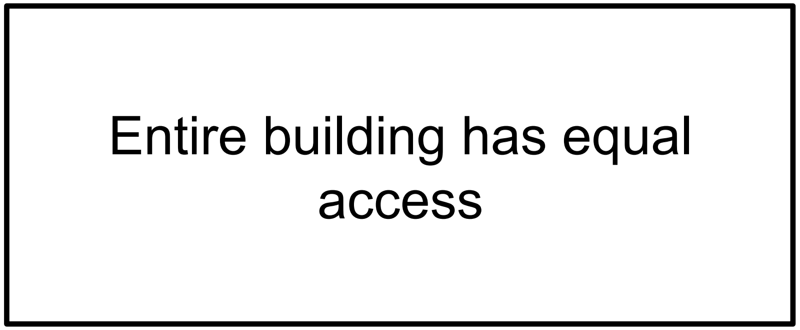
LiU EXPANDING REALITY

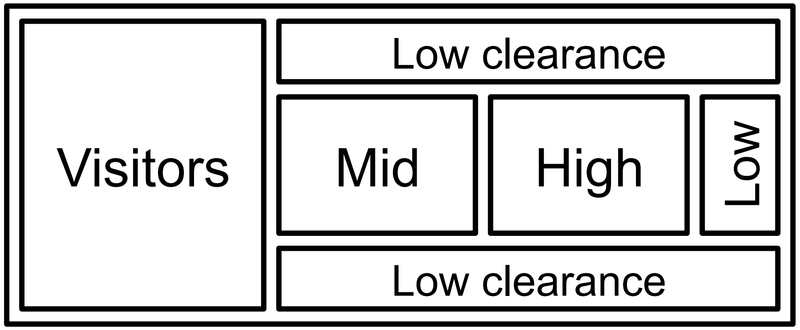

24hour food chain
Residential area
Head office
Tram stop
Two entrances, main and car park.

Site and Facility Design Considerations

Facility design

- Internal security, including working areas and visitor areas, should be considered carefully.
- There should not be equal access to all locations within a facility.
    - Anyone that enters the facility should have access to the restrooms, but not to the server rooms.
- Valuable and confidential assets should be located at the centre of protection.





Site and Facility Design Considerations

Facility design

- Walls and partitions can be used to compartmentalize working areas into security areas.
  - This avoids *shoulder surfing* and eavesdropping.

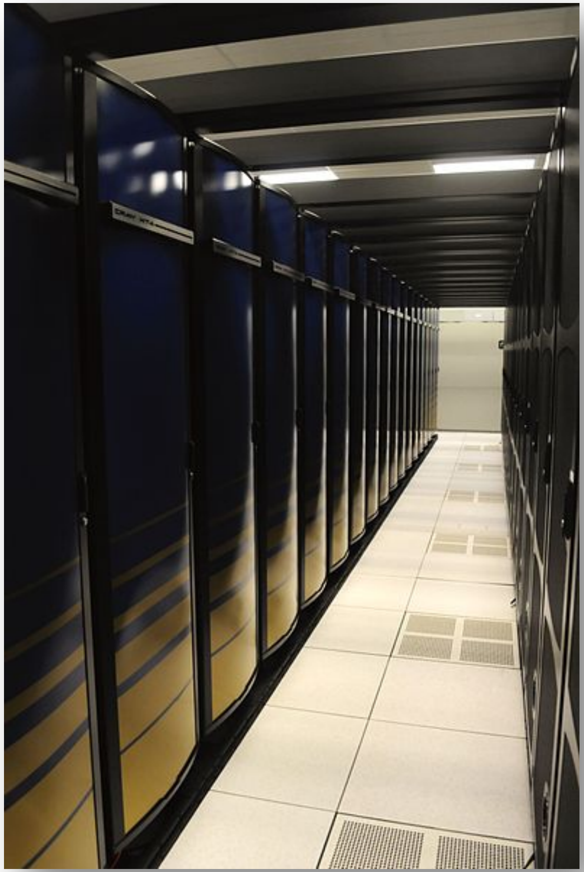
- Floor to ceiling walls should be used to separate areas with different level of confidentiality.

- Only people with clearance corresponding to the classification of the work area should be allowed access.

Site and Facility Design Considerations

Facility design

- Server rooms should have very high protection.
  - No problem making them human incompatible
    - Low lighting, loud noise, equipment stacked making it hard to manoeuvre.
  - Designed to support optimal operation and block human access or intervention.
  - Ensure that the walls to the server room has a one-hour minimum fire rating (i.e. slow penetration of fire).



Site and Facility Design Considerations

Visitors

- Plan how to handle visitors:
  - Assign an escort to visitor, their access and activities are monitored closely.
  - This includes external contractors, such as plumbers.
  - Failing to track visitors can lead to malicious activity.
  - Design areas where visitors can roam freely, like lobbies etc. This is convenient for family and friends of employees.

LiU EXPANDING REALITY

Site and Facility Design Considerations

Escorting ex-employees

- If an employee is immediately dismissed, possibly due to misconduct, then they should be escorted out of the building.

- Key cards to the building should be taken immediately.

Forms of Physical Access Controls

Fences, Gates, Turnstiles and Mantraps

- A fence defines a perimeter, they clearly differentiate areas that are under specific level of security.
  - Barbed wire, concrete walls, invisible perimeters using motion and/or heat detectors.

- A gate is a controlled exit and entry point in a fence.
  - Use as few gates as possible
  - Make sure that the deterrent factor is as high as the fence, i.e. do not use a simple easy to break gate for a 8 feet concrete wall.

- Turnstiles are gates that only work in one direction.

Forms of Physical Access Controls

Fences, Gates, Turnstiles and Mantraps

- A mantrap is a double set of doors that can be protected by a guard.
  - The purpose is to immobilize a subject until he or she has identified and authenticated themselves.
  - If the subject is authorized then the inner door is opened for access.
  - If the subject is not authorized then both doors are locked until security personnel reach the area.
  - Mantrap can include other security measures, such as metal detectors, scales to weigh the subject (to avoid piggybacking), and other forms of authentication.

Forms of Physical Access Controls

Lighting

- Another type of perimeter defence:
  - Discourages intruders who prefer to work in the dark (thieves etc.).
  - Not very strong perimeter defence and should be used in combination with other mechanisms.
  - Combined with guards, dogs, CCTV it can be very useful.
  - Avoid lighting up other security mechanisms, so as to not give them away, such as guard posts, CCTV, etc.

  - Strong lighting can cause glare in cameras and can disrupt other mechanisms, and so it should be avoided.

Forms of Physical Access Controls

Security guards and dogs

- Most static mechanisms require that personnel at some point intervene.
- Security guards are there to intervene when something has happened.
- Guards can be used to monitor access or to watch surveillance monitors.
- Guards can adapt and make judgment calls.

Forms of Physical Access Controls

Security guards and dogs

- Unfortunately security guards do not fit into all situations, and getting good guards that are reliable may not be easy.
  - Subject to physical injury, illness, vacation, distractions, and vulnerable to social engineering.
  - Only offer protection up to the point where their life is endangered.
  - They are unaware of the scope of the operations within a facility, and are not equipped to respond to every situation.
  - Security guards are very expensive.

Forms of Physical Access Controls

Security guards and dogs

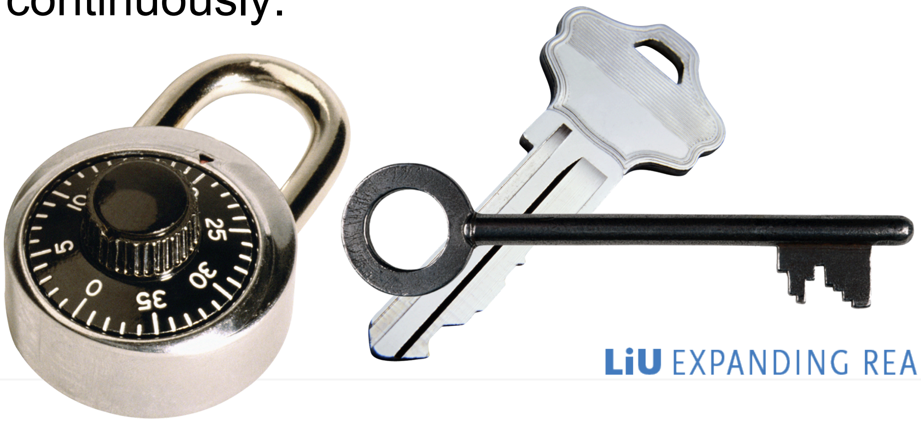
- Dogs are an alternative.
  - They can be used as perimeter defence.
  - Excellent at detection and deterring would-be intruders.
  - Are however also expensive and require maintenance.

LiU EXPANDING REALITY

Forms of Physical Access Controls

Keys and Combination locks

- Locks are designed to prevent access, and are a crude way of forcing identification and authentication:
  - If you have the key or combination then you are who you say you are, and have certain rights.
  - Key-based are cheap, but susceptible to picking and expensive to replace if somebody looses a key.
  - Programmable combination locks are more expensive to invest in, but the code can be replace continuously.



Forms of Physical Access Controls

Badges

- Badges, identification cards, and security IDs are forms of physical identification.
  - Can be simple, a picture of the person that owns the badge is placed on the badge. The badge is then showed to security personnel to gain entrance.
  - Can be complex and include magnetic strips or RFIDs that allow the badge to be used as a key.

Forms of Physical Access Controls

Motion detectors

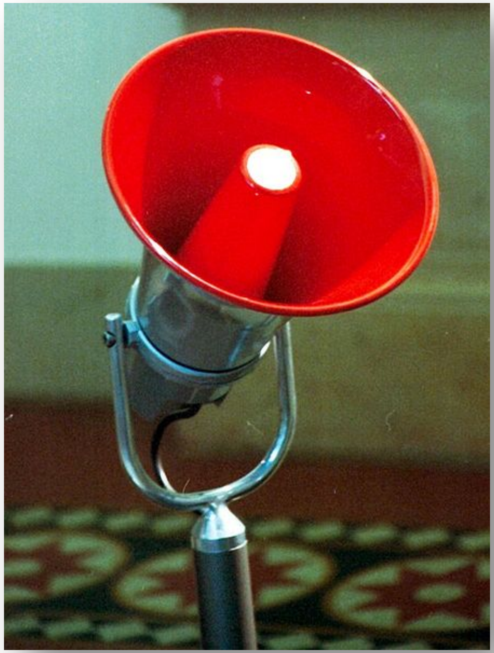
- ***Infrared motion detectors*** – Measure changes in infrared light
- ***Heat-based motion detectors*** – Measure changes in heat
- ***Wave pattern motion detectors*** – Measure changes in reflections of microwave signals
- ***Capacitance motion detectors*** – Measure changes in the electrical or magnetic field
- ***Photoelectric motion detector*** – Changes in visible light
- ***Audio motion detector*** – Listens for abnormal sounds

Forms of Physical Access Controls

Intrusion alarms

Whenever a motion detector registers a significant change it triggers an alarm.

- **Deterrent alarm** – Shuts doors, engages additional locks, makes it harder to continue the attack
- **Repellent alarms** – Audio siren or bell and turn on lights – force attackers away.
- **Notification alarm**s – Usually silent, but record data about incident and notifies admin, security guards, law enforcements etc. Bring authorized personnel in hope of catching intruder.



Forms of Physical Access Controls

Motion detection and Intrusion alarms

- As sensitivity of detection and alarms increase, false triggers occur more often.
  - Animals, bugs, even authorized personnel may accidently trigger one system.

- It is advisable to combine multiple systems and require that two or more of them trigger in quick succession before the alarm is raised.

Forms of Physical Access Controls

Access abuse

- Humans are experts at abusing security mechanisms
  - Propping open secured doors
  - Placing the mouse on the keyboard to avoid auto-logoff
  - Same PIN or password for many applications/facilities
  - *Masquerading* – Using someone else's security ID to gain entry into a facility.
  - *Piggybacking* – Following someone through a secured gate or doorway.

- Using trails of logs, including when access was request, how access was used, and who requested access can be useful in reconstruct abuse events.

Forms of Physical Access Controls

Emanation security

- Electrical devices emanate electrical signals that can be intercepted by unauthorized individuals.

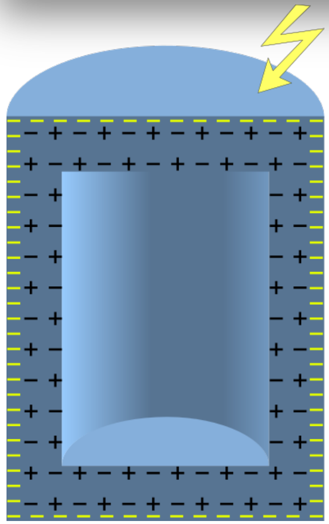
- The signals may contain confidential, sensitive, or private data.
  - Wireless networking, mobile phones, radio, etc.

- Using the right equipment, unauthorized users can interpret electromagnetic or radio frequencies and interpret the confidential data.

Forms of Physical Access Controls

Emanation security

- **Faraday cage**
  - A box, mobile room or entire building that is designed with an external metal skin, often a wire mesh.
    - Skin is applied front, back, left, right, top and bottom.
  - This skin prevents electromagnetic signals from exiting or entering the area that the cage encloses.



LiU EXPANDING REALITY

Forms of Physical Access Controls

Emanation security

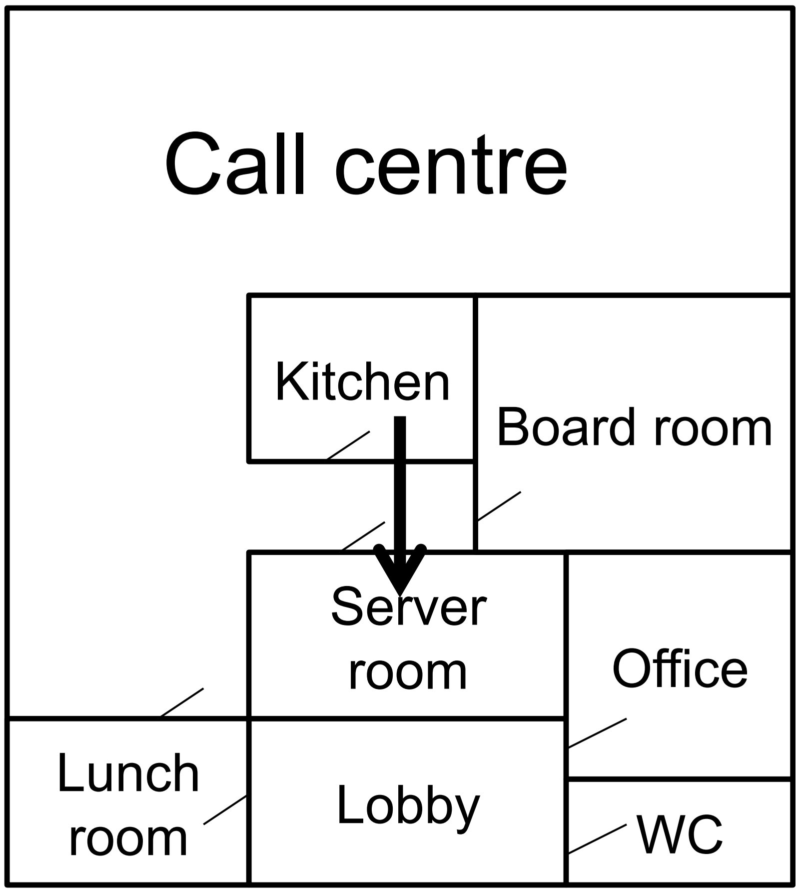
- **White noise**
  - Broadcast false traffic at all times to mask or hide the presence of real emanations.
    - Use an existing real signal that is not confidential
    - A constant signal, or random noise
    - Maybe not as effective as a Faraday cage, but much cheaper

Environment and Life Safety

- **Electricity**
  - Electricity does not only keep IT running, but also keeps air conditioning, fans, heating, etc. that can be crucial for personnel in some environments.
  - UPS is not only for IT but can also be used for environment systems.
- **Temperature, Humidity and Static**
  - Server rooms should have a temperature between 15 to 23 degrees Celsius.
  - Humidity needs to be controlled: high humidity causes corrosion, low humidity causes static electricity.
  - Non static carpeting in low humidity environments can still generate static charges enough to do permanent circuit damage.

Environment and Life Safety

- **Water**
  - Server rooms should be placed away from water, and no water pipes should run through the server room.
  - Water and electricity spells disaster for the components, but it also poses a very real risk to personnel that may be electrocuted.
  - If the dishwasher breaks and floods the kitchen then it may run into the server room if there is clearance under the doors.

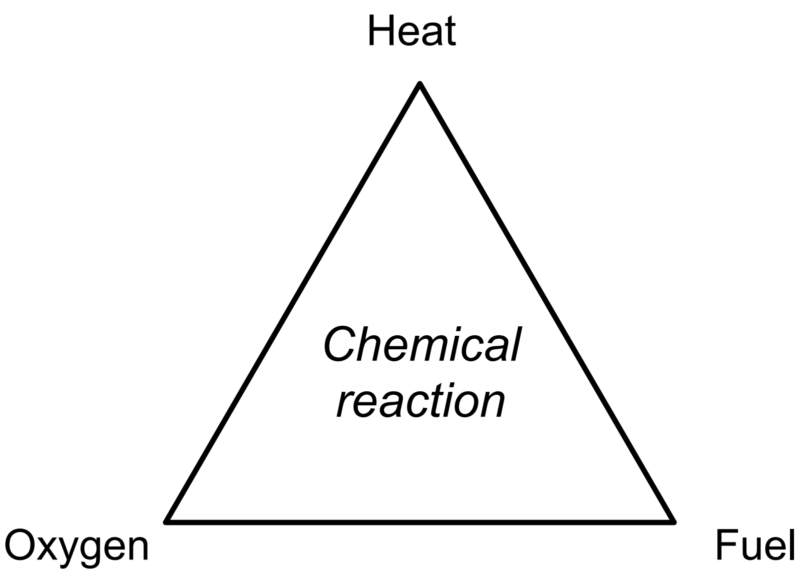


Environment and Life Safety

- **Water**
  - Do not focus solely on plumbing leaks, but also consider flooding when placing the server room (maybe the basement isn't the best place for the server room).
  - Ground floor is not a great idea either, as it is usually easier to break into rooms on the ground floor.
  - Some recommend the absolute middle of the building, but there are other things to consider (ventilation, etc.).

Environment and Life Safety

- **Fire prevention, Detection and Suppression**
- The fire triangle demonstrates the different ways one can suppress fire.
  - Water suppresses temperature.
  - Dry powders suppress fuel supply.
  - CO_2 suppresses oxygen supply.
  - Halon substitutes and other non-flammable gases interfere with the chemistry of combustion.

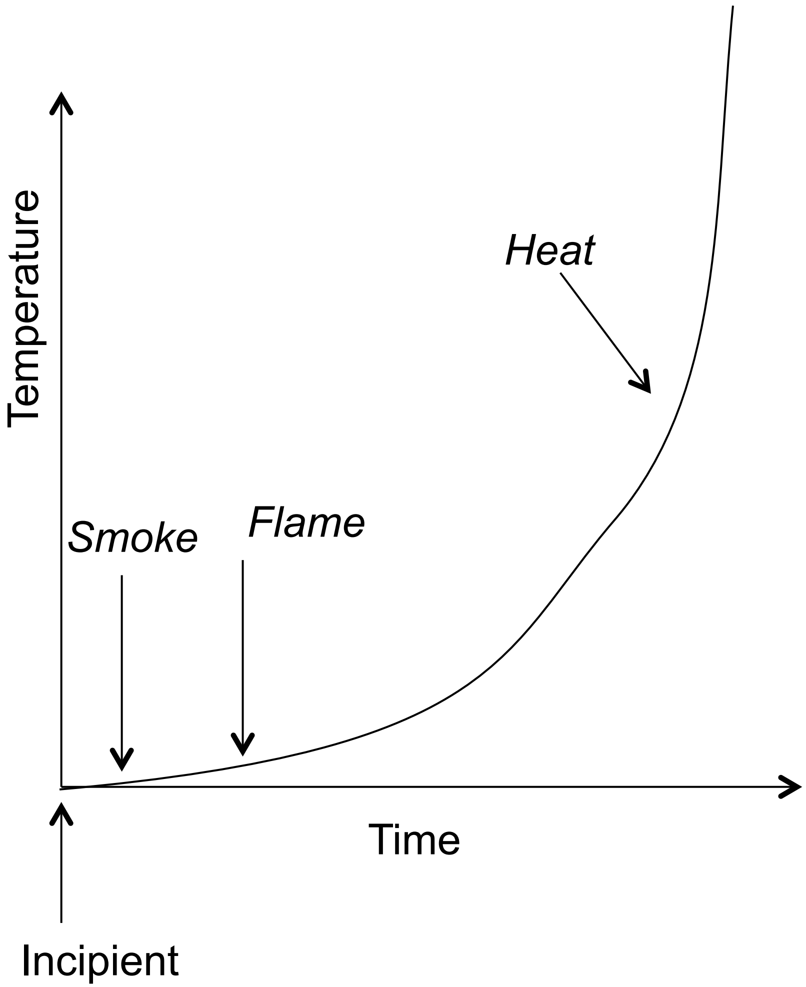


- Selecting a suppression medium should include considering the fire triangle, what are you trying to achieve?

LiU EXPANDING REALITY

Environment and Life Safety

- Personnel awareness of fire is key, as it is much easier to extinguish a fire in its early stages.
- Once the fire has hit stage 4 everything in the area is burning and it is to late to salvage anything.
- Select extinguishers carefully, you can not use a water extinguisher on burning liquids, as they splash the liquid and usually the liquid floats on water.



Environment and Life Safety

- There are automatic fire detection systems that can trigger when a piece inside of them melt or when they detect high speed temperature increase.
- This usually triggers an alarm, but can also trigger automatic extinguish.

- Water sprinklers are common in areas were people are working:
  - They can be prefilled with water, ready to dispense at any time (but can leak).
  - They can be dried and filled first when the alarm is raised (slower but not prone to leaks).
  - Exists combinations, where pre-alarms fill the pipes and then the emergency alarm releases the water.

Environment and Life Safety

- There are automatic fire detection systems that can trigger when a piece inside of them melt or when they detect high speed temperature increase.
- This usually triggers an alarm, but can also trigger automatic extinguish.

- For server rooms it is preferable to use gas based extinguishers.
  - Gas discharge systems usually remove oxygen from the air.
  - This can be hazardous for humans, and should therefore never be used in an environment where personnel exists.
  - Excellent for server rooms, but some gases are not environment friendly and may be illegal.

Linköpings universitet

expanding reality

www.liu.se