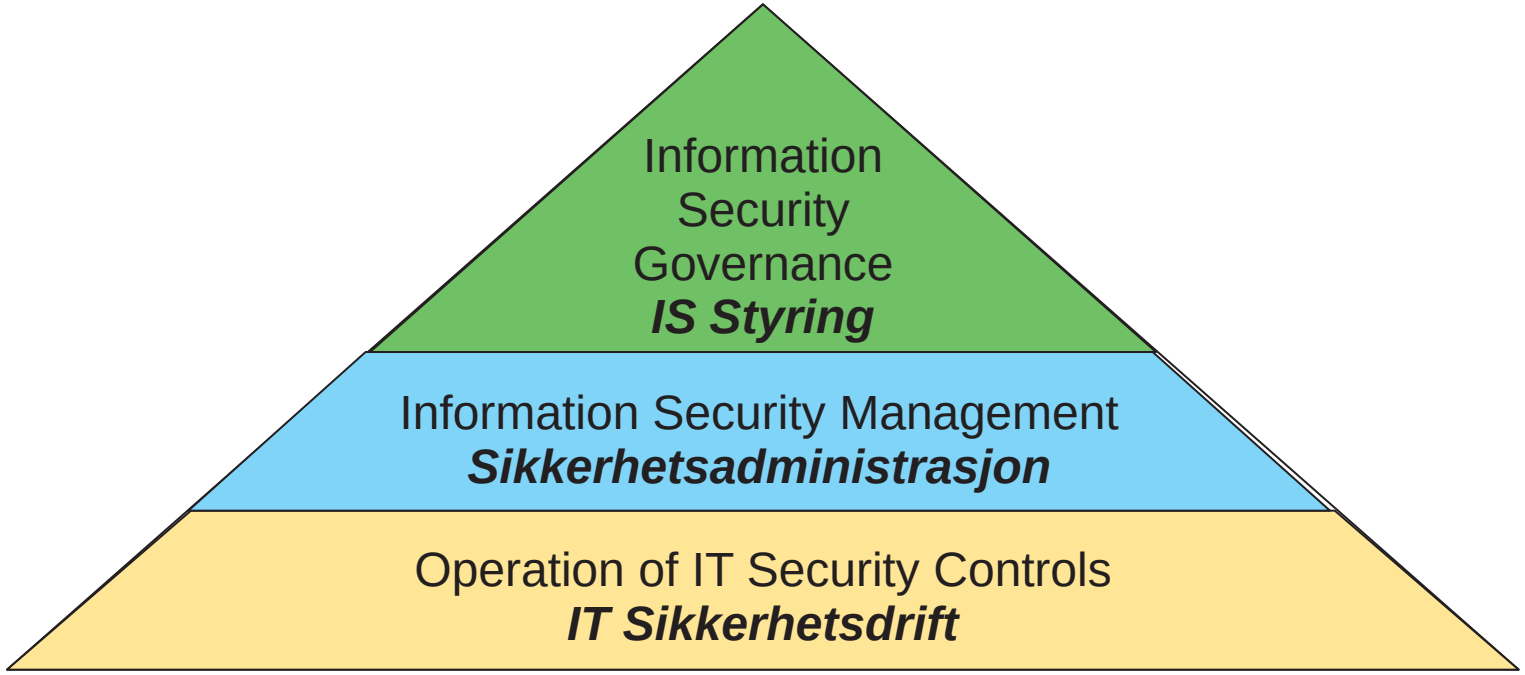
INF3510 Information Security
University of Oslo
Spring 2012

Lecture 2

Information Security Management, Human Factors & Physical Security

Audun Jøsang

IT security activities in the organisation



What is information security management?

Includes:

- Risk management,
- Definition and maintenance of security policies
- Establishing and running a security organisation (ISMS)
- Information classification
- Definition of security procedures, standards & guidelines
- Deployment and maintenance of security controls
- Security education and training
- Disaster recovery and business continuity planning

Who is responsible for ISM?

- Management
  - CEO, CSO, CIO
  - Allocate resources, endorse and abide security policies
- IT Security staff
- General security staff, i.e. guards, janitors etc.
  - Important for physical security
- IT staff
- Users
- Third parties
  - Outsourced information security management
  - Customers, suppliers, business partners

Terminology

- Standards: Guidelines on best practice or widely accepted methods for controlling information security and can be used as checklists for a security program.
- Best practice: Implementation of widely accepted security methods that provide the best level of assurance
- Baseline: The minimum level of security necessary to support and enforce the security policy
- Due diligence: Investigating and understanding risk
- Due care: Having security policies and implementing a reasonable security program that balances the identified risks.

IS Management Standards

- ISO Security Management standards:
  - ISO/IEC 27002 Information Technology – Code of practice for information security management
  - ISO/IEC 27001 Information Security Management Systems
  - ISO standards cost money
- USA
  - NIST (National Institute for Standards and Technology) Special Publications, including SP800-12, SP800-14, SP800-18, SP800-26 and SP800-30, SP800-64
  - NIST standards are free

ISO/IEC 27002– What is it?

Code of practice for information security management

- A checklist of general security controls to be considered implemented/used in organisations
- Internationally recognised generic information security standard

Objective:

- "… to provide practical guidelines for developing organizational security, standards and effective security management practices and to help build confidence in inter-organizational activities."

ISO/IEC 27002 - History

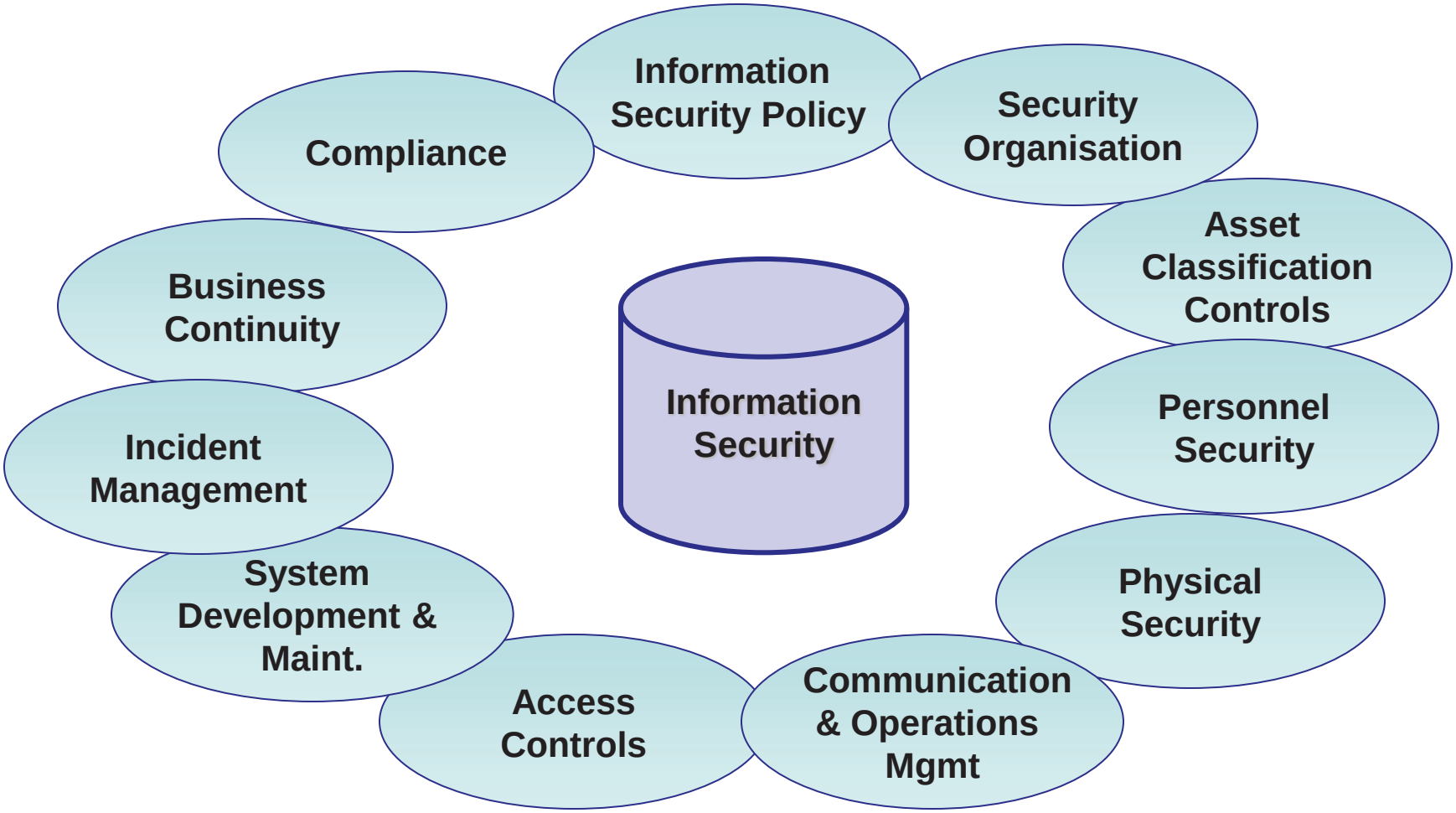
- In early 1990's, recognized need for a practical guide for information security management
  - Group of leading companies in the UK combined to develop *"Code of Practice for Information Security Management"*
  - Published in UK as BS7799 version 1 in Feb. 1995
  - New version adopted as ISO/IEC 17799:2001
  - Updated to ISO/IEC 27002:2005.

Structure of ISO/IEC 27002

- ISO/IEC 27002 identifies:
  - 11 high level security objectives with corresponding controls as a basis for Information Security Management.
  - includes 133 controls

"Not all the controls described will be relevant to every situation, nor can they take account of local environmental or technological constraints, or be present in a form that suits every potential user in an organization."

The 11 Objectives of ISO/IEC 27002



ISO/IEC 27002 - IS Policy

Information security policy

- Objective: To provide management direction and support for information security

- *"Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization"*.

ISO/IEC 27002– IS Policy

Information security policy document

- Should be:
  - Approved by management
  - Published and communicated to all employees
- Should state management commitment and set out organisation's approach to managing information security
- Review and evaluation:
  - Policy should have a defined owner responsible for development, review and evaluation according to a defined review process
  - Time schedule for review should be specified

ISO/IEC 27002 - IS Policy

Information security policy document

- At a *minimum*, the document should include:
  a) definition of information security, its overall objectives and scope …
  b) Statement of management intent …
  c) A framework for setting control objectives and controls including risk assessment and risk management
  d) Brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organisation, e.g.
  e) Definition of general and specific responsibilities for information security management including reporting security incidents
  f) References to supporting documentation

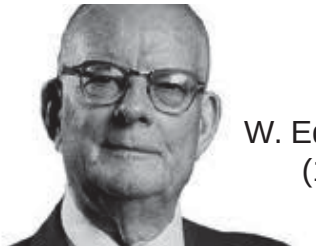
ISO/IEC 27001:2005

Information Security Management Systems – Requirements

- This new international version of the standard clarifies and strengthens some requirements of the original British standard, and includes changes to the following areas:
  - risk assessment,
  - contractual obligations,
  - scope,
  - management decisions,
  - measuring the effectiveness of selected controls.

ISO/IEC 27001- What is it?

- Specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS (Information Security Management System)
- A comprehensive approach to information security management
- Not just a set of goals and controls as in the code of practice ISO/IEC 27002
- Organisations can be certified against ISO/IEC 27001
- To be used in conjunction with ISO/IEC 27002
- Based on Deming's Plan-Do-Check-Act (PDCA) model

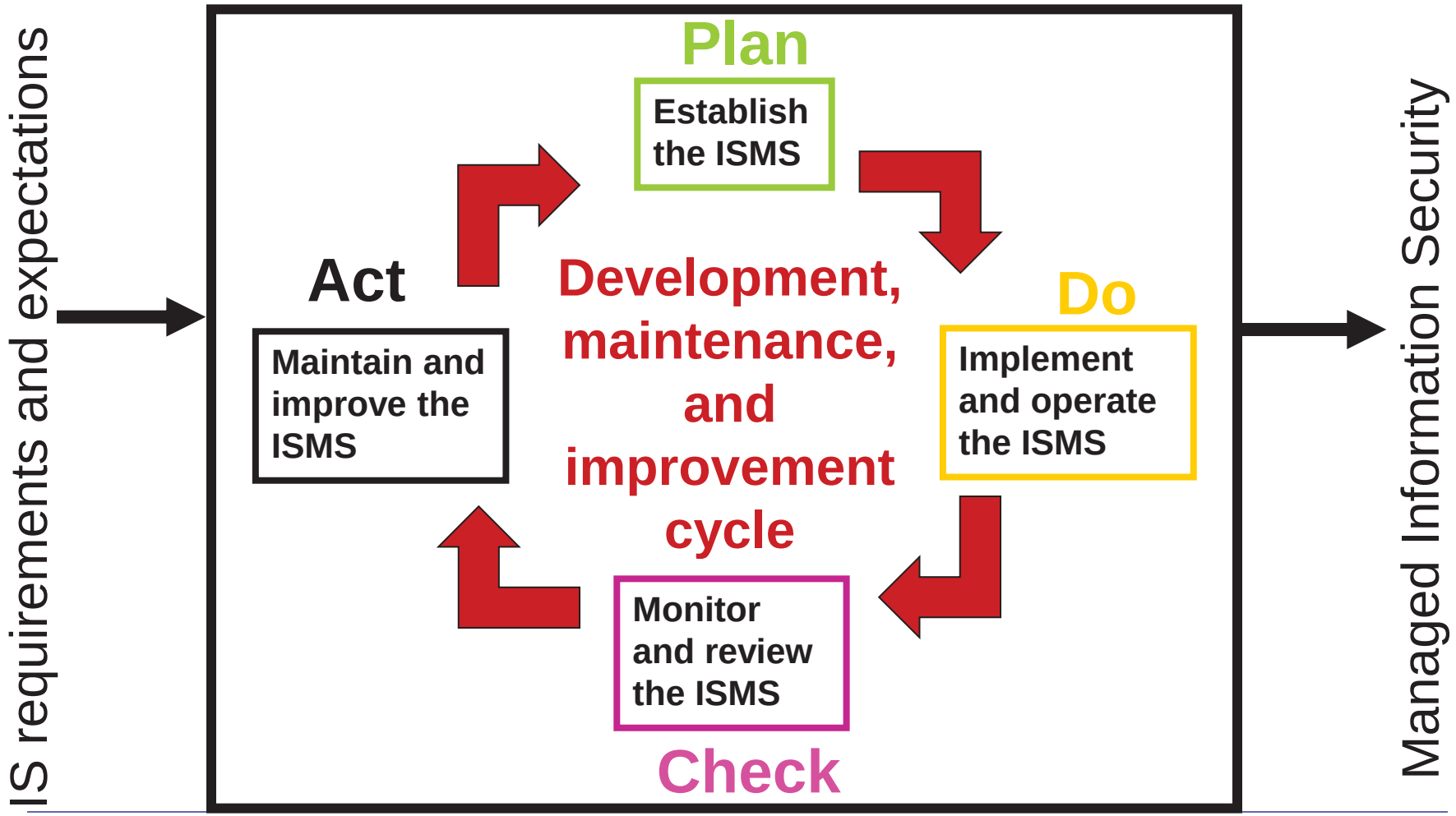


W. Edwards Deming
(1900-1993)

ISO/IEC 27001- History

- The need to establish a certification scheme for information security management emerged late 1990s
- A general approach to security management was needed for certification purposes, not just a code of practice as in BS:7799:1995
- BS 7799 part 2:1999 created to define a comprehensive ISMS (Information Security Management System) against which certification was possible.
- Led to the dramatic conclusion that **the concept of an ISMS is perhaps of far greater and fundamental importance than the original Code of Practice**.

ISO/IEC 27001- The PDCA Model



CISSP & 27001 security program phases

CISSP phases (Harris, Security Program Development, p.68)	ISO 27001 PDCA phases
1. Plan and organise	Plan: Establish ISMS
2. Implement	Do: Implement ISMS
3. Operate and maintain	Do: Operate ISMS
4. Monitor and evaluate	Check: Monitor and review ISMS Act: Maintain and improve ISMS

- Harris defines her own security program cycle
- ISO27001 adopts the Deming circle for quality control
- Synthesis between Harris and ISMS gives 5 phases:
- 1) Plan, 2) Implement, 3) Operate, 4) Review, 5) Improve

ISO/IEC 27001- Plan Phase

- Establish the ISMS
- Purpose: Establish policy, objectives, processes and procedures
- Steps:
  - Define scope and boundaries
  - Define policy for the security program (ISMS)
  - Analyse and identify the greatest risks
  - Identify and evaluate options for the treatment of risks
  - Select control objectives and controls for the treatment of risks
  - Obtain management approval and authorization
  - Prepare a statement of applicability

ISO/IEC 27001- Do phase

- Implement and operate the ISMS
- Purpose: Implement selected controls, and promote actions to manage identified risks
- Steps:
  - Develop blueprints for controls selected in Plan phase
  - Implement the controls selected in the Plan phase
  - Define how to measure the effectiveness of the selected controls
  - Implement training and awareness programs
  - Manage operations and resources

ISO/IEC 27001- Check phase

- Monitor and review the ISMS
- Purpose: to ensure that controls are working effectively
- Steps:
  - Execute monitoring procedures and other controls
  - Measure the effectiveness of controls
  - Review the level of residual risk and acceptable risk
  - Conduct internal ISMS audits at planned intervals
  - Undertake a management review of the ISMS on a regular basis (at least once per year)
  - Record actions and events that could have an impact on the effectiveness or performance of the ISMS.

ISO/IEC 27001- Act phase

- Maintain and improve the ISMS
- Purpose: Take action as a result of the Check phase
- Steps:
  - Implement identified improvements in the ISMS
  - Take appropriate corrective and preventive actions
  - Communicate the results and actions and agree with all interested parties
  - Ensure that the improvements achieve their intended objective

ISO/IEC 27001Output

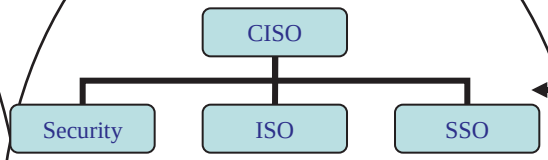
Risk Assessment

ISO 27001

Business Continuity Plan

Security Policy

Policies



Security Organisation

People

Incident Reporting

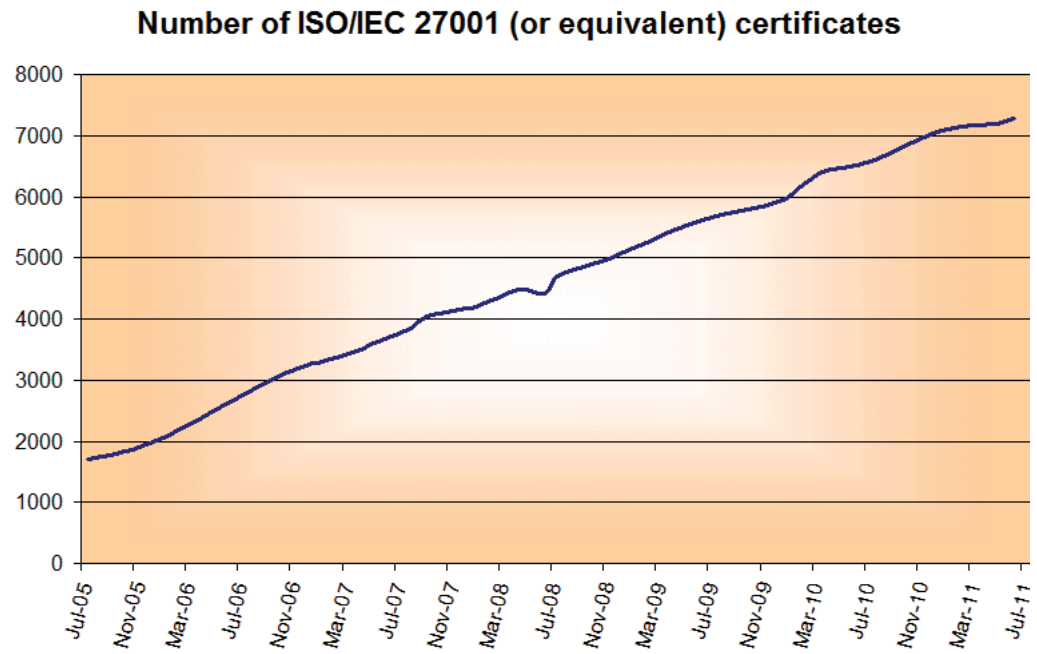
Incident Handling

Disaster Recovery

Procedures

ISO/IEC 27001Certification

- Certification according to ISO27001 is conducted by DNV (Veritas) in Norway
  - http://www.dnv.no/



Source: Ted Humphrey

The Human Factor

- Personnel integrity
  - Making sure personnel do not become attackers
- Personnel as defence
  - Making sure personnel do not fall victim to social engineering attacks

Personnel Integrity

Preventing employees from becoming attackers

- Consider:
  - Employees
  - Executives
  - Customers
  - Visitors
  - Contractors & Consultants
- All these groups obtain some form of access privileges
- How to make sure privileges are not abused?

Personnel Integrity

- A company's existence depends on the integrity of its employees.
- New employees may get access to extremely sensitive and confidential information.
- The new employee's ethical outlook is *a priori* unknown.
- Unauthorized release of sensitive information could destroy reputation or cause financial damage
- An employee, who has just resigned to take up a position with a major competitor, may want to steal important trade secrets.

Strengthening employee integrity

- Difficult to determine long term integrity at hiring
  - Integrity can change, influenced by events
- All personnel must participate in security awareness
- Reminders about security policy and warnings about consequences of intentional breach of policy
  - Will strengthen power of judgment
- Personnel in highly trusted positions must be supported, trained and monitored
- Support and monitor employees in particular situations
    - Conflict, loss or change of job, personal problems
    - Try to stay on good terms with staff leaving the company

Personnel Departure

- Different reasons for departure
  - Voluntary
  - Redundancy
  - Termination
- Different types of actions
  - Former employee may keep some privileges
  - Revoke all privileges
  - Escort to the exit.
- During exit interview, terms of original employment agreement reviewed (i.e. non-compete, wrongful disclosure, etc.

Personnel as Defence: Stopping Social Engineering Attacks

- Social Engineering Basics
  - "Management of human beings according to their place and function in society" (Websters Dictionary)
  - Everybody practices SE
    - Social interactions, politeness, negotiations, diplomacy
  - SE can also be used as part of attacking information systems, then it's called SE attacks.
  - Distinction blurred between SE and SE attacks.

Social Engineering Attacks

- According to Kevin Mitnick:
  - "The biggest threat to the security of a company is not a computer virus, an unpatched hole in a program, or a badly installed firewall. In fact the biggest threat could be you."
  - "What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time, organisations overlook that human element".

From "How to hack people", BBC NewsOnline, 14 Oct 2002

SE Tactics: Develop Trust

- People are naturally helpful and trusting
- Ask during seemingly innocent conversations
- Slowly ask for increasingly important information
- Learn company lingo, names of key personnel, names of servers and applications
- Cause a problem and subsequently offer your help to fix it (aka. reverse social engineering)
- Talk negatively about common enemy
- Talk positively about common hero
- Get introduced by trusted person

SE Tactics: Induce strong affect

- Heightened emotional state makes victim
  - Less alert
  - Less likely to analyse deceptive arguments
- Triggered by attacker by creating
  - Excitement (“you have won a price”)
  - Fear (“you will loose your job”)
  - Confusion (contradictory statements)

SE Tactics: Information overload

- Reduced the target's ability to scrutinize arguments proposed by the attacker
- Triggered by
  - Providing large amounts of information to produce sensory overload
  - Providing arguments from an unexpected angle, which forces the victim to analyse the situation from new perspective, which requires additional mental processing
  - Subliminal messages, e.g. "tell me, how can I get a new password ?". The words "tell me" is a subliminal order to the victim to provide new password.

SE Tactics: Reciprocation

- Exploits our tendency to return a favour
  - Even if the first favour was not requested
  - Even if the return favour is more valuable
- Double disagreement
  - If the attacker creates a double disagreement, and gives in on one, the victim will have a tendency to give in on the other
- Expectation
  - If the victim is requested to give the first favour, he will believe that the attacker becomes a future ally

SE Tactics:
Diffusion of responsibility and moral duty

- Make the target feel the he or she will not be held responsible for actions
- Make the target feel that satisfying attacker's request is a moral duty
- Create situations where target feels obliged to help

SE Tactics: Authority

- People are conditioned to obey authority
  - Milgram and other experiments
  - Considered rude to even challenge the veracity of authority claim
- Triggered by
  - Faking credentials
  - Faking to be a director or superior
  - Skilful acting (con artist)

SE Tactics: Commitment creep

- People have a tendency to follow commitments, even when recognising that it might be unwise.
- It's often a matter of showing personal consistency and integrity
- Triggered e.g. by creating a situation where one commitment naturally or logically follows another.
  - First request is harmless
  - Second request causes the damage

Multi-Level Defence against Social Engineering Attacks

Source: David Gragg: http://www.sans.org/rr/whitepapers/engineering/

PHYSICAL SECURITY

- **Natural Physical Security**
- **Physical Access Control**
- **Environmental Security**

Threats to Physical Security

- Unintentional acts
  - acts of human error or failure,
  - deviations in quality of service,
- Deliberate acts
  - espionage or trespass,
  - theft and compromises to intellectual property
- Forces of nature
- Technical failures
  - technical hardware & equipment failures or errors
  - technical software failures or errors
- Management failures
  - technical obsolescence.

Natural Physical Security

Crime Prevention Through Environmental Design (CPTED)

- *CPTED is the proper design and effective use of the built environment which may lead to a reduction in the fear and incidence of crime, and an improvement of the quality of life."* –

  US National Crime Prevention Institute

CPTED Strategies

- Natural Surveillance
- Natural Access Control
- Territorial Reinforcement
- Activity Support

CPTED Natural Surveillance

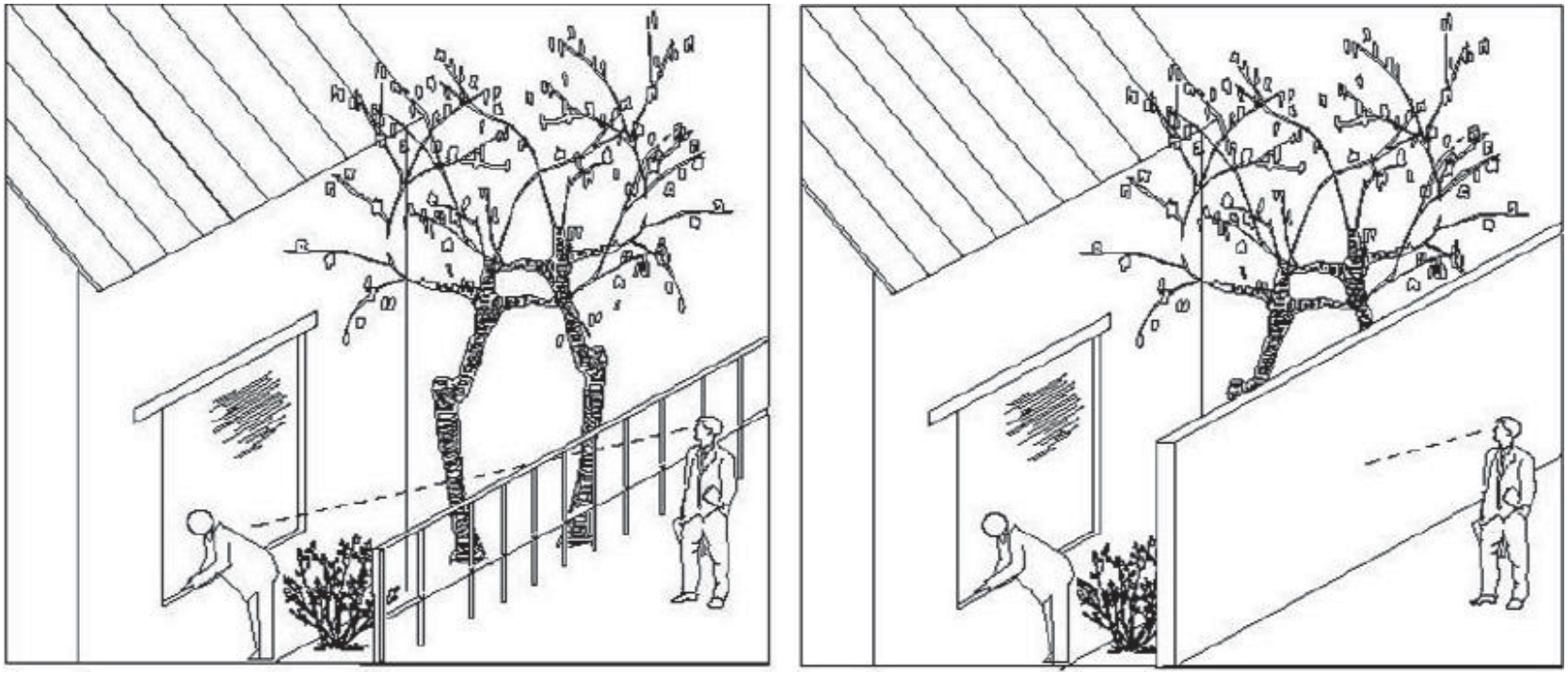
- A design concept directed primarily at keeping intruders easily observable. Promoted by features that maximize visibility of people, parking areas and building entrances: doors and windows that look out on to streets and parking areas; pedestrian-friendly sidewalks and streets; front porches; adequate night time lighting.

CPTED Natural Surveillance

This stairwell design providing access to a parking garage creates opportunities for surveillance as well as creating the opportunity to be heard if assistance is needed.

CPTED Natural Surveillance

- **Permeable fencing allows surveillance**



CPTED Natural Access Control

- A design concept directed primarily at decreasing crime opportunity by denying access to crime targets and creating in offenders a perception of risk. Gained by designing streets, sidewalks, building entrances and neighbourhood gateways to clearly indicate public routes and discouraging access to private areas with structural elements.

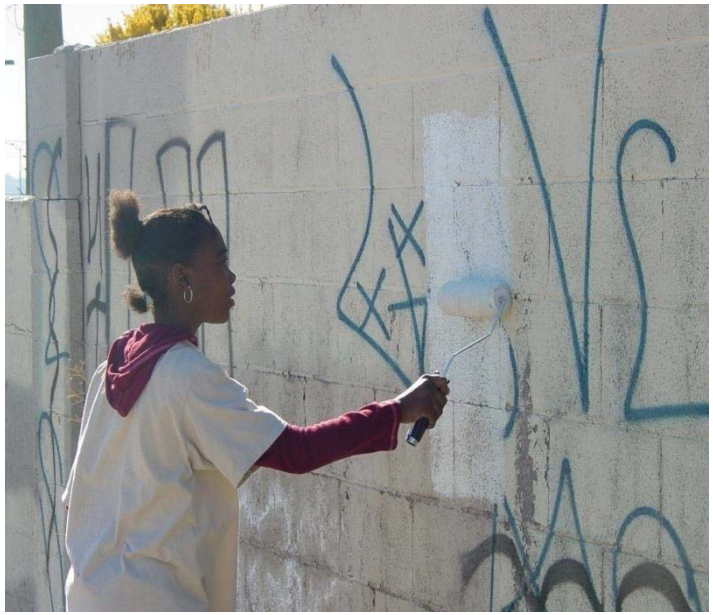
CPTED Natural Access Control

The bollard lights placed at the entrance to this office building provide Natural Access Control because they guide you toward the building's entrance. There are no signs to indicate the building's entrance, but the combination of a walkway, landscaping, and bollard lights forces visitors to follow the path to the entrance.

CPTED Territorial Reinforcement

- Physical design can create or extend a sphere of influence. Users then develop a sense of territorial control while potential offenders, perceiving this control, are discouraged. Promoted by features that define property lines and distinguish private spaces from public spaces using landscape plantings, pavement designs, gateway treatments, and "CPTED" fences.

CPTED Territorial Reinforcement



Painting over graffiti immediately sends a message that the area is cared for and will be well maintained.

This shop front clearly defines the barrier from the public area to the office building.

CPTED Activity Support

- Planned activities for the areas that need to be protected. Designed to get people to work together to increase the overall awareness of acceptable and unacceptable activities in the area.
  - E.g.
    - Sport courts in parks attract healthy activity
    - Company BBQ parties on company grounds

CPTED Activity Support

This company BBQ gives staff and neighbours the perception that the area is being actively used and cared for, which discourages trespassing and littering.

Physical Access Control through Target hardening

Physical access control through target hardening is a process wherein a building is made into a more difficult or less attractive target. It does not necessarily mean the construction of an impenetrable bunker, although this would be the extreme case of target hardening.

Physical Access Controls

- Walls, Fencing, and Gates
- Guards
- Dogs, ID Cards, and Badges
- Locks and Keys
- Mantraps
- Electronic Monitoring
- Alarms and Alarm Systems
- Computer Rooms
- Walls and Doors

- *To ensure that no unauthorized person can get physical access to facilities and systems, or damage and steal equipment.*

Multilayered Physical AC

- Defence in depth
  - Requires that the organisation establish multiple layers of controls
  - Attackers will have to penetrate many protection layers in order to access sensitive information and systems
  - Slows down, and makes successful attacks much harder

Defence in Depth

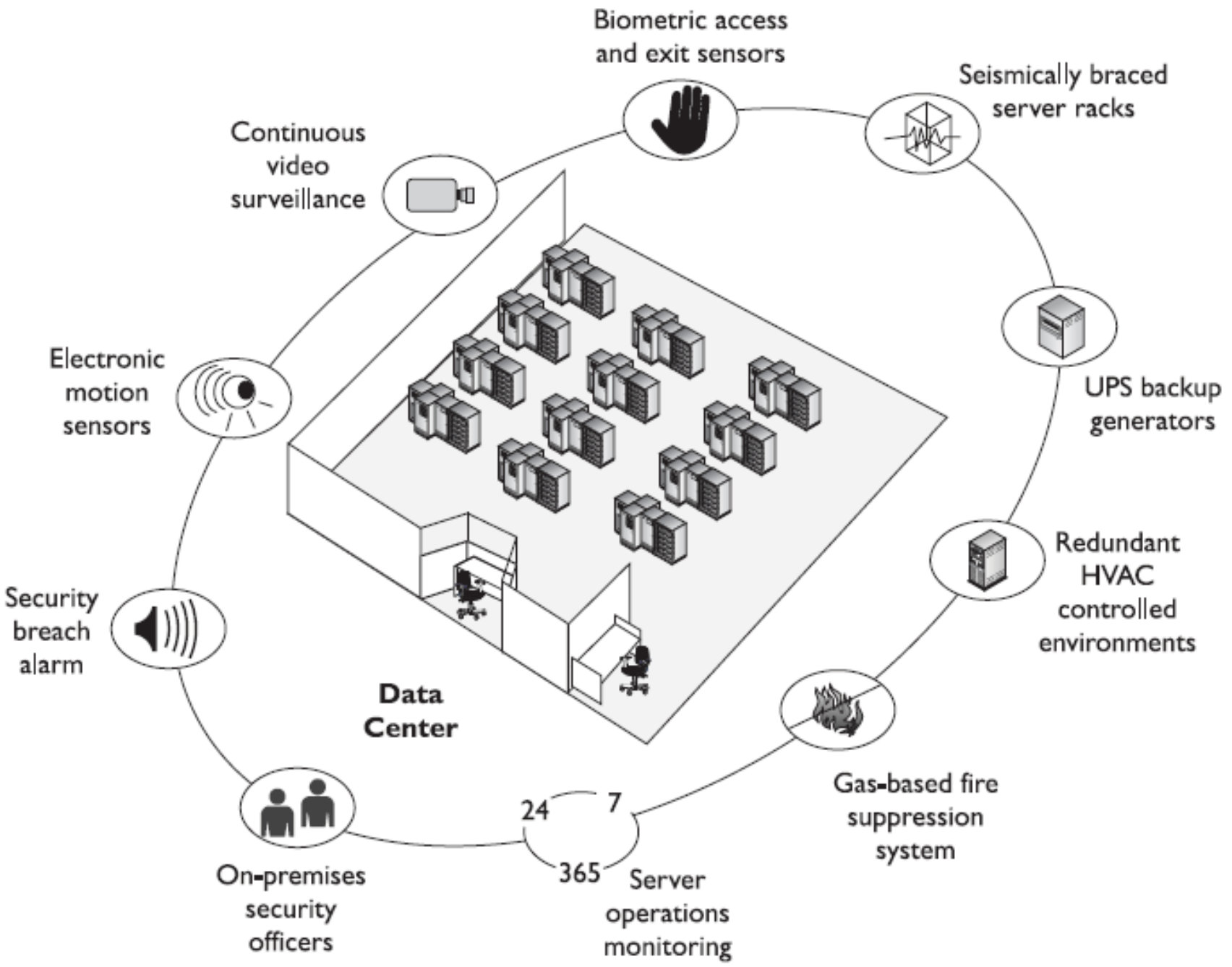


Figure 6-5 A data center should have many physical security controls.

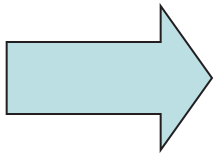
Electronic Monitoring

- Records events where other types of physical controls are not practical
- May use cameras with video recorders
- Drawbacks:
  - reactive and do not prevent access or prohibited activity
  - recordings often not monitored in real time and must be reviewed to have any value
  - Human security guards tire quickly and will no longer react to events recorded by video surveillance

Automated video surveillance

Suspicious events are rare

Attention from the guard is needed for very few occasions



Limited human participation

The guard is “replaced” by vision algorithms

Automated Video Surveillance

- Large scale video surveillance systems deployed on top of IP-network
- System of scattered low cost video sensors
  - Focus on the design of computer vision algorithms
  - PC is attached to each video source
  - Stream full quality video or just images
- Alarms triggered by vision systems to get human attention to suspicious events.

Remote Computing Security

- Remote site computing - distant from the organizational facility
- Telecommuting - computing using telecommunications including Internet, dial-up, or leased point-to-point links
- Employees may need to access networks on business trips
- Telecommuters need access from home systems or satellite offices
- To provide a secure extension of the organization's internal networks, all external connections and systems must be secured

Environmental Security

- Good physical security should protect resources against accidental damage and forces of nature,

  as well as deliberate acts, so include protection against
  - Fire & Smoke
  - Water damage
  - Power failure,
  - Structural collapse

Fire Safety

- The most serious threat to the safety of the people who work in the organization is the possibility of fire
- Fires account for more property damage, personal injury, and death than any other threat
- It is imperative that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards

Heating, Ventilation, and Air Conditioning

HVAC areas that can cause damage to IT systems:

- Temperature
  - Optimal temperature for IT equipment (and people) is 20-24°C
- Dust
  - Can obstruct cooling, can cause device malfunctioning
- Humidity
  - Optimal humidity for IT equipment is 40%-55%
- Static
  - One of the leading causes of damage to sensitive circuitry is electrostatic discharge (ESD)
  - A person can generate up to 12,000 volts of static current by walking across a carpet
  - Often caused by low air humidity

Power Management and Conditioning

- Electrical quantity (voltage level and amperage rating) and quality (cleanliness and proper installation) of the power are important
- Any noise that interferes with the normal 50 Hertz (or 60 Hertz) cycle can result in inaccurate time clocks or unreliable internal clocks inside the CPU
- Grounding
  - Grounding ensures that the returning flow of current is properly discharged
  - If not properly installed could cause damage to equipment and injury or death to the person
- Overloading a circuit not only causes problems with the circuit tripping but can also overload the power load on an electrical cable, creating the risk of fire

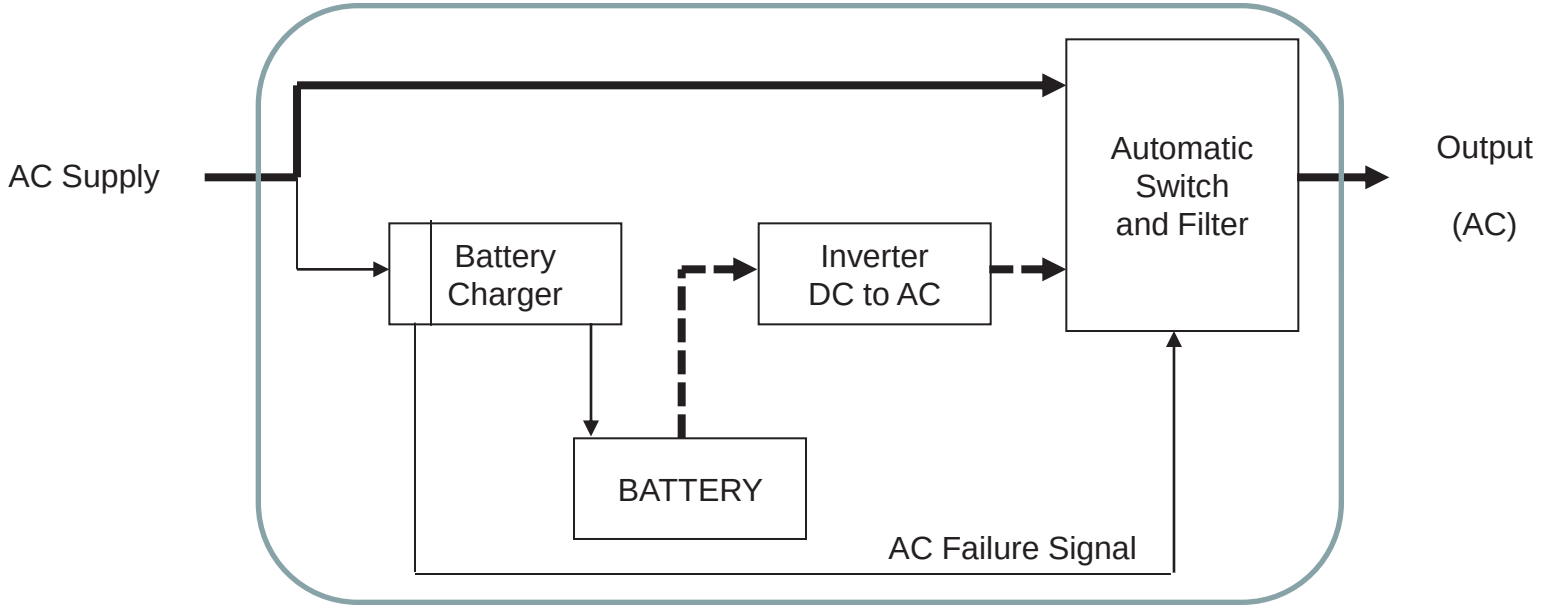
Electrical Terms

- **Fault:** momentary interruption in power
- **Blackout:** prolonged interruption in power
- **Sag:** momentary drop in power voltage levels
- **Brownout:** prolonged drop in power voltage levels
- **Spike:** momentary increase in power voltage levels
- **Surge:** prolonged increase in power voltage levels

Uninterruptible Power Supplies (UPSs)

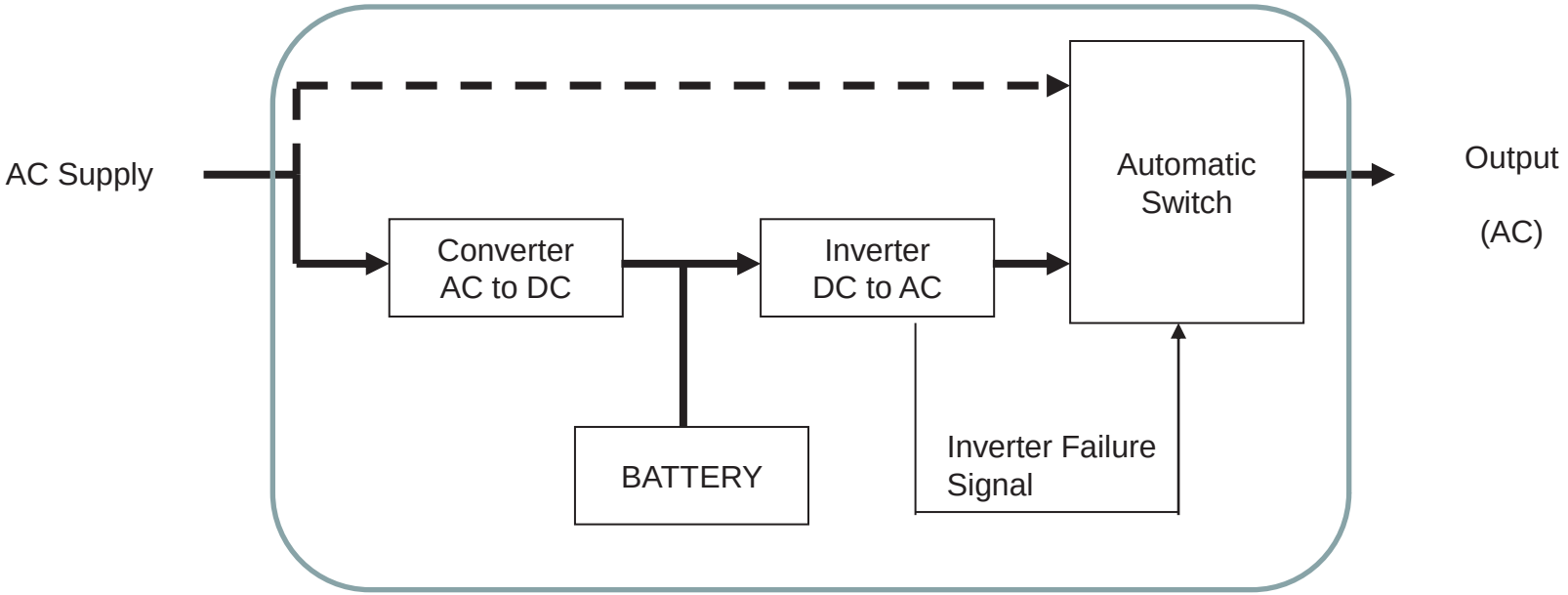
- In case of power outage, a UPS is a backup power source for major computer systems
- There are four basic configurations of UPS:
  - **Standby:** battery or generator, causes short interruption
  - **Ferro-resonant standby:** softens interruption using magnetic filter
  - **Line-interactive:** minimal interruption
  - **True online:** no interruption
- AC: Alternate Current, provided by power company
  - 220V, 50Hz (Europe) or 110V, 60Hz (US)
  - Local diesel generators can replace power company i.c.o. blackout
- DC: Direct Current, provided by battery or power supply

Line-Interactive UPS



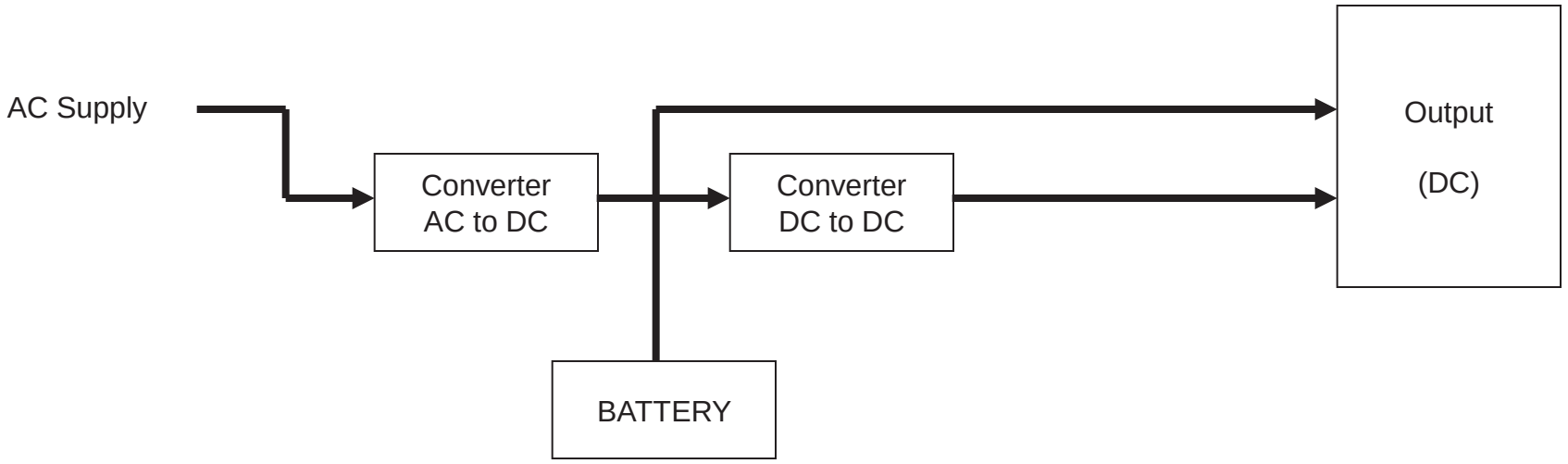
- AC power normally bypasses the battery and inverter
- Power is taken from battery in case AC supply fails

True On-line UPS



- Normal power supply always goes through converter, battery and inverter
- AC can bypass battery and inverter in case of failure

Laptop Computer Power Supply



- Power always goes through converter and battery
- DC levels other than that provided by the battery can be provided by DC-to-DC converter.

End of lecture

- We have looked at:
  - IS Management
  - Personnel security
  - Physical Security