Exaples of threats

Type	Threats
Physical damage	Fire Water damage Pollution Major accident Destruction of equipment or media Dust, corrosion, freezing
Natural events	Climatic phenomenon Seismic phenomenon Volcanic phenomenon Meteorological phenomenon Flood
Loss of essential services	Failure of air-conditioning or water supply system Loss of power supply Failure of telecommunication equipment
Disturbance due to radiation	Electromagnetic radiation Thermal radiation Electromagnetic pulses
Compromise of information	Interception of compromising interference signals Remote spying Eavesdropping Theft of media or documents Theft of equipment Retrieval of recycled or discarded media Disclosure Data from untrustworthy sources Tampering with hardware Tampering with software Position detection
Technical failures	Equipment failure Equipment malfunction Saturation of the information system Software malfunction Breach of information system maintainability
Unauthorised actions	Unauthorised use of equipment Fraudulent copying of software Use of counterfeit or copied software Corruption of data Illegal processing of data
Compromise of functions	Error in use Abuse of rights Forging of rights Denial of actions Breach of personnel availability
Hacker, cracker (challenge, ego, rebellion, status, money)	Hacking Social engineering System intrusion, break-ins

	Unauthorized system access
Computer criminal (destruction of information, illegal information disclosure, monetary gain, unauthorized data alteration)	Computer crime (e.g. cyber stalking) Fraudulent act (e.g. replay, impersonation, interception) Information bribery Spoofing System intrusion
Terrorist (blackmail, destruction, exploitation revenge, political gain, media coverage)	Bomb/Terrorism Information warfare System attack (e.g. distributed denial of service) System penetration System tampering
Industrial espionage (competitive advantage, economic espionage)	Defence advantage Political advantage Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorized system access (Access to classified, proprietary, and/or technology-related information)
Insiders (curiosity, ego, intelligence, monetary gain, revenge, unintentional errors and omissions (e.g. data entry error, programming error))	Assault on an employee Blackmail Browsing of proprietary information Computer abuse Fraud and theft Information bribery Input of falsified, corrupted data Interception Malicious code (e.g. virus, logic bomb, Trojan horse) Sale of personal information System bugs System intrusion System sabotage Unauthorized system access

Examples of vulnerabilities

Type	Vulnerability
Hardware	Insufficient maintenance/faulty installation of storage media Lack of periodic replacement schemes Susceptibility to humidity, dust, soiling Sensitivity to electromagnetic radiation Lack of efficient configuration change control Susceptibility to voltage variations Susceptibility to temperature variations Unprotected storage Lack of care at disposal Uncontrolled copying
Software	No or insufficient software testing Well-known flaws in the software No 'logout' when leaving the workstation Disposal or reuse of storage media without proper erasure Lack of audit trail Wrong allocation of access rights Widely-distributed software Applying application programs to the wrong data in terms of time Complicated user interface Lack of documentation Incorrect parameter set up Incorrect dates Lack of identification and authentication mechanisms like user authentication Unprotected password tables Poor password management Unnecessary services enabled Immature or new software Unclear or incomplete specifications for developers Lack of effective change control Uncontrolled downloading and use of software Lack of back-up copies Lack of physical protection of the building, doors and windows Failure to produce management reports
Network	Lack of proof of sending or receiving a message Unprotected communication lines Unprotected sensitive traffic Poor joint cabling Single point of failure Lack of identification and authentication of sender and receiver Insecure network architecture Transfer of passwords in clear Inadequate network management (resilience of routing) Unprotected public network connections
Personnel	Absence of personnel Inadequate recruitment procedures

	Insufficient security training Incorrect use of software and hardware Lack of security awareness Lack of monitoring mechanisms Unsupervised work by outside or cleaning staff Lack of policies for the correct use of telecommunications media and messaging
Site	Inadequate or careless use of physical access control to buildings and rooms Location in an area susceptible to flood Unstable power grid Lack of physical protection of the building, doors and windows
Organization	Lack of formal procedure for user registration and de-registration Lack of formal process for access right review (supervision) Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties Lack of procedure of monitoring of information processing facilities Lack of regular audits (supervision) Lack of procedures of risk identification and assessment Lack of fault reports recorded in administrator and operator logs Inadequate service maintenance response Lack or insufficient Service Level Agreement Lack of change control procedure Lack of formal procedure for ISMS documentation control Lack of formal procedure for ISMS record supervision Lack of formal process for authorization of public available information Lack of proper allocation of information security responsibilities Lack of continuity plans Lack of e-mail usage policy Lack of procedures for introducing software into operational systems Lack of records in administrator and operator logs Lack of procedures for classified information handling Lack of information security responsibilities in job descriptions Lack or insufficient provisions (concerning information security) in contracts with employees Lack of defined disciplinary process in case of information security incident Lack of formal policy on mobile computer usage Lack of control of off-premise assets Lack or insufficient 'clear desk and clear screen' policy Lack of information processing facilities authorization Lack of established monitooring mechanisms for security breaches Lack of regular management reviews Lack of procedures for reporting security weaknesses Lack of procedures of provisions compliance with intellectual rights