# ENTERPRISE INFORMATION SYSTEMS

- Security in information systems

# Security in information systems

Literature:

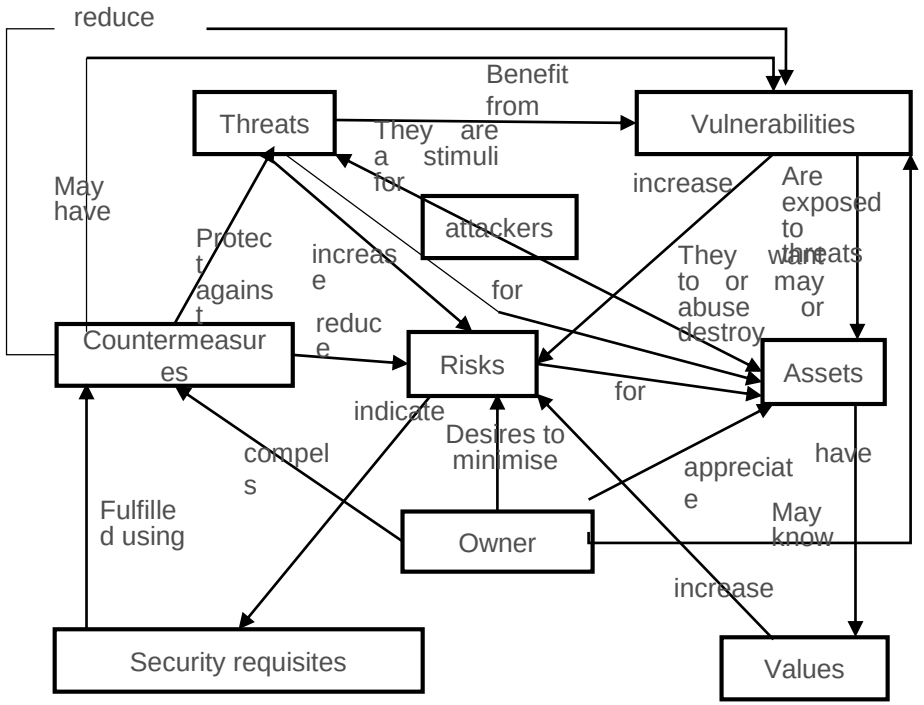

- GÁLA, Libor, Jan POUR and Zuzana ŠEDIVÁ. Business informatics. 2nd edition (segments 42 and 43) 2. Prague: Grada, 2009. ISBN 978-80-247-2615-1. Pages 331 - 352.
- TVRDÍKOVÁ, Milena. Application of information technologies in corporate management: tools for improvement of the quality of the information systems. In *Management in the information society*. 1st Ed. Prague: Grada, 2008. ISBN 978-80-247-2728-8. Pages 155 - 166.

# Security in information systems

**IS/ICT security** is an IS/ICT property whose level is impacted by all the aspects, which are related to the definition, achievement and maintenance of a suitable level of security requirements (confidentiality, integrity, availability, individual responsibility, authenticity and reliability) that respects the culture and sector in which the IS/ICT is operated. Gála 2009.

# Security in information systems

**Security terminology**




**Source: Gála, p. 332**

# Security in information systems

## IS vulnerabilities

### Vulnerability

Physical - the IS/ICT element is physically located in an environment in which it can easily be damaged, destroyed or lost;

Natural - the IS/ICT element is endangered, for instance, by floods, fire, lightning

Technological - the IS/ICT element does not allow, for instance, permanent smooth operation

Physical - the IS/ICT element works along such principles, which allow its abuse - for instance, electromagnetic radiation of the communication networks

Human - the IS/ICT element is endangered by the action of people, their mistakes and ignorance

# Security in information systems

Attackers - people who make intentional attacks:

Hacker - considers the attack as a challenge and a resource to get prestige

Spy - makes attacks in order to get information

Terrorist - makes attacks in order to cause apprehension and fear

Criminal - attacks the systems for own financial gain

# Security in information systems

Attackers - people who make intentional attacks:

Vandal - attacks the systems with the objective to destroy or damage them

Cracker - usually a programmer who makes an effort to penetrate into foreign systems for the purpose of stealing information

Phreaker - his objective is to get telecommunication information and allow access to other computers.

Phracker - his objective it to get free access to telephone services

# Security in information systems

**The security policy** is a set of principles and rules that the organisation uses to protect its assets. The security policy is continuously updated in accordance with changes in the environment and may include:

- The policy of permissible use of assets
- Specification of the educational process in the field of security
- Clarification of the mode of implementation and enforcement of security measures
- A procedure for evaluation of the effectiveness of a policy leading to the implementation of its change

# Security in information systems

**Security policy:**

- Promiscuous - does not restrict anybody and allows the subjects to do everything, including what they should not do
- Liberal - allows everything, excluding the exceptions that are explicitly stated
- Cautious - forbids everything except what is explicitly permitted
- Paranoid - forbids doing anything that is potentially dangerous, and therefore also anything that need not be explicitly prohibited

# Security in information systems

**Risk Management (RM)**

Hazard Analysis:

- Definition of the scope - review of assets (equipment, networks…), plan (accreditation, evaluation of conformity….) and methodology (list, testing of breaches….)
- Specification of the environment - characterisation of the operating environment in connection with data sensitivity
- Identification of assets - description of system assets including the logical and operating aspects
- Identification of counter-measures - identification of existing security and counter-measure options
- Identification of vulnerability and threats - identification of physical, administrative, technical and operational threats
- Analysis of vulnerability - scenarios for each threat and evaluation of vulnerability
- Determination of risks and consequences - determination of the probability of the risks and their classification according to significance

# Security in information systems

**Risk Management (RM)**

Cost-benefit analysis - allows comparison of the costs of countermeasures with the estimated loss if the countermeasures were not implemented. When determining the value of the countermeasures, we include the investment, implementation, operation and maintenance as well as other direct and indirect costs.

Selection and implementation of countermeasures - includes the creation of suitable countermeasures including the compilation of their documentation, operating guidelines of the organisation.

# Security in information systems

**Risk Management (RM)**

Testing and evaluation - means the periodical testing and evaluation of the effectiveness of the countermeasure in order to be able to restart the management process in a case where the selected countermeasure becomes ineffective.

Planning of exceptional situations - means the building of a plan of potential emergency situations and emergency responses or alternative operation, including planning of post-accident operations. The objective of the plan is to specify prevention of damage and securing the reinstatement and continuity of operations.

# Security in information systems

**Audit procedure:**

- Detection - is an ascertained event that is related to IS/ICT security
- Resolution - determines whether it is necessary to record the event in the security audit record or directly trigger a security alarm
- Processing of a security alarm - a security alarm is triggered or a security audit message is issued

# Security in information systems

**Audit procedure:**

- Analysis - assessment of an event in the context of earlier ascertained messages
- Aggregation - distributed records of partial security audit records are merged into a single security audit record
- Generation of a report - audit reports are generated from the security audit records
- Archiving - parts of the security audit are stored in the archive

# Security in information systems

Certification - process of comprehensive technical and non-technical evaluation of information system security

Accreditation - formal acknowledgement that the information system is secure and fulfils the conditions required for such a system

Definition and assertion of roles:

- Corporate IS/ICT security council
- Security manager of the organisation
- Unit security manager
- IS security administrator
- Security auditor

# Security in information systems

Threats:

- Natural and physical - disasters, accidents, failures in the electric power supply
- Technical - data carrier and computer failures
- Technological - disorders caused by software - viruses, Trojans
- Human
  - Intentional - hackers, terrorists, spies
  - Unintentional - ignorance, errors, negligence

# Security in information systems

## Countermeasures

| Classification aspect | | Example of a countermeasure |
|---|---|---|
| Preventive | Administrative | • User education and training<br>• Definition of the data archiving policy. |
| | Physical | • Computers, mainly servers, are kept in locked rooms<br>• The security staff control the access of unauthorised persons |
| | Technological | • Confidential data is encrypted<br>• Access passwords are changed at regular intervals. |
| Dynamic | Administrative | • Guidelines exist for user behaviour during registration of incidents |
| | Physical | • The tracking systems automatically monitor the respective rooms.<br>• A generator or UPS (Uninterruptible Power Supply) will ensure the power supply. |
| | Technological | • An attempt to get unauthorised access will result in automatic blocking of the account.<br>• The tracking systems automatically monitor the work of the system and immediately notify the administrator of any deviations.<br>• The system automatically shuts down its endangered parts. |
| Follow-up | Administrative | • Defined mechanisms for return of the system to normal exist |
| | Physical | • A substitute technical component of the system that was destroyed after the attack exists (e.g. substitute keyboard, substitute power supply, etc.). |
| | Technological | • Data and software backups exist including configurations. |

Source: Gála, p. 34

# Security in information systems

**Authentication:**

It is a technique used to verify the proclaimed identity of any subject with the target to convince the counter-party of own identity and ensure protection against its falsification.

Authentication of an entity - we verify that the entity (person or computer system) is really what it claims to be

Authentication of a message - used to verify that the given subject is the originator of the message, which was created at a certain moment in the past

# Security in information systems

**EIS data backup:**

Backup may be done in the following two basic modes:

- On-line - Backup creation process in normal operating conditions.
- Off-line - Backup is done outside normal operating hours, usually by implementation of a special medium

# Security in information systems

**EIS data backup:**

- Unstructured - CD, DVD, not popular among companies
- Full + incremental - backup of all data. Subsequently, only backup of files that have changed since the last time is done. The disadvantage is that I must have the first full backup and all incremental backups available
- Full + differential - full backup of all data + all files that have changed since the last full backup
- Full backup

# Security in information systems

**Backup media:**

- Magnetic tape
- Fixed disk
- NAS - Network Attached Storage - connected to the local area network
- Optical disk
- Others - USB flashdisk

# Security in information systems

Specific EIS functions in the area of security:

- Creation of users - possible authentication by domain or directly by EIS
- Creation of user groups - to which rights are subsequently assigned in terms of system function
- Creation of data owners
- Creation of the data owner group - data ownership within the framework of the table or transactions
- Roles - combination of both preceding principles
- Access rights matrix - every button, menu has its own identification number, which can be assigned to a group of users