TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

IV

Practical info

01.09.15
08.09.15
15.09.15
22.09.15
~~29.09.15~~
06.10.15
13.10.15
20.10.15
~~27.10.15~~
03.11.15
~~10.11.15~~
17.11.15
24.11.15
01.12.15
08.12.15
15.12.15

Practical info

ITX8043

Foundations and Management of Cyber Security

vs.

ITX8090

Information and Cyber Security Assurance in Organisations

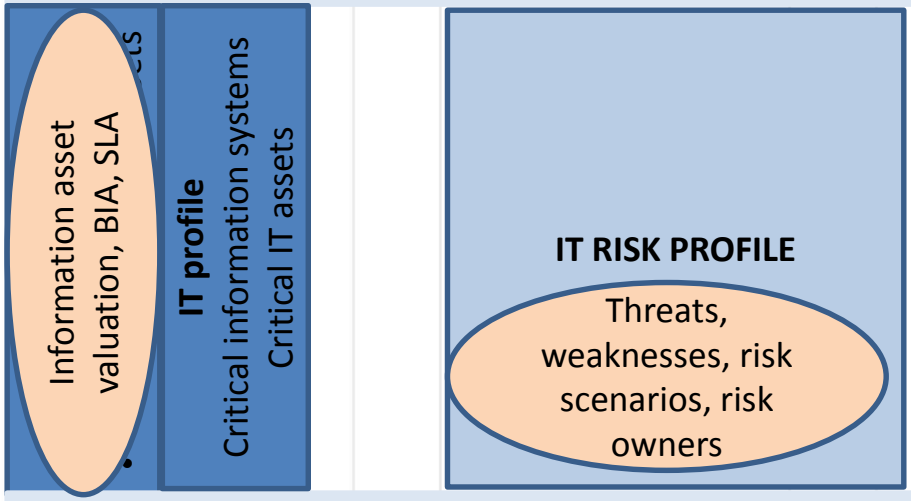
Practical info

Course page

https://courses.cs.ttu.ee/pages/ITX8090

Concept progress

Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.



IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc …)

Definitions (threat)

ISO 27005

A potential cause of an incident, that may result in harm of systems and organization

NIST

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

Definitions (threat)

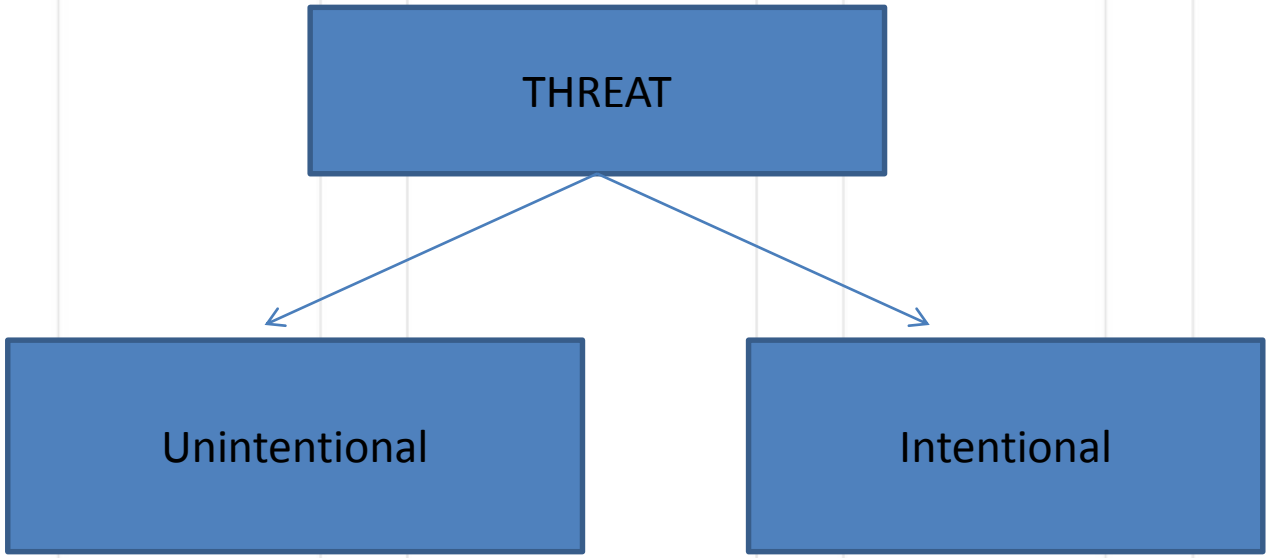
National Information Assurance Glossary

Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

ENISA gives a similar definition

Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Threats



Threats

Unintentional (elemental)

- Environmental - lightning, flood, too low or high temperatures, fire and the like;
- Technical faults - a power failure, computer failure and the like;
- Human threats - errors, mistakes, illness, exits and the like;

One threat can lead to another, such as lightning - > computer failure, flood - > power failure.

Threats

Intentional (attacks)

- Physical attacks;
- Misuse of resources;
- Resource blocking;
- Information fishing;
- Data forgery;
- Manipulation with systems;
- …

Definitions (vulnerability)

ISO 27005

A weakness of an asset or group of assets that can be exploited by one or more threats where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission

National Information Assurance Glossary

Vulnerability — Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited

Definitions (vulnerability)

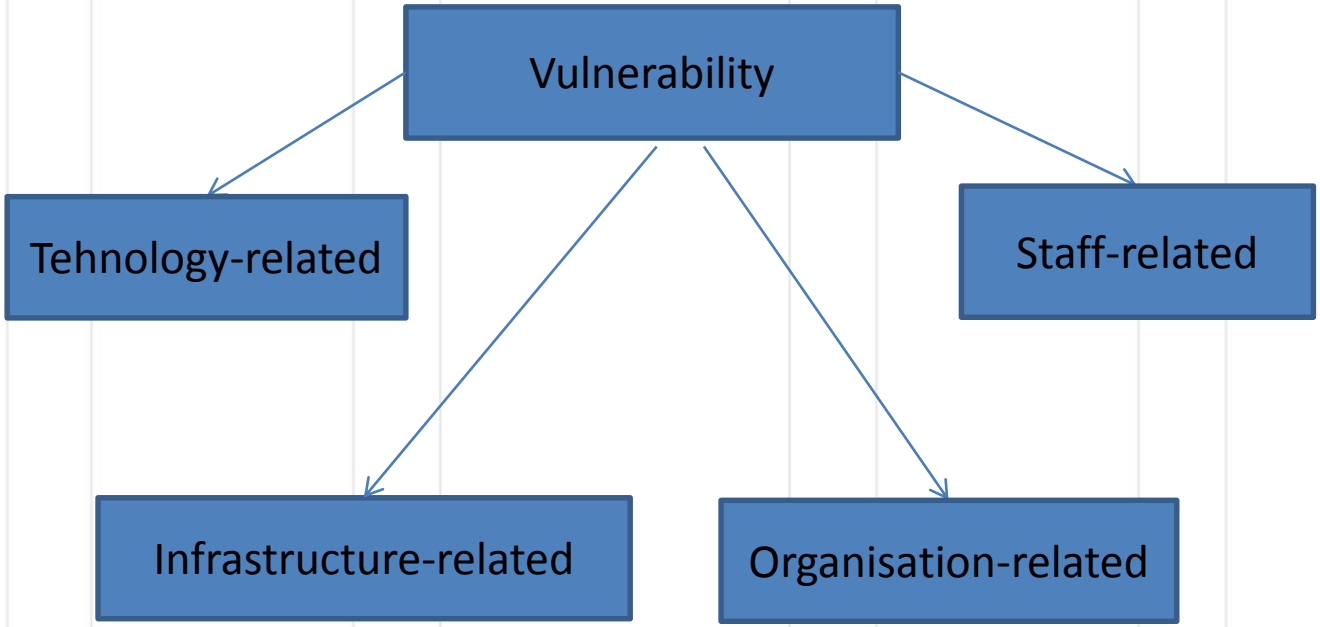
NIST

A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

ENISA

The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

Vulnerability



Vulnerability

Technology-related

- Obsolete technology, „legacy“;
- Improper placement;
- Errors in programs, operating systems;
- Weaknesses in technology management;
- ...

Vulnerability

Infrastructure-related

- Unfavorable location;
- Natural conditions;
- Decaying infrastructure;
- Communication system installation deficiencies;
- Malicious neighbor;
- ...

Vulnerability

Staff-related

Lack of experience;

Excessive trust;

Incorrect procedures;

Ignorance and low motivation level;

Failure to comply with security requirements;

Self-interest;

...

Vulnerability

Organisation-related

- Lack of security organisation;
- Shortcomings in the organisation of work;
- Resource management deficiencies;
- Documenting drawbacks;
- Deficiencies in selection of security measures;
- Deficiencies in control of security measures;
- ...

Listing sources

Internal possibilities

- Predefined forms;
- Interviews;
- Questionnaires;
- Debates;
- Analysis of the documents;
- Observations;
- Incidents occurred;
- Audit reports.

External possibilities

- Standards;
- Statistics;
- How is the in other similar businesses?
- How is the country as a whole?
- How is Europe?
- What are the trends in the world?
- Agencies.

Pairing (NIST)

Table 3-2. Vulnerability/Threat Pairs

Vulnerability	Threat-Source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

Risk scenario

Component	Description
Participant	Internal (employee, temporary employee) External (competitor, external business partner, regulator, market operator)
Threat	Malicious Accidental Malfunction Natural error External requirement
Event	Disclosure Disruption Modification Theft

Risk scenario

Component	Description
Event	Destruction Structure change Ineffective Use Regulations violation Misuse
Information asset/IT asset	Organisation Processes Infrastructure IT infrastructure Information Applications
Time	Time period The critical/non- critical time Detection speed

Advising questions

1. Asset - **what** should be protected?
2. Threat - **who** or **what** uses the advantage of the weakness?
3. Weakness - **why** is asset vulnerable?
4. Risk - **what** may happen if weakness exploited and **how** likely is it?

Practice

Exercise V

PhD Andro Kull
CISA, CISM, CRISC, ABCP
E-mail: Andro@consultit.ee
Skype: andro.kull