Funded by the Erasmus+ Programme of the European Union

Overview of Understanding and Handling Cyber-Attacks

Basic Knowledge on e-Security

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CyberPhish
Safeguarding your digital future

Learning Goals

Explain the concept of e-security and the importance of adopting a proactive approach to cyber threats through the concept of cyber hygiene

Funded by the Erasmus+ Programme of the European Union

Student Workload

Lecture	0,5 h
Audio and video material	0,5 h
Case studies	0,5 h
Further reading	1 h
Preparation for exam	0,5 h

Funded by the Erasmus+ Programme of the European Union

Contents

Information contents and its security need

Intellectual property; personal data; identity

How does malicious software get into device?

What are reasons and consequences of identity thefts and personal data disclosure?

CyberPhish
Safeguarding your digital future

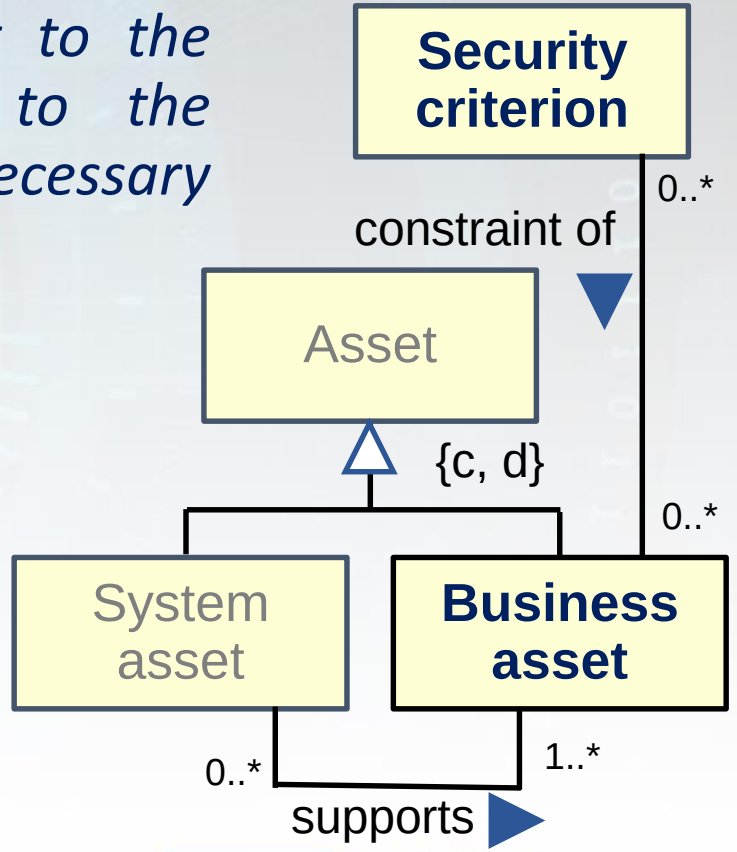
Funded by the Erasmus+ Programme of the European Union

Business Asset and Security Criterion

Open information *versus* **Private information**

- **Business asset:** *information, process, skill inherent to the business of the organisation that has value to the organisation in terms of its business model and is necessary for achieving its objectives*

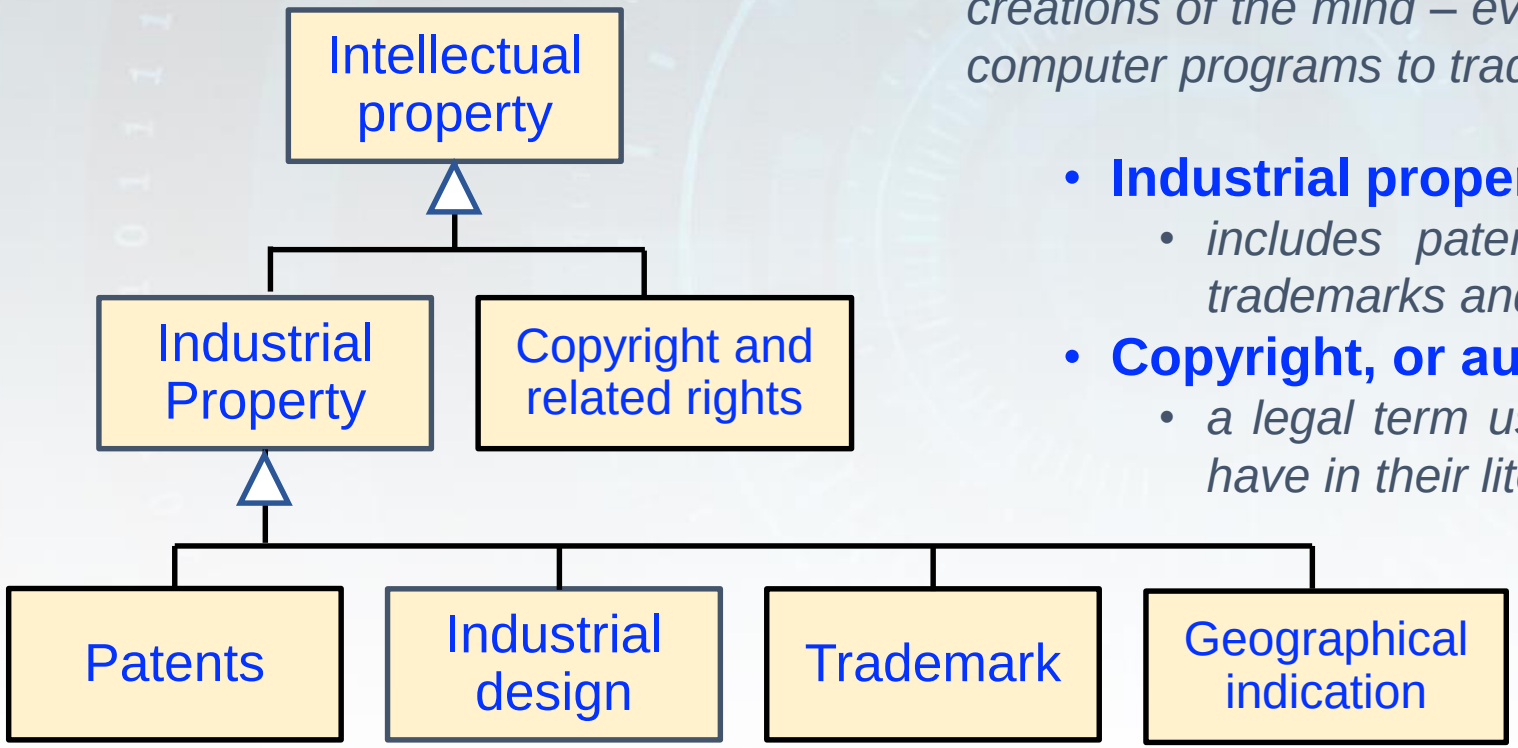
  - **Confidentiality:** *a property of being made not available or disclosed to unauthorized individuals, entities or processes*
  - **Integrity:** *a property of safeguarding the accuracy and completeness of assets*
  - **Availability:** *a property of being accessible and usable upon demand by an authorised entity*



[*Dubois at al., 2010*]

Funded by the Erasmus+ Programme of the European Union

Intellectual Property



Intellectual Property

creations of the mind – everything from works of art to inventions, computer programs to trademarks and other commercial signs

- **Industrial property**
  - *includes patents for inventions, industrial designs, trademarks and geographical indications*
- **Copyright, or authors' right**
  - *a legal term used to describe the rights that creators have in their literary, artistic and scientific works*

WIPO: What is intellectual property? https://www.wipo.int/about-ip/en/

Personal Data

'**Personal data**' *means any information relating to an identified or identifiable natural person ('data subject') an identifiable natural person is one who can be identified, directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

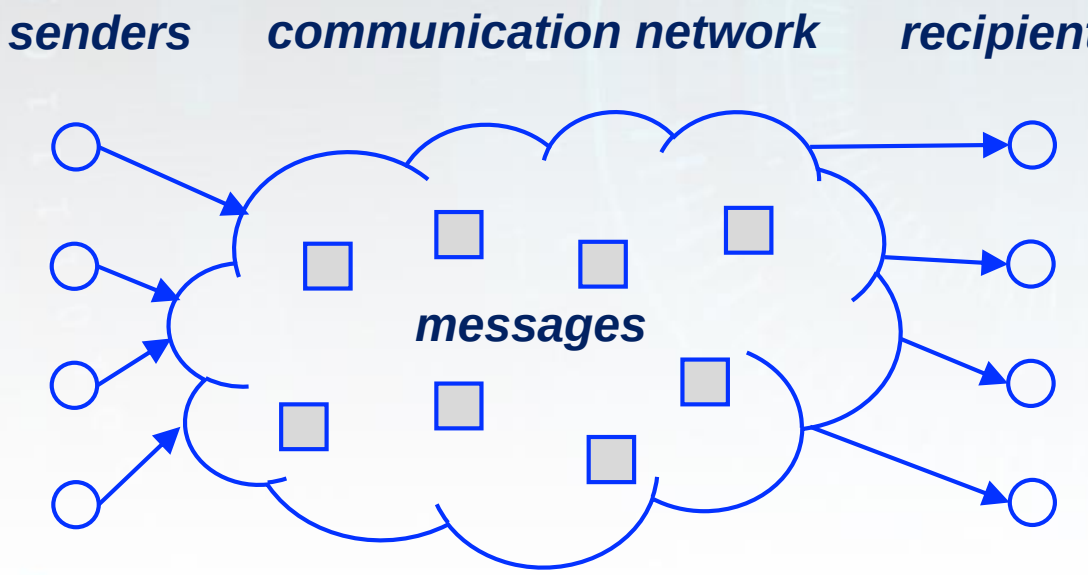
EU General Data Protection Regulation.
URL: https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=uriserv:OJ.L.2016.119.01.0001.01.ENG

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Identity

- An **identity** *is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons*
  - *Names, identifiers, digital pseudonyms, addresses*, and *etc*.

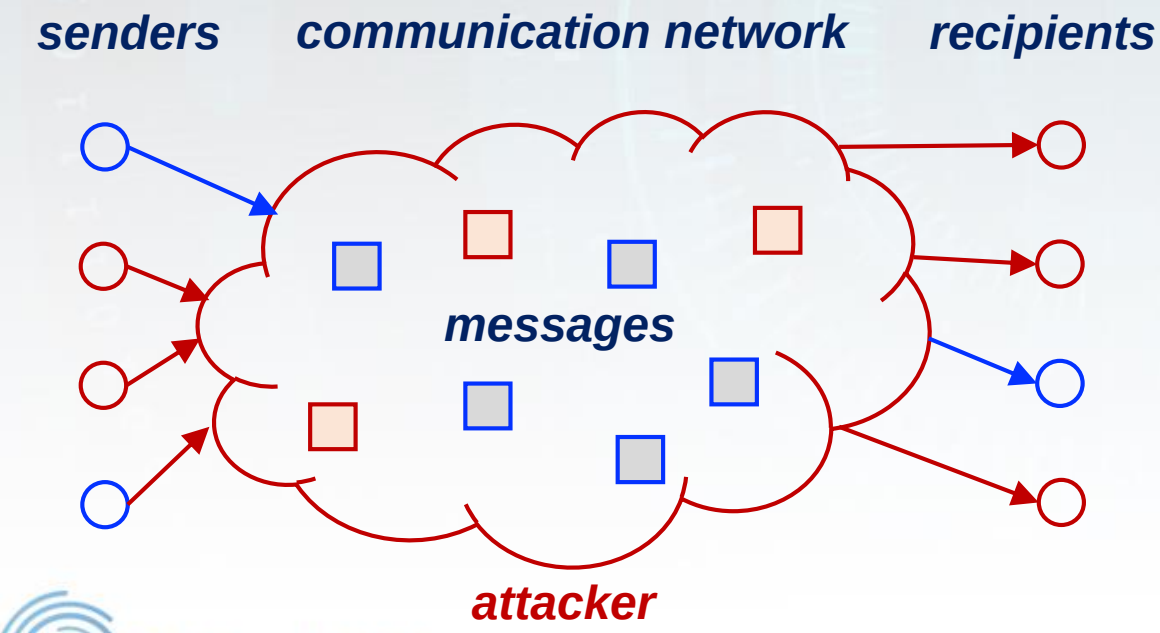


- **Anonymity** *means that subject is not identifiable within a set of the anonymity set, i.e., all subjects*
- **Undetectability** *of an item of interest means that the attacker is not able to distinguish between whether the item of interest exists or not*
- **Unlinkability** *of two or more items of interest means that the attacker cannot sufficiently distinguish whether they are related or not*

[*Pfitzmann and Hansen, 2010*]

Identity

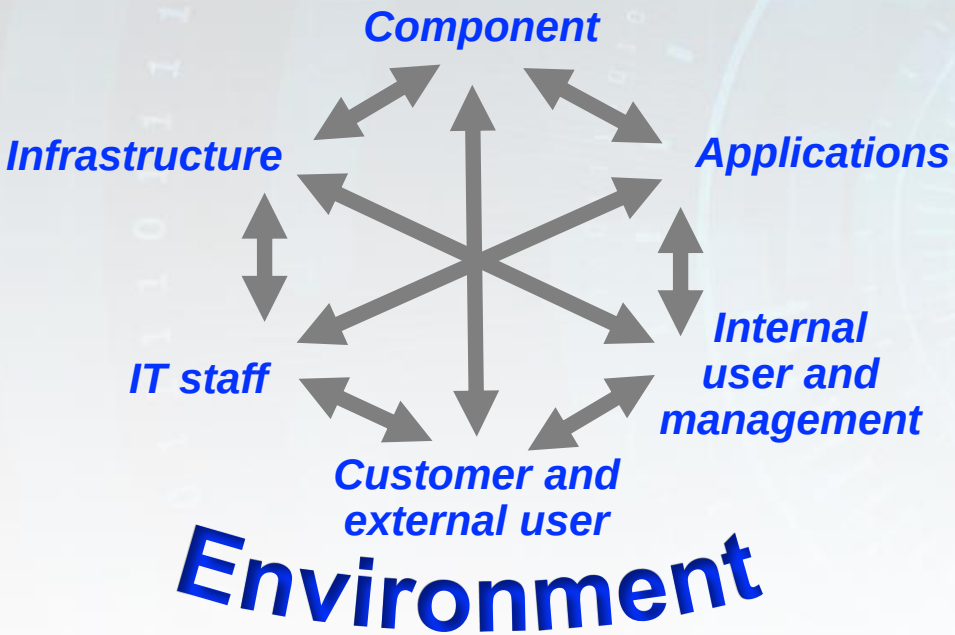
- An **identity** *is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons*
  - *Names, identifiers, digital pseudonyms, addresses*, and *etc*.



- **Anonymity** *means that subject is not identifiable within a set of the anonymity set, i.e., all subjects*
- **Undetectability** *of an item of interest means that the attacker is not able to distinguish between whether the item of interest exists or not*
- **Unlinkability** *of two or more items of interest means that the attacker cannot sufficiently distinguish whether they are related or not*

[Pfitzmann and Hansen, 2010]

How Malicious Software Gets into Device



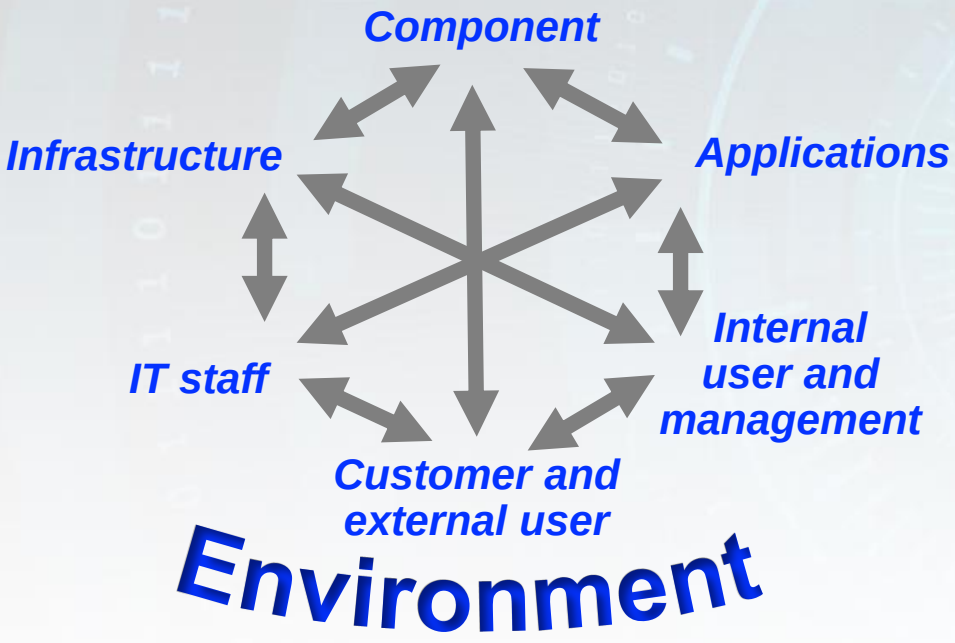
[Anderson, 2008]

***Threat agent's dream*:**

- Acquire massive amount of computing power and brute-force **ALL** the possible combinations of the encrypted key
- Install **keylogger** *or* **trojanised** version of the message viewer
  - *Use outdate (insecure) software in devices connected to the Internet*
  - *Install remote control malware*
  - *Decrypted message could be read from computer's memory or hard disk*

Funded by the Erasmus+ Programme of the European Union

How to Get Someone's Password



[Anderson, 2008]

- Guess the password
- Ask for the password
  - **https://youtu.be/opRMrEfAIiI**
  - **https://youtu.be/UzvPP6_LRHc**

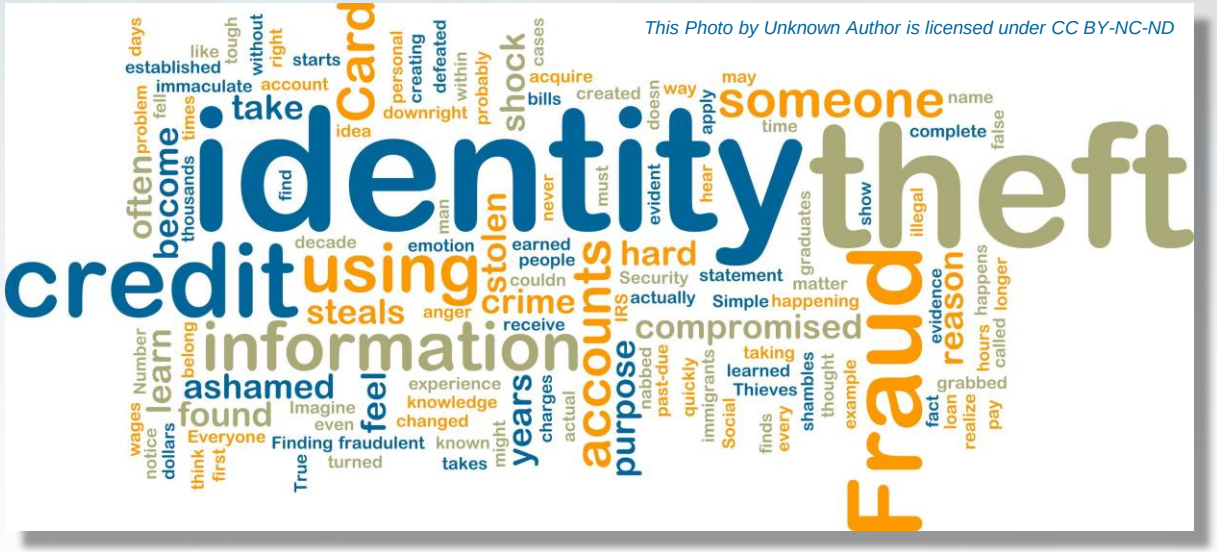
password	master
123456	sunshine
12345678	ashley
qwerty	bailey
abc123	passw0rd
monkey	shadow
1234567	123123
letmein	654321
trustno1	superman
dragon	qazwsx
baseball	michael
111111	football
Iloveyou	

Funded by the Erasmus+ Programme of the European Union

Reasons

of Identity and Personal Data Thefts

- Insufficient security training
- Lack of (appropriate) security policies
- Unawareness
  - *several organisational units*
- Social hacking
  - *empathy to help someone in need*
- Easy access of information
  - *emails IDs*
  - *phone extension numbers of employees*



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Consequences
of Security Attacks to Organisation

- **Symptoms**
  - *Increased CPU usage*
  - *Slow device or web browser speeds*
  - *Problems connecting to networks*
  - *Freezing or crashing*
  - *Modified or deleted files*
  - *Appearance of strange files, programs, or desktop icons*
  - *Programs running, turning off, or reconfiguring themselves*
  - *Strange device behavior*
  - *Emails/messages being sent automatically and without user's knowledge*

- Reputation damage
- Fraudulent information usage
- Information loss
- Privacy loss
- Economic losses
- Lawsuits and arbitrations
- Operational downtime
- Sabotage and dangers of terrorism

Funded by the Erasmus+ Programme of the European Union

Summary

- **Business assets** describe information contents
  - *Intellectual property, personal data, and identity*
  - *Security need*: *confidentiality, integrity, availability*
- **Ways** for malicious software to get into device
- **Reasons** and **consequences** of identity thefts and personal data disclosure

Funded by the Erasmus+ Programme of the European Union

Assignments

Discuss what are ***identifiability***, ***linkability*** and ***detectability*** from attacker's perspective

Discuss how device should be protected against ***malicious software***

e.g., against spyware, keylogger, Trojans, and etc.

Have you ever experienced any symptoms of device "***misbehaviour***"? How did you fix them?

Funded by the Erasmus+ Programme of the European Union

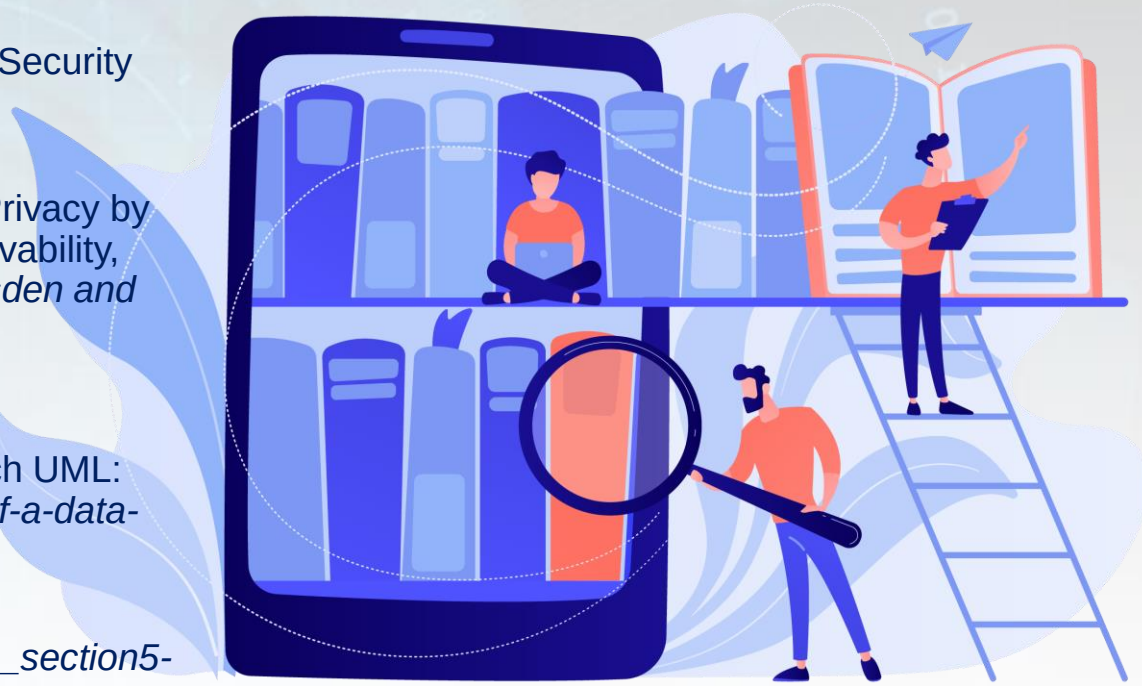
Further Reading

Material used in preparation of this lecture

- **Anderson, R.** (2008) Security Engineering: A Guide to Building Dependable Distributed Systems, *2nd edn. Wiley, New York*
- **Dubois E., Heymans P., Mayer N., Matulevičius R.** (2010) A Systematic Approach to Define the Domain of Information System Security Risk Management. *Intentional Perspectives on Information Systems Engineering 2010: 289-306*
- **Pfitzmann, A., Hansen, M.** (2010) A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. *Technical Report, TU Dresden and ULD Kiel*

Useful links

- **Strawbridge G.** (2020) 5 Damaging Consequences Of A Data Breach UML: *https://www.metacompliance.com/blog/5-damaging-consequences-of-a-data-breach/*
- **State of New Jersey 2014 Hazard Mitigation Plan**. URL: *https://www.state.nj.us/njoem/programs/pdf/mitigation2014b/mit2014_section5-23.pdf*
- **World Intellectual Property Organisation**, What is intellectual property? URL: *https://www.wipo.int/about-ip/en/*



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Short Videos

- Understanding intellectual property
  - ***https://youtu.be/UqZJPuyK9VY***
- What is personal data under GDPR?
  - ***https://youtu.be/qJX3fbq3fOg***
- Intellectual Property Theft
  - ***https://youtu.be/0y0KV0B1v10***
- The most horrific case of identity theft
  - ***https://youtu.be/CJ40tAm8cTE***
- What can happen to your personal data online?
  - ***https://youtu.be/v4IIH3sJlMc***

Thank you!