Risk Modeling Using Graphs and Tables

An Exercise

Fabio Massacci, Federica Paci, Katsiaryna Labunets

What we are going to do (1)

- This is an exercise to evaluate your level of **comprehension** of graphical and tabular **risk models**
- You **will learn** two notations that you are going to use for the assignments
- This is **not** an **exam** and you **will not be evaluated** based on this exercise
- This exercise is organized in two sessions
  - We want to test the effect that time to complete the questionnaire has on your level of comprehension of the risk models

What we are going to do (2)

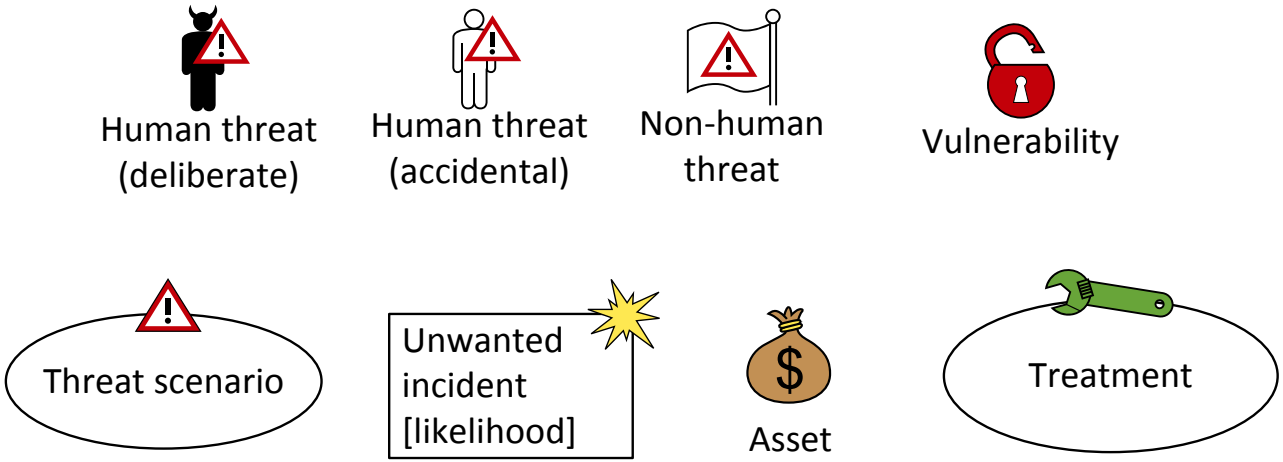
- **Session 1**
  1. You will be introduced to the graphical and tabular notation for representing risk models and an application scenario (10 min)
  2. You will be asked to fill a demographic questionnaire (5 min)
  3. You will be asked to download a risk model (graphical or tabular) and answer questions about the model (20 min)
  4. You will be asked to answer a post-task questionnaire (2 min)
  5. 10 minutes break

What we are going to do (3)

- **Session 2**
  1. You will be introduced to the second application scenario (2 min)
  2. You will be asked to download a risk model (different from the one used in Session 1) and answer questions about the model (40 min)
  3. You will be asked to answer a post-task questionnaire (2 min)
- **Open Discussion**
  - You provide us feedback

CORAS

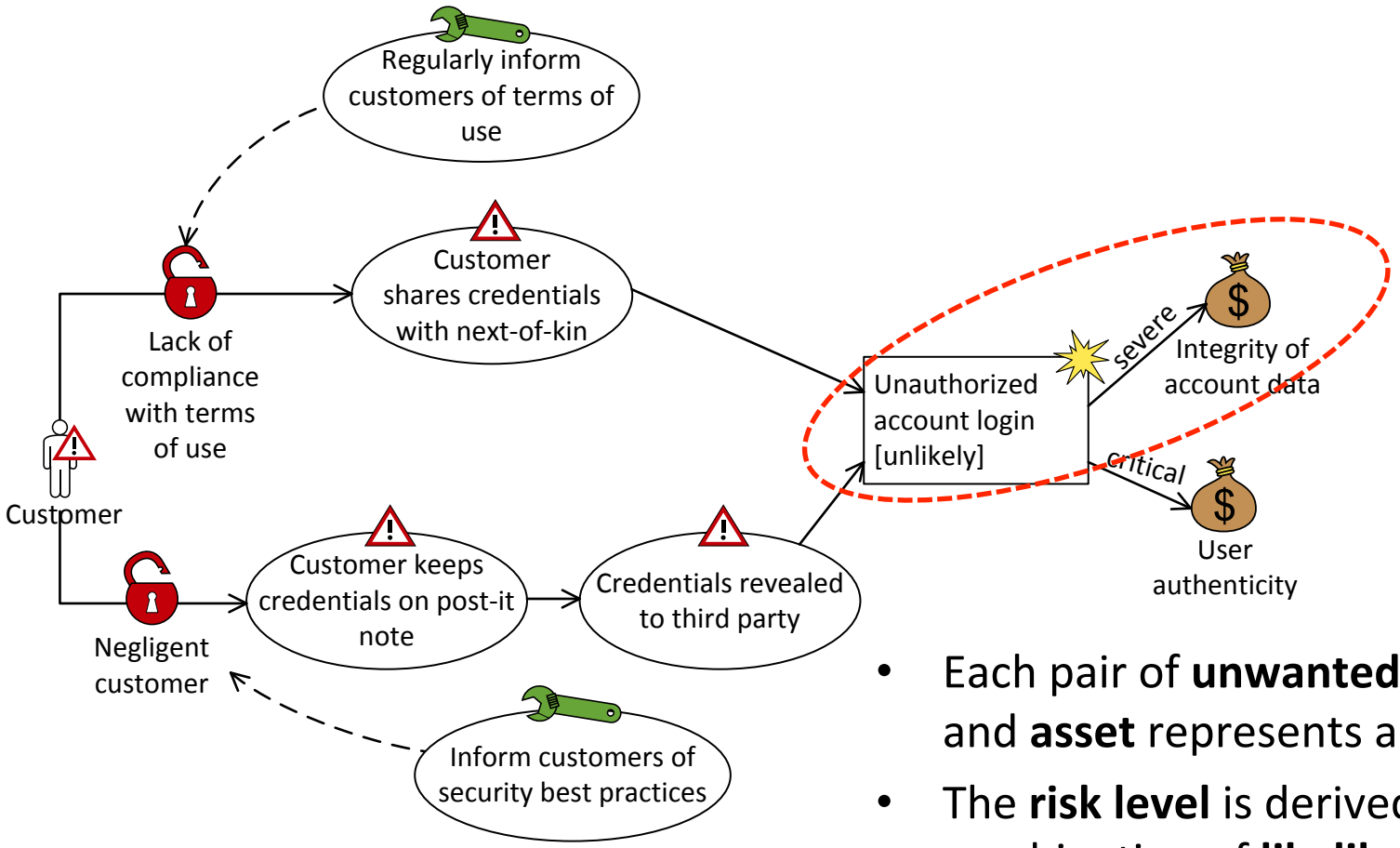
CORAS Elements



CORAS terms

Term	Definition	Icon
Threat	A potential cause of an unwanted incident	
Vulnerability	A weakness, flaw or deficiency that opens for, or may be exploited by a threat to cause harm to or reduce the value of an asset	
Threat scenario	A chain or series of events that is initiated by a threat and that may lead to an unwanted incident	
Unwanted incident	An event that harms or reduces the value of an asset	
Asset	Something to which a party assigns value and hence for which the party requires protection	
Likelihood	The frequency or probability for something to occur	
Consequence	The impact of an unwanted incident on an asset in terms of harm to or reduced asset value	
Treatment	An appropriate measure to reduce risk level	

CORAS Example



- Each pair of **unwanted incident** and **asset** represents a **risk**
- The **risk level** is derived from the combination of **likelihood** and **consequence**

NIST 800-30

NIST 800-30 Terms

Term	Definition
Threat event	An event (or scenario) or situation that has the potential for causing undesirable consequences or impact
Threat source	The adversarial, accidental, structural or environmental exploitation of a vulnerability
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source
Impact	A harmful event that may occur given the potential for threats exploiting vulnerabilities
Asset	Operations, individuals, physical or non-physical entities that can be harmed due to a threat event and its impact
Overall likelihood	The likelihood that a threat event results in adverse impact
Level of impact	The degree of impact in terms of harm to assets
Security control	Safeguards or countermeasures to protect the confidentiality, integrity and availability of a system and its information

NIST Example

Threat event	Threat source	Vulnerabilities	Impact	Asset	Overall likelihood	Level of impact	Security control
Customer shares credentials with next-of-kin	Customer	Lack of compliance with terms of use	Unauthorized account login **Risk**	Integrity of account data	Unlikely **Risk level**	Severe	Regularly inform customers of terms of use
Customer shares credentials with next-of-kin	Customer	Lack of compliance with terms of use	Unauthorized account login	User authenticity	Unlikely	Critical	Regularly inform customers of terms of use
Customer keeps credentials on post-it note which is revealed to third party	Customer	Negligent customer	Unauthorized account login **Same risk, but other causes**	Integrity of account data	Unlikely	Severe	Inform customers of security best practices
Customer keeps credentials on post-it note which is revealed to third party	Customer	Negligent customer	Unauthorized account login	User authenticity	Unlikely	Critical	Inform customers of security best practices

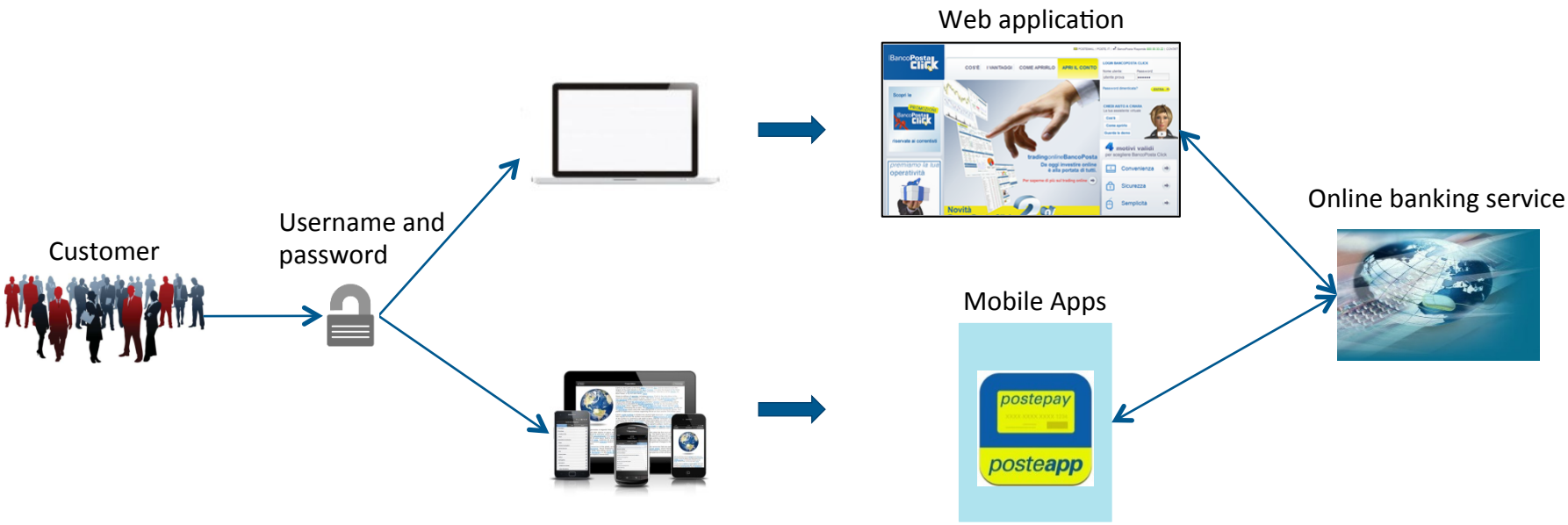
Scales and Risk Criteria

Risk Criteria

		Consequence/Impact				
		Insignificant	Minor	Severe	Critical	Catastrophic
Likelihood	Certain					
	Very likely					
	Likely					
	Unlikely					
	Very unlikely					

Poste Italiane Scenario

Poste Italiane Scenario

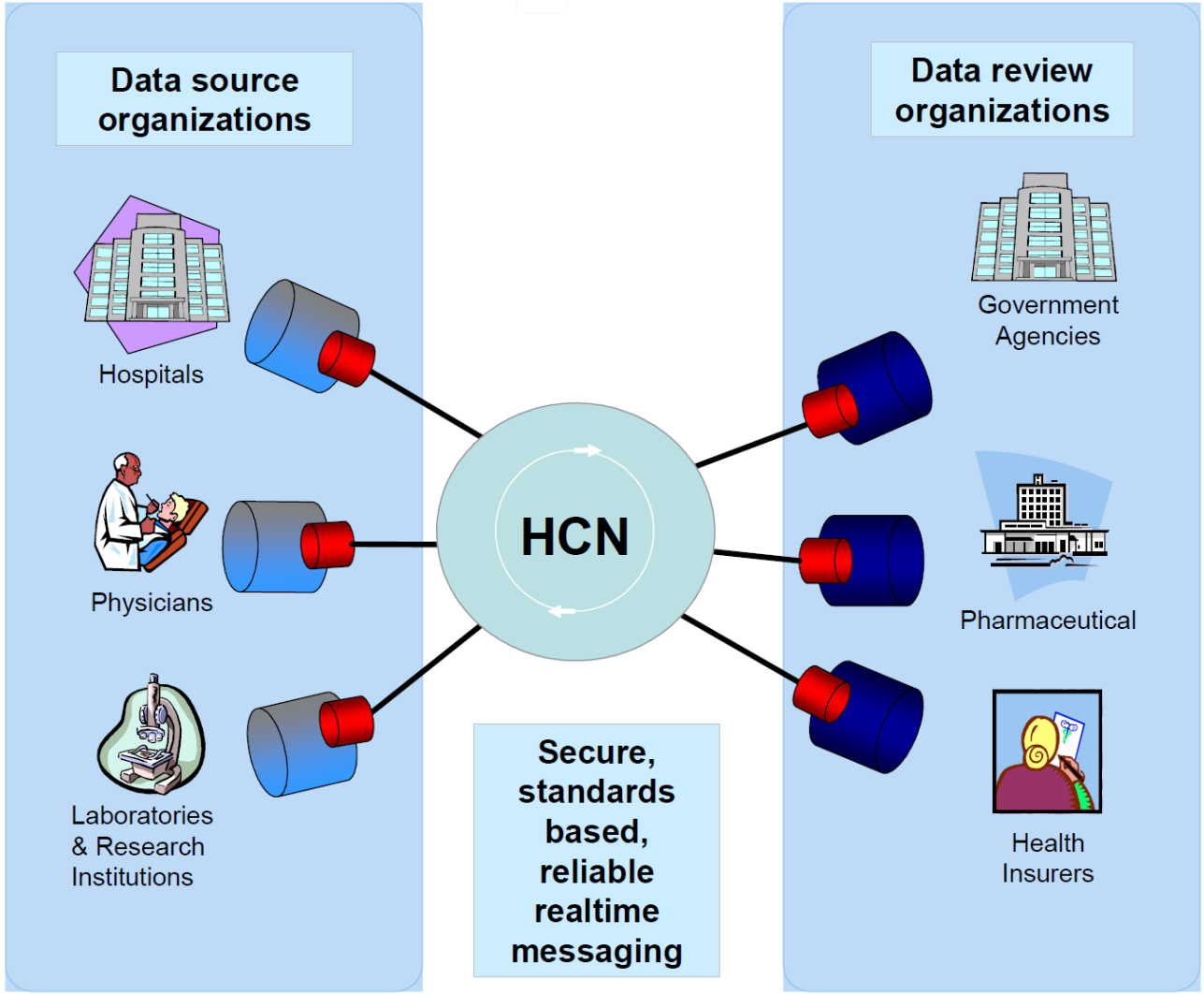


Poste Italiane Assets

- The Poste Italiane risk assessment is with respect to the following assets
  - **Integrity of account data**
    Includes personal information, as well as the bank account balance
  - **User authenticity**
    This means that the person that is logged in as a user is identical to the user
  - **Confidentiality of customer data**
    Includes personal information, as well as information about savings, loans, account balance, etc.
  - **Availability of service**
    The online banking services shall be available to the customers 24/7

Healthcare Collaborative Network (HCN) Scenario

Healthcare Collaborative Network Scenario



Healthcare Collaborative Network Assets

- The HCN risk assessment is with respect to the following assets
  - **Data confidentiality**
    Health records and all other sensitive information shall not be made available or disclosed to unauthorized individuals
  - **Data integrity**
    Information shall be protected from unauthorized changes
  - **Privacy**
    Patient information shall be provided in an anonymous way and personally identifiable information shall not be disclosed to unauthorized individuals