UNIVERSITY OF Southampton
Electronics and Computer Science

COMP6236
Software Engineering and Cyber Security
Risk Analysis with CORAS

Dr Mu Yang

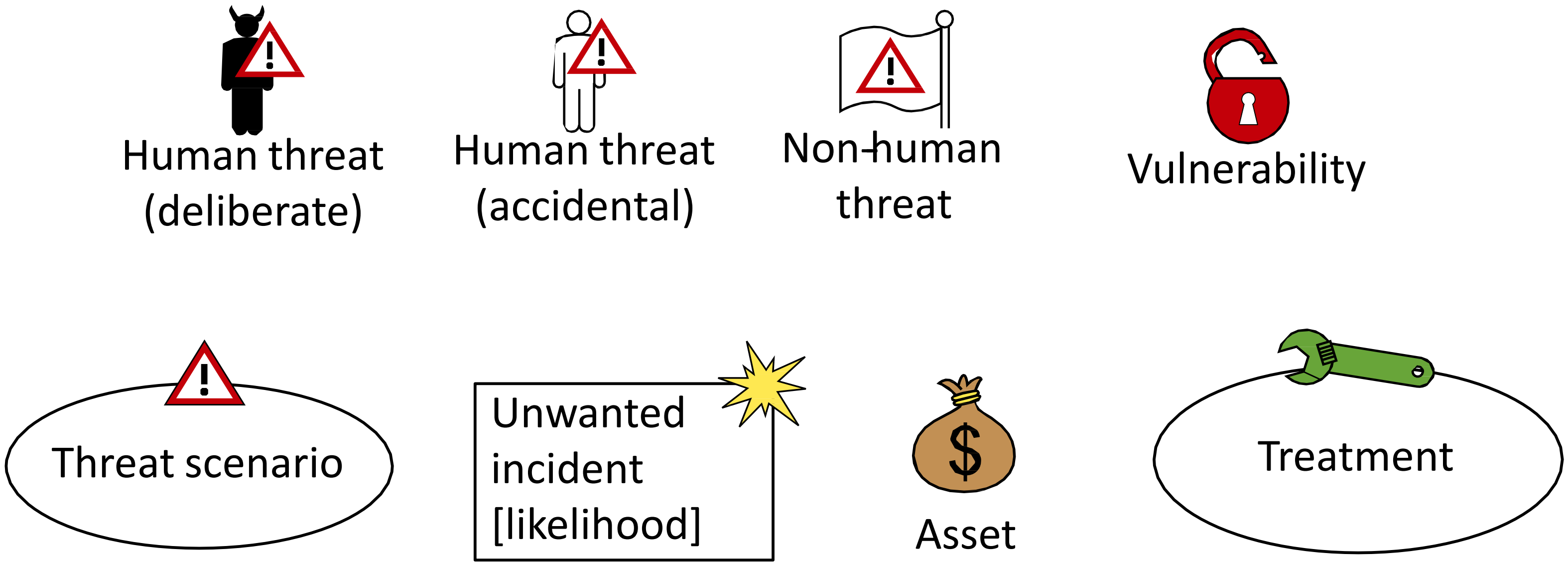
Lecture Outline

- What is CORAS?
  - CORAS Language
  - CORAS Process
  - CORAS Tool

What is CORAS?

- The **CORAS language** (diagrams)
  - A graphical language that supports the analysis process
  - Basis for communication, documentation and analysis
- The **CORAS process**
  - A process for security risk analysis
  - Based on internationally established standards (*ISO 31000)*
- The **CORAS tool**
  - A graphical editor

CORAS Language



Human threat (deliberate)

Human threat (accidental)

Non-human threat

Vulnerability

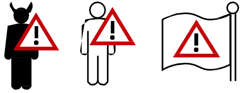
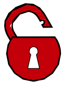
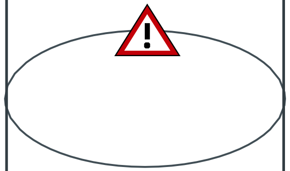
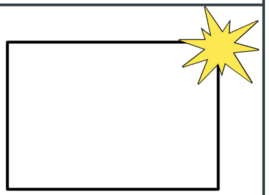
Threat scenario

Unwanted incident [likelihood]

Asset

Treatment

CORAS Language

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	

CORAS Language

Term	Definition	Icon
Asset	Something to which a party assigns value and hence for which the party requires protection	💰
Treatment	An appropriate measure to reduce risk level	🔧
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	

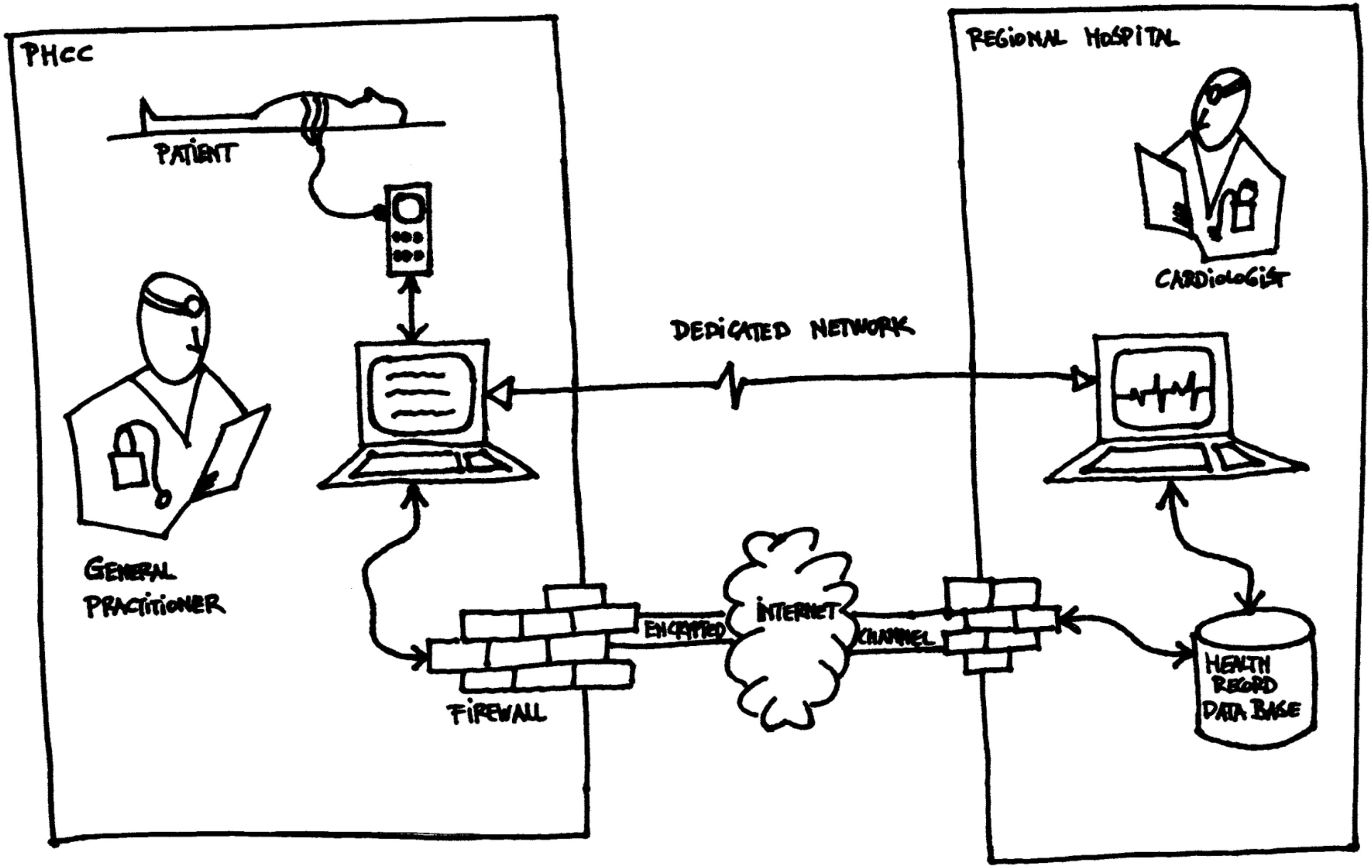
The CORAS diagrams

- **Asset diagrams** - Describe the focus of the analysis
- **Threat diagrams** - Describe scenarios which may cause harm to the assets
- **Risk diagrams** - Summarise the risks presented in threat diagrams
- **Treatment diagrams** - Add proposed treatments to threat diagrams
- **Treatment Overview diagrams**- Add proposed treatments to risk diagrams

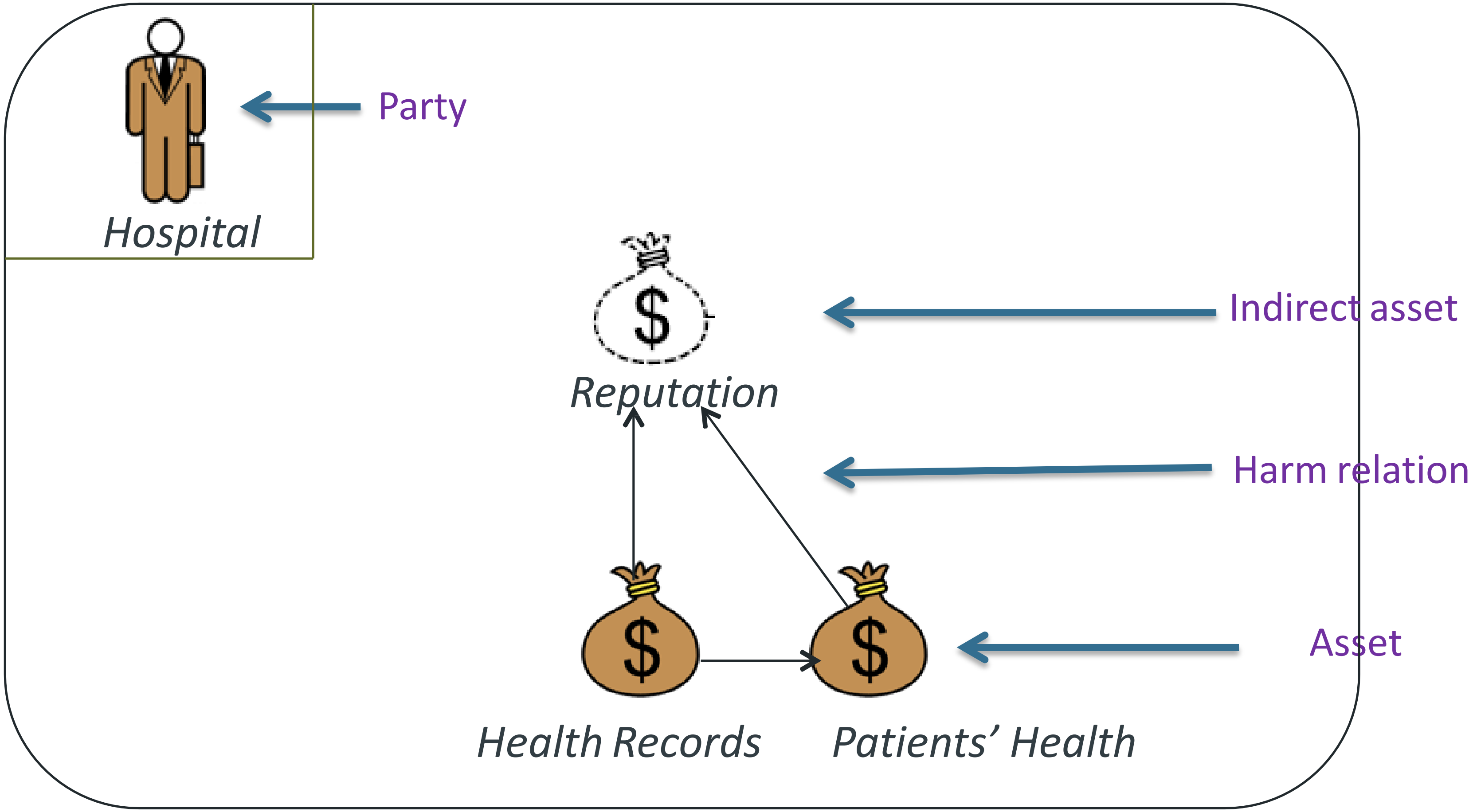
A Case Study

In one region of the country, an experimental telemedicine system has been set up. A dedicated network between the regional hospital and several primary health care centres (PHCC) allows a general practitioner (GP) to conduct a cardiological examination of a patient (at the PHCC) in cooperation with a cardiologist located at the hospital. During an examination, both of the medical doctors have access to the patient's health record, and all data from the examination is streamed to the cardiologist's computer.

The National Ministry of Health is concerned whether the patient privacy is sufficiently protected, and hires a risk analysis consultancy company to conduct a risk analysis of the cardiology system with particular focus on privacy. The consultancy company appoints a team of two consultants to do the job. They are in the following referred to as "the analysts" and assigned the roles of risk analysis leader and risk analysis secretary, respectively.


PHCC
PATIENT
GENERAL PRACTITIONER
FIREWALL
ENCRYPTED
INTERNET
CHANNEL
DEDICATED NETWORK
REGIONAL HOSPITAL
CARDIOLOGIST
HEALTH RECORD DATA BASE

Asset Diagrams



Party

Hospital

Indirect asset

Reputation

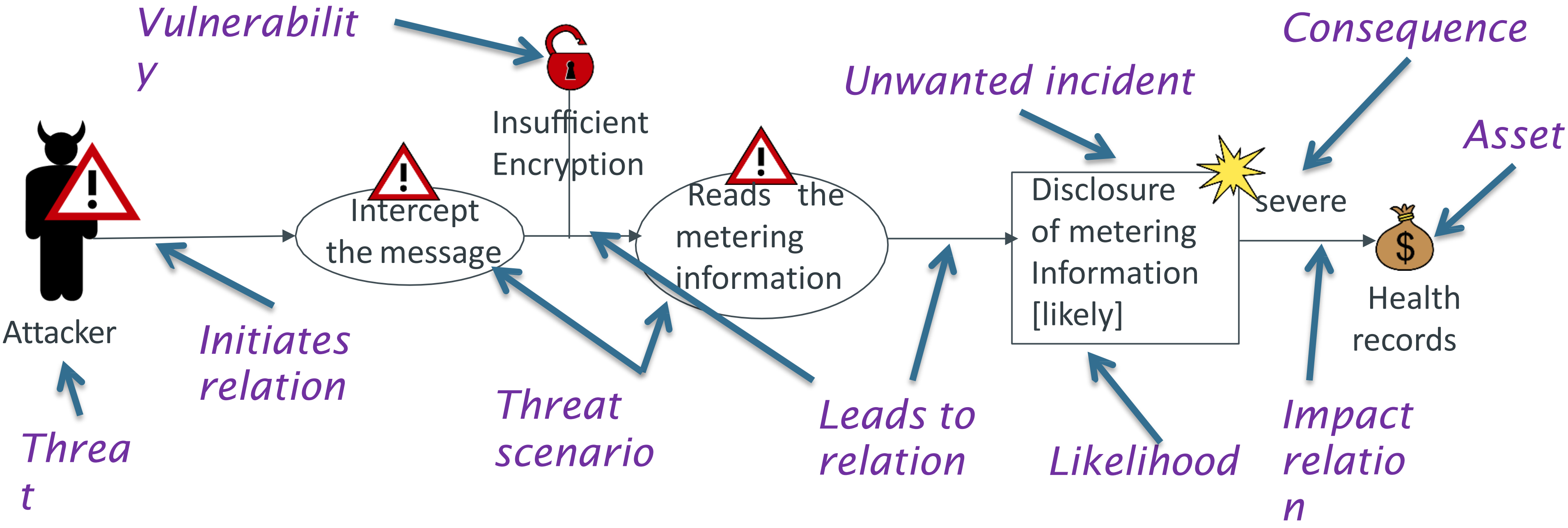
Harm relation

Asset

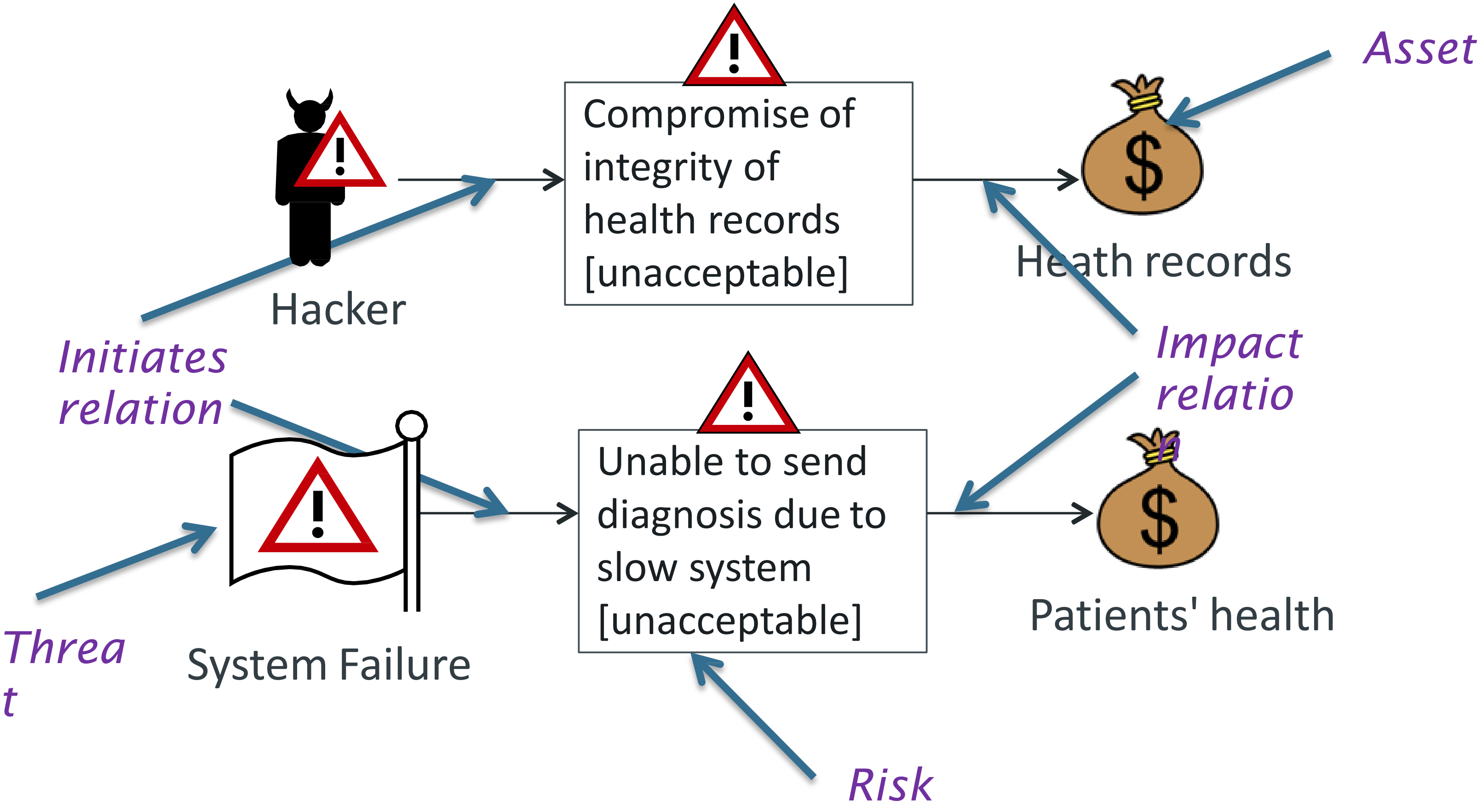
Health Records

Patients' Health

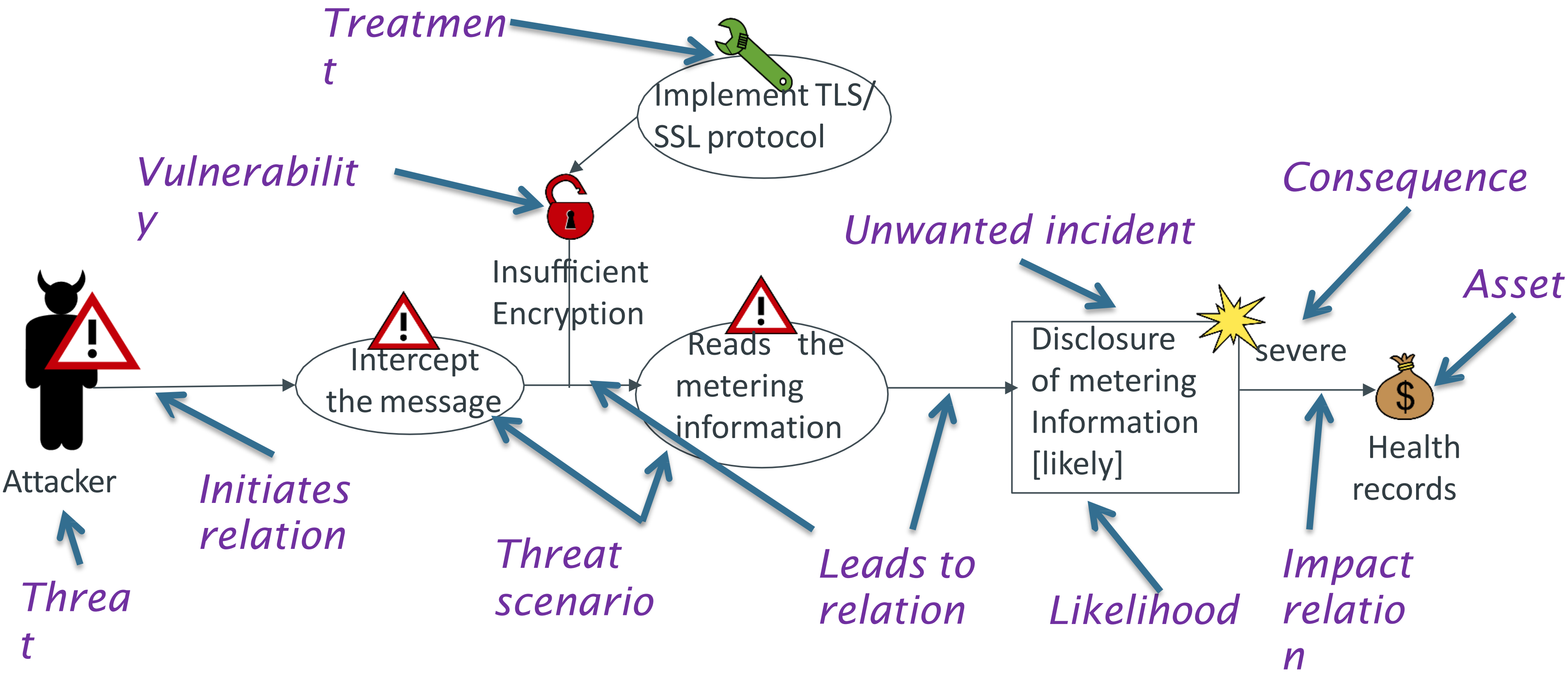
Threat Diagrams



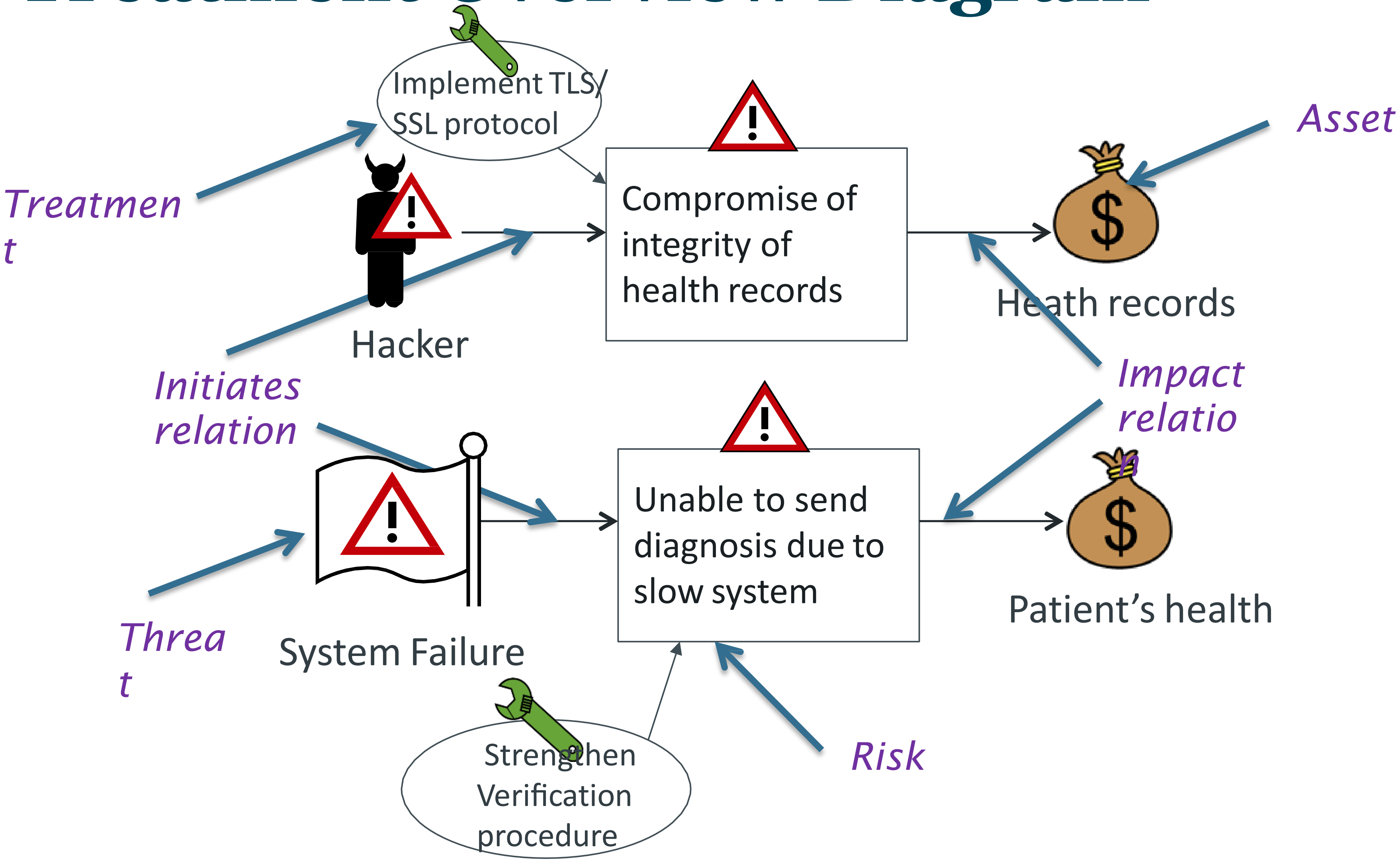
Risk Diagrams


Asset
Compromise of integrity of health records [unacceptable]
Hacker
Heath records
Initiates relation
Impact relatio
n
Unable to send diagnosis due to slow system [unacceptable]
Patients' health
Threa
t
System Failure
Risk

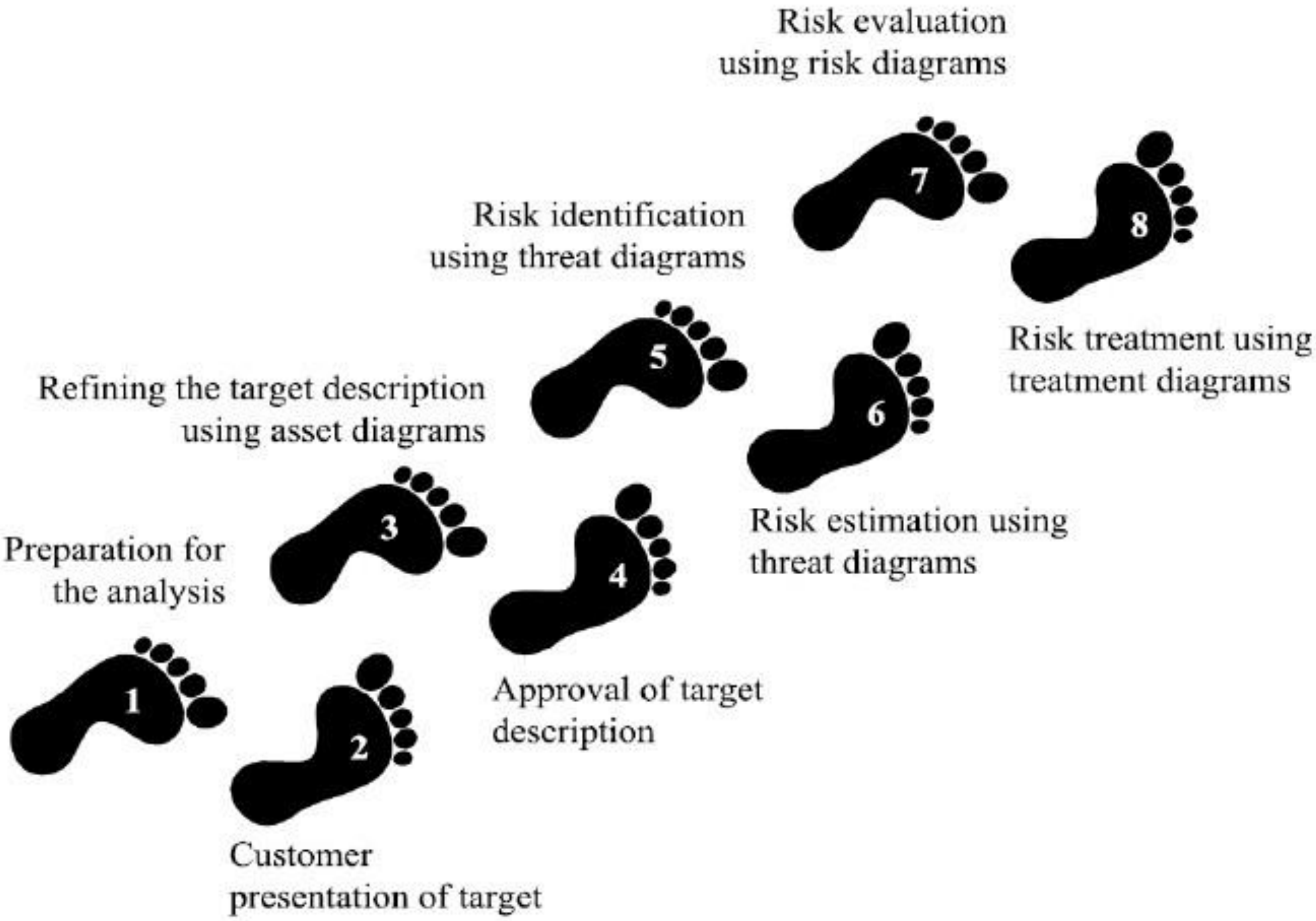
Treatment Diagrams



Treatment Overview Diagram


Implement TLS/ SSL protocol
Treatment
Hacker
Compromise of integrity of health records
Heath records
Asset
Initiates relation
Impact relation
System Failure
Threat
Unable to send diagnosis due to slow system
Patient's health
Strengthen Verification procedure
Risk

CORAS Process



Preparation for the analysis

Customer presentation of target

Refining the target description using asset diagrams

Approval of target description

Risk identification using threat diagrams

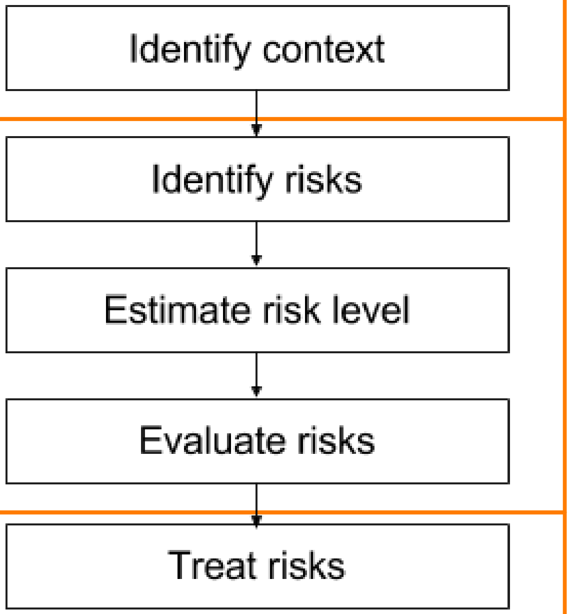
Risk estimation using threat diagrams

Risk evaluation using risk diagrams

Risk treatment using treatment diagrams

CORAS Process

1. Preparation for the analysis
2. Customer presentation of the target
3. Refining the target description using asset diagrams
4. Approval of the target description
5. Risk identification using threat diagrams
6. Risk estimation using threat diagrams
7. Risk evaluation using risk diagrams
8. Risk treatment using treatment diagrams



Identify context

Identify risks

Estimate risk level

Evaluate risks

Treat risks

Example: Local Bank

- Local Bank is a private bank. Its business is to offer financial services to its customers.
- Local Bank has a web application and an online banking system.
- Local Bank is using a database to manage customer information
- Local Bank has decided it wants to do a risk analysis of the system.
- Of particular concern for the management is:
  - the web application for customers
  - the online banking system that connects to both their customer database and the web application.

Step 1 Preparation

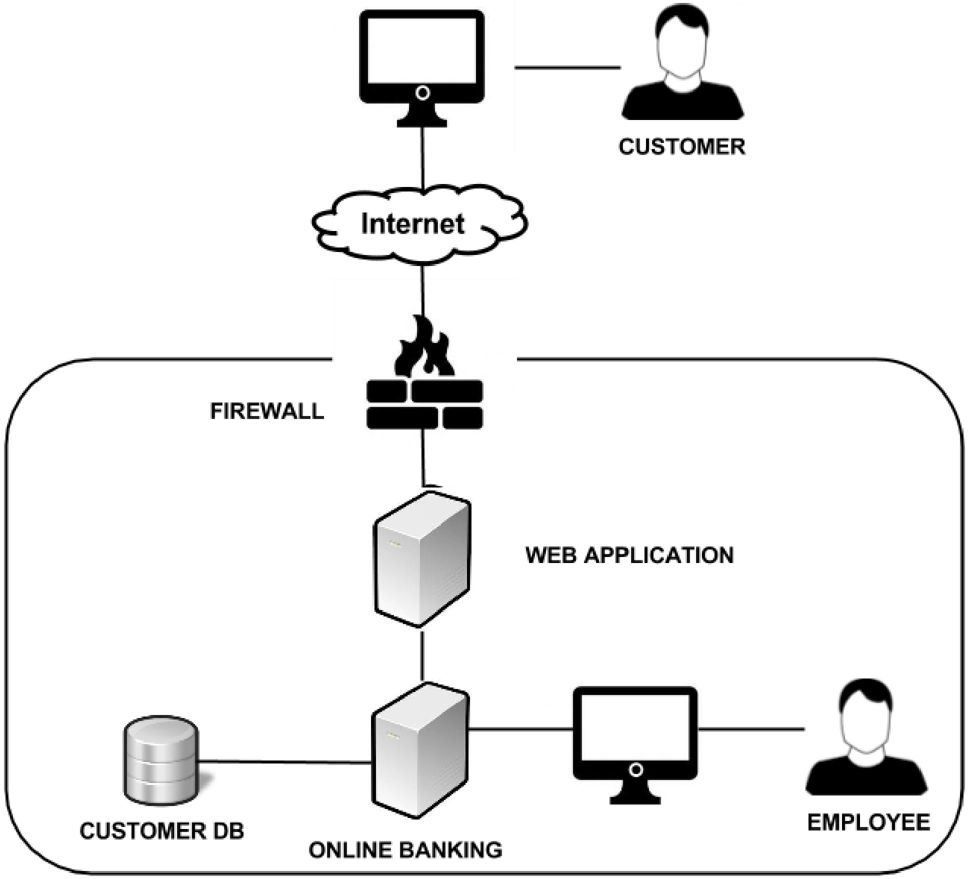
- **Objective**
  - to do the necessary initial preparations prior to the actual startup of the analysis
- **Tasks**
  - Roughly setting the scope and focus
  - Informing the client of its responsibilities

Step 2 Customer presentation

- **Objective**
  - achieve an initial understanding of the target of risk analysis
- **Tasks**
  - Client presents the goals and the target of the analysis
  - The focus and scope of the analysis is set
  - Meetings and workshops are planned
- **Artifacts**
  - Description of the target

Example: Customer presentation

- Of particular concern for the management is:
  - the web application that connects to both their customer database and their online banking portal.

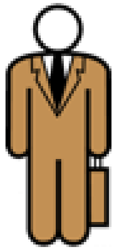


Step 3 Refining the target

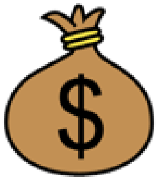
- **Objective**
  - ensure a common understanding of the target analysis
- **Tasks**
  - The target as understood by the risk analysts is presented
  - Identify the parties and assets
  - Conduct a high-level analysis
- **Artifacts**
  - Asset diagram
  - High-level analysis: preliminary list of Unwanted incidents

Identify asset

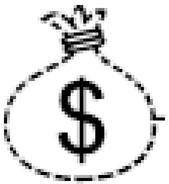
- Identify involving parties
- Identify assets of each party intends to protect:
  - The “THINGS” that are valuable
- Notations to be used in Asset Diagram



Party



Direct Asset



Indirect Asset

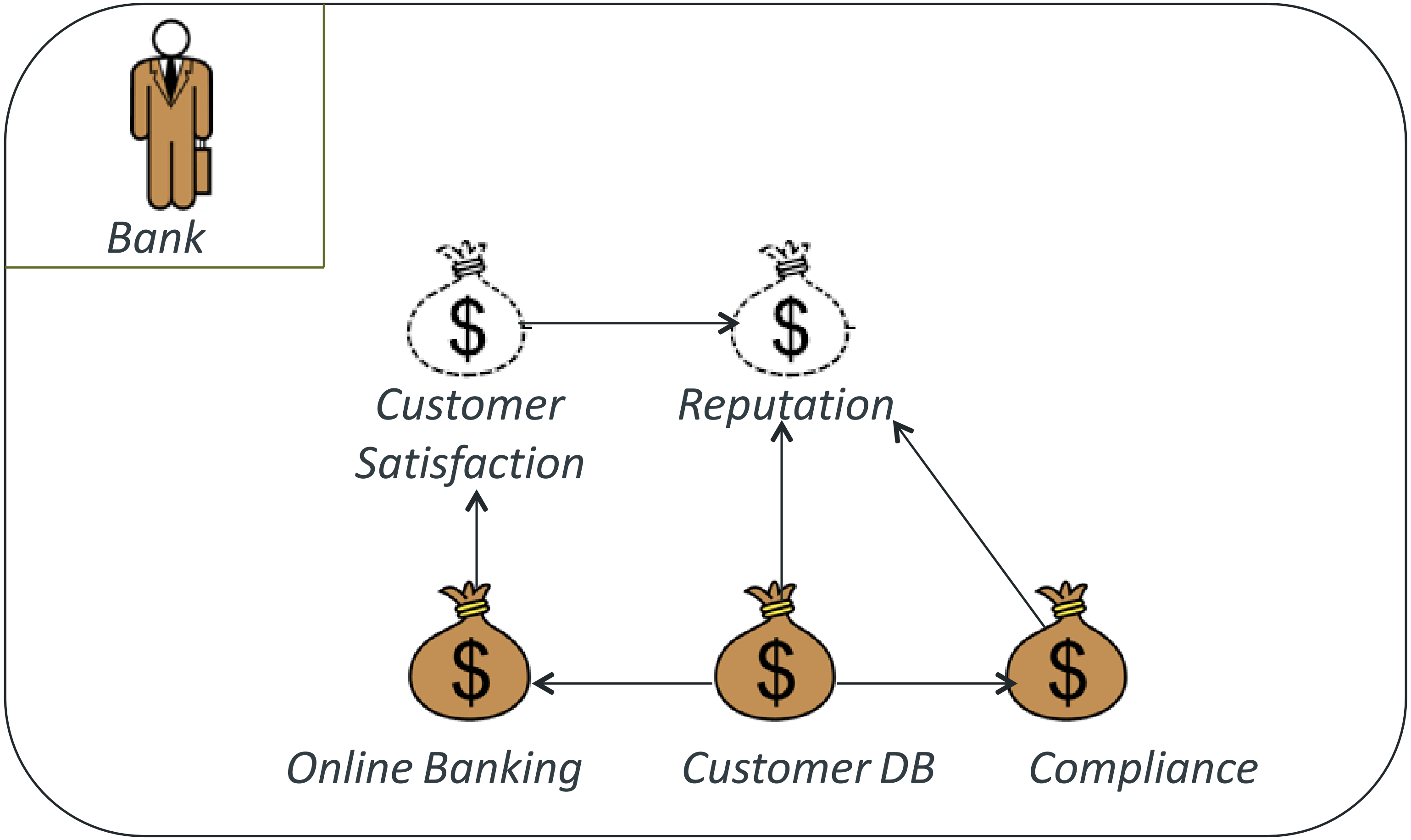
Example: Identify Party and Asset

- Party:
  -
- Asset:
  -
  -
  -
  -
  -

Example: Identify Party and Asset

- Party:
  - Local Bank
- Asset:
  - Customer DB
  - Online banking
  - Compliance
  - Bank reputation
  - Customer satisfaction

Example: Asset diagram



High level Risk analysis

- Preliminary list of Unwanted Incidents

Who/ What is the cause?	How? What may happen? What does it harm?	What makes this possible?
...	...	.....
....	....	.....

High level Risk analysis

Who/ What is the cause?	How? What may happen? What does it harm?	What makes this possible?
Hacker	Customer's browser infected by a Trojan	Poor Security Awareness
System Failure	Web application goes down	Immature Technology
Cyber Criminal	Keylogger installed on employee computer	Poor Security Awareness

Step 4 Approval of the target

- **Objective**
  - decide a ranking of the assets; establish scales for estimating risks and criteria for evaluate risks
- **Tasks**
  - Define Likelihood scale and its description
  - Define Consequence scale for each direct asset
  - Agree on Risk evaluation criteria
- **Artifacts**
  - Likelihood and Consequence scales
  - Risk function and Risk evaluation criteria

Define Likelihood scale

- Likelihood: the frequency or probability of something to occur

Likelihood	Description
Certain	Five times or more per year
Likely	Two to five times per year
Possible	Once a year
Unlikely	Less than once per year
Rare	Less than once per ten years

Define Consequence scale

- Online Banking

Consequence	Description
Catastrophic	Downtime in range [1 week,∞>
Severe	Downtime in range [1 day, 1 week>
Moderate	Downtime in range [1 hour,1 day>
Minor	Downtime in range [1 minute, 1 hour>
Insignificant	Downtime in range [0, 1 minute>

Define Consequence scale

- Customer DB

Consequence	Description
Catastrophic	Range of [50%,100%] of records are affected
Severe	Range of [20%,50%] of records are affected
Moderate	Range of [10%,20%] of records are affected
Minor	Range of [1%,10%] of records are affected
Insignificant	Range of [0%,1%] of records are affected

Define Consequence scale

- Compliance

Consequence	Description
Catastrophic	Chief executive officer is sentenced to jail for more than 1 year
Severe	Chief executive officer is sentenced to jail for up to 1 year
Moderate	Claim for indemnification or compensation
Minor	Fine
Insignificant	Illegal data processing is ordered to cease

Example: Risk Evaluation Matrix

Risk Function (Compliance)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Severe	Catastrophic
Rare	🟩	🟩	🟨	🟨	🟨
Unlikely	🟩	🟩	🟨	🟨	🟥
Possible	🟩	🟩	🟨	🟨	🟥
Likely	🟩	🟨	🟨	🟨	🟥
Certain	🟩	🟨	🟨	🟥	🟥

🟩	Acceptable
🟨	Monitor
🟥	Need to be treated

Example: Risk Evaluation Matrix

Risk Function (Customer DB)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Severe	Catastrophic
Rare	🟩	🟩	🟨	🟥	🟥
Unlikely	🟩	🟩	🟨	🟥	🟥
Possible	🟩	🟩	🟨	🟥	🟥
Likely	🟩	🟨	🟨	🟥	🟥
Certain	🟩	🟨	🟥	🟥	🟥

🟩 Acceptable

🟨 Monitor

🟥 Need to be treated

Example: Risk Evaluation Matrix

Risk Function (Online Banking)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Severe	Catastrophic
Rare	🟩	🟩	🟨	🟨	🟥
Unlikely	🟩	🟩	🟨	🟨	🟥
Possible	🟩	🟩	🟨	🟥	🟥
Likely	🟩	🟨	🟨	🟥	🟥
Certain	🟩	🟨	🟥	🟥	🟥

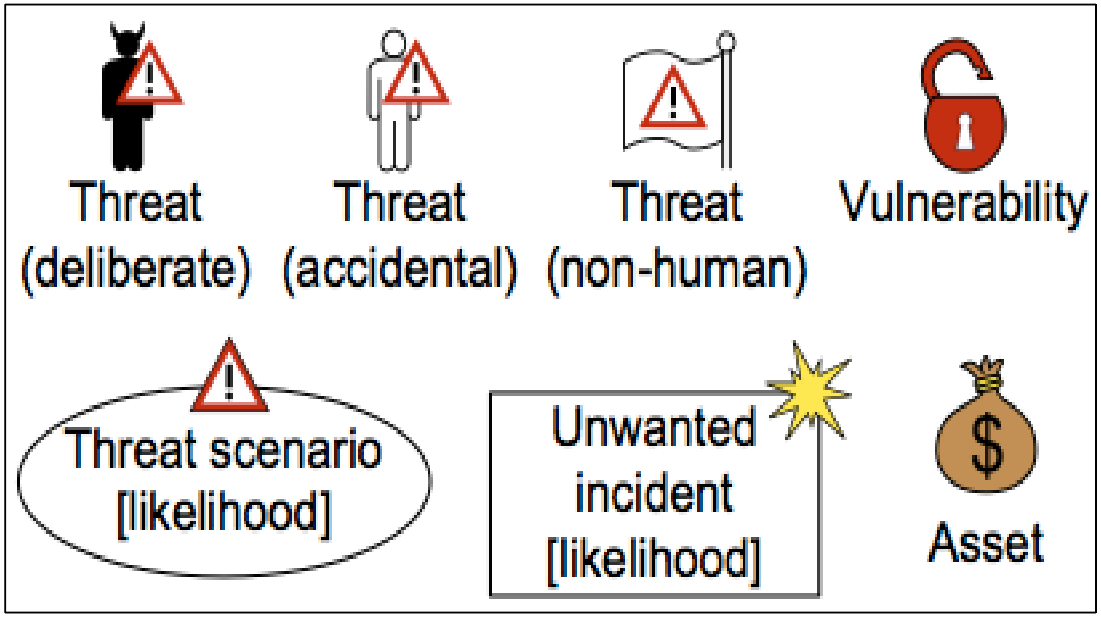
🟩	Acceptable
🟨	Monitor
🟥	Need to be treated

Step 5 Risk Identification

- **Objective**
  - Identify unwanted incidents, threats, threat scenarios and vulnerabilities
- **Tasks**
  - Identify Assets and Threats
  - Identify Unwanted Incidents
  - Identify Threat Scenarios
  - Identify Vulnerabilities
- **Artifacts**
  - Threat diagram

Step 5 Risk Identification

- Notations to be used in Threat Diagram



Step 5.1 Identify Assets and Threats

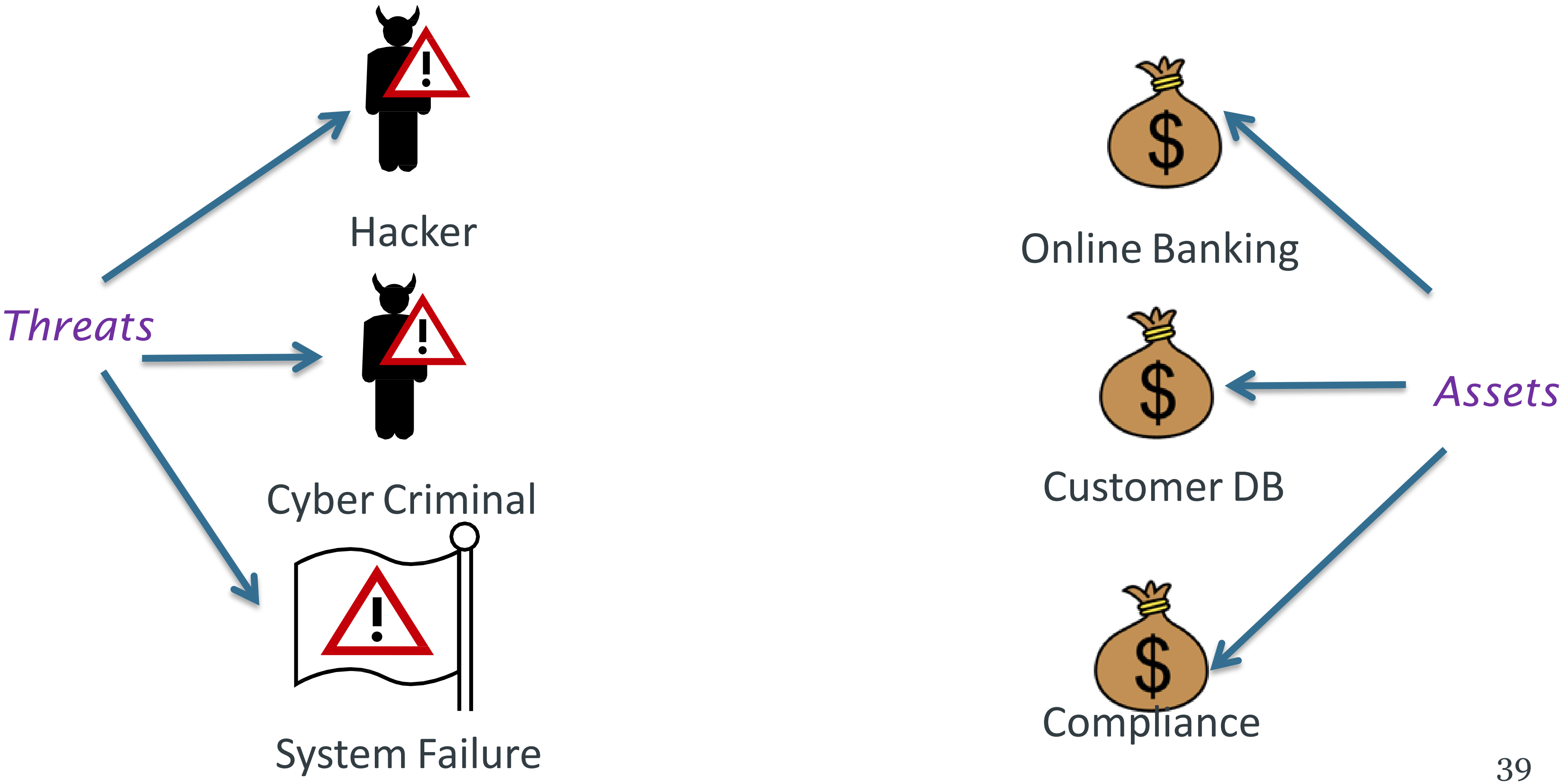
- What are the threats?

Threats

Assets

Step 5.1 Identify Assets and Threats

- What are the threats?



Threats

Hacker

Cyber Criminal

System Failure

Assets

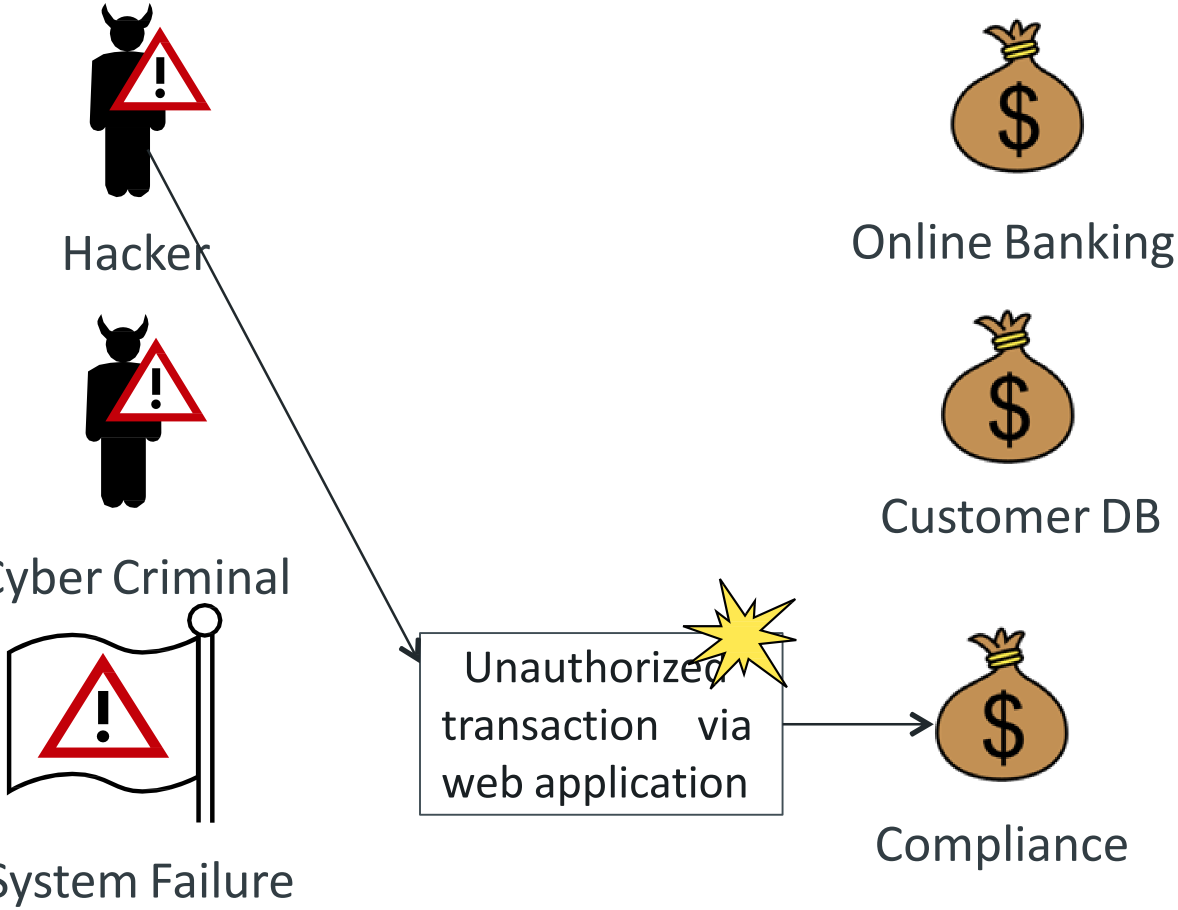
Online Banking

Customer DB

Compliance

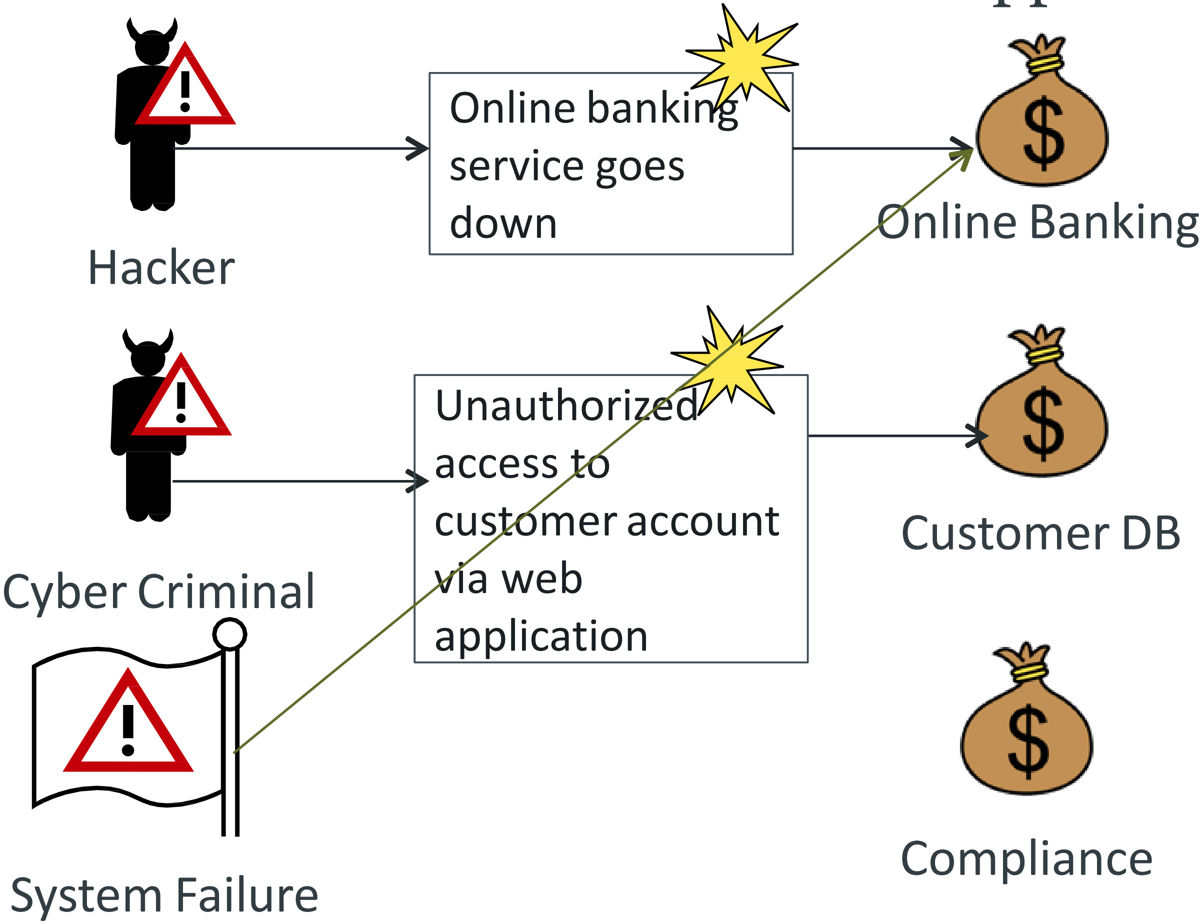
Step 5.2 Identify Unwanted Incidents

- What unwanted incidents do we fear will happen?



Step 5.2 Identify Unwanted Incidents

- What unwanted incidents do we fear will happen?



Hacker

Cyber Criminal

System Failure

Online banking service goes down

Unauthorized access to customer account via web application

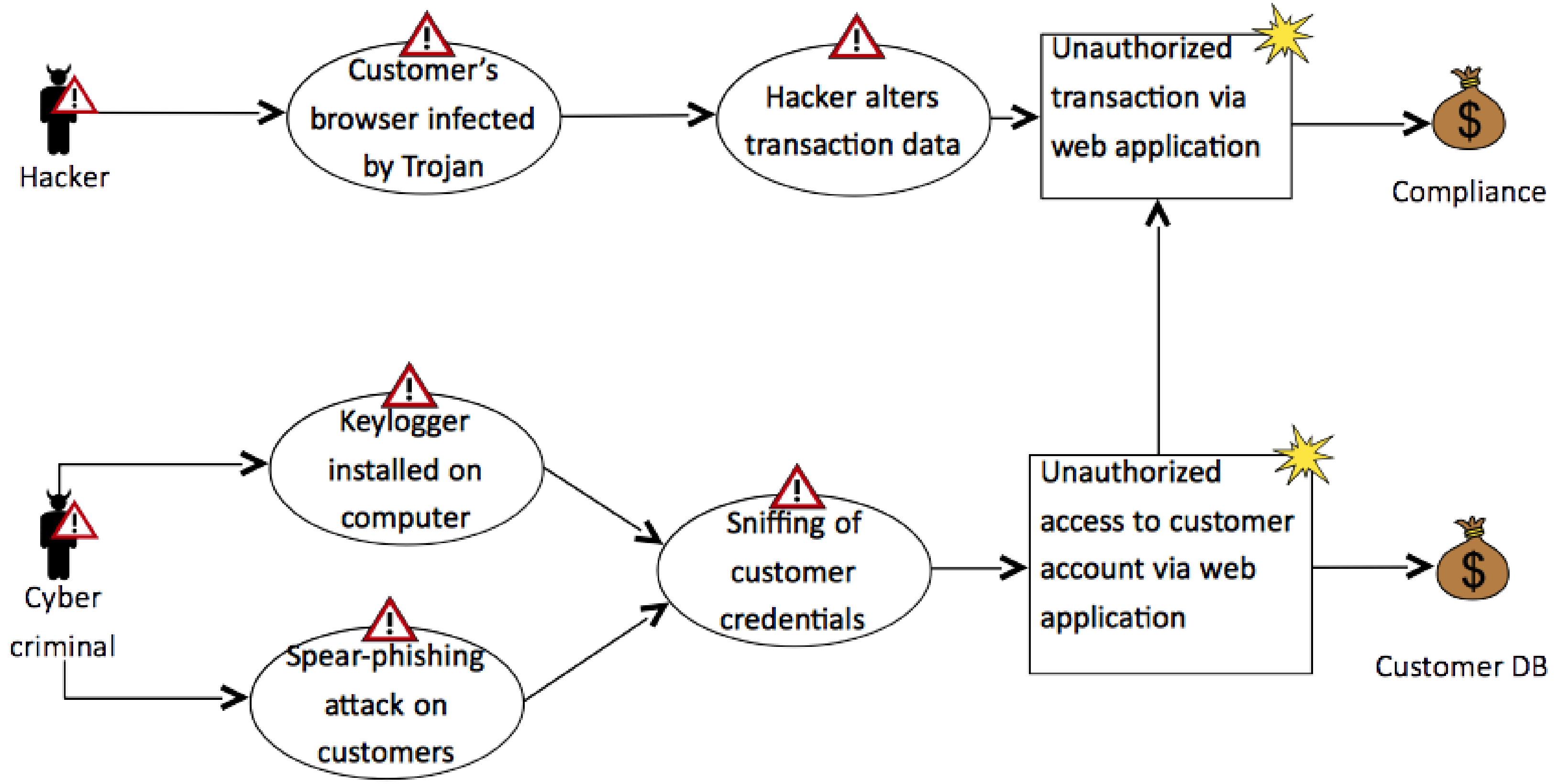
Online Banking

Customer DB

Compliance

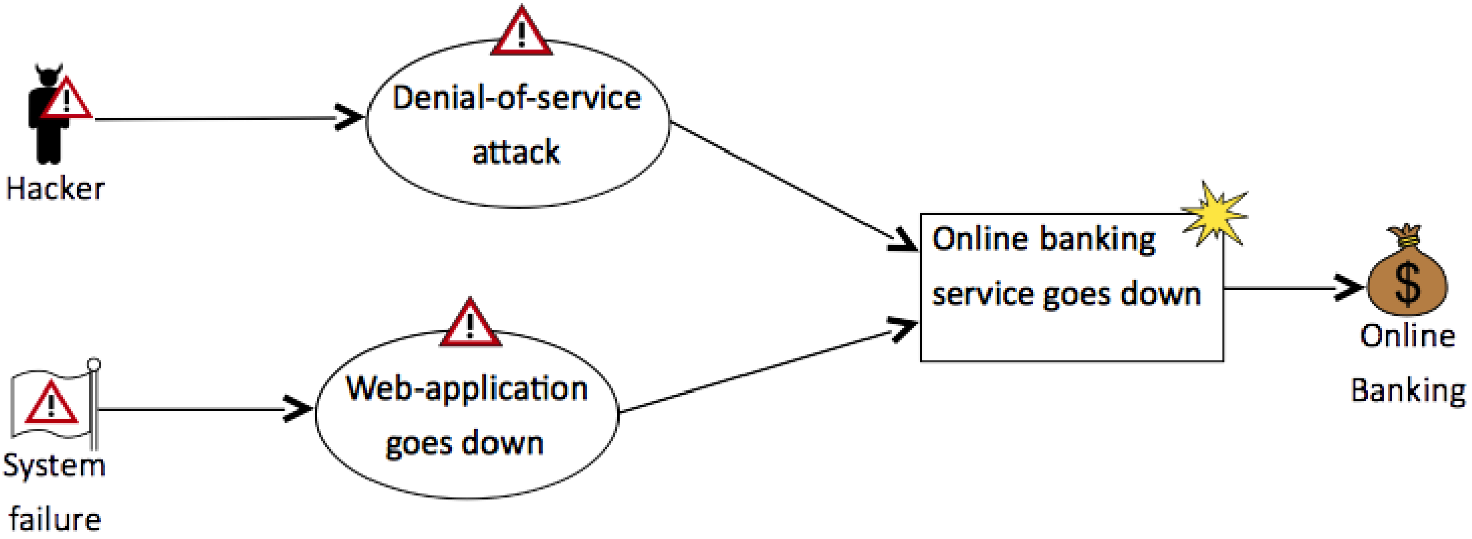
Step 5.3 Identify Threat Scenarios

- How does it happen?


Hacker
Customer's browser infected by Trojan
Hacker alters transaction data
Unauthorized transaction via web application
$
Compliance
Cyber criminal
Keylogger installed on computer
Spear-phishing attack on customers
Sniffing of customer credentials
Unauthorized access to customer account via web application
$
Customer DB

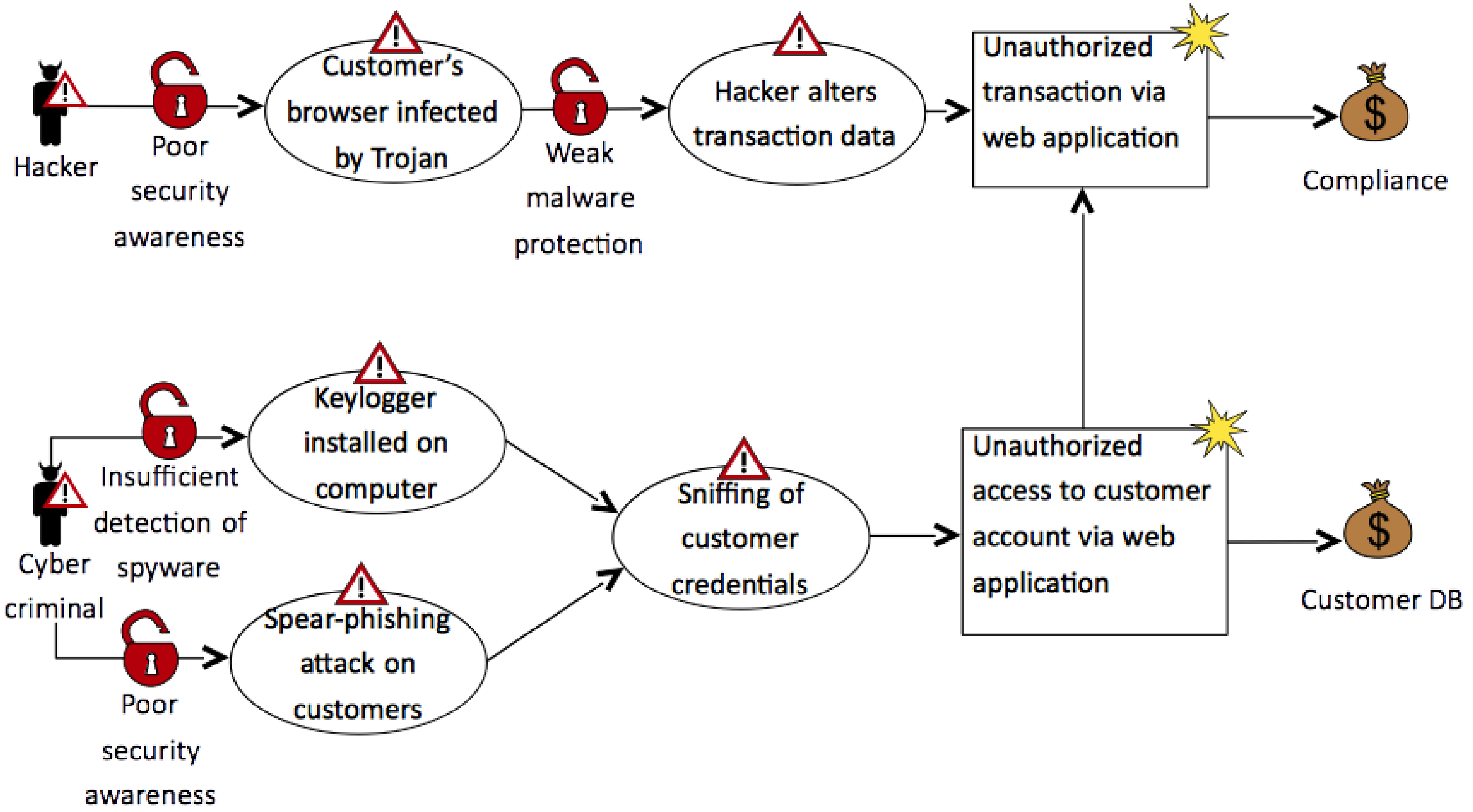
Step 5.3 Identify Threat Scenarios

- How does it happen?



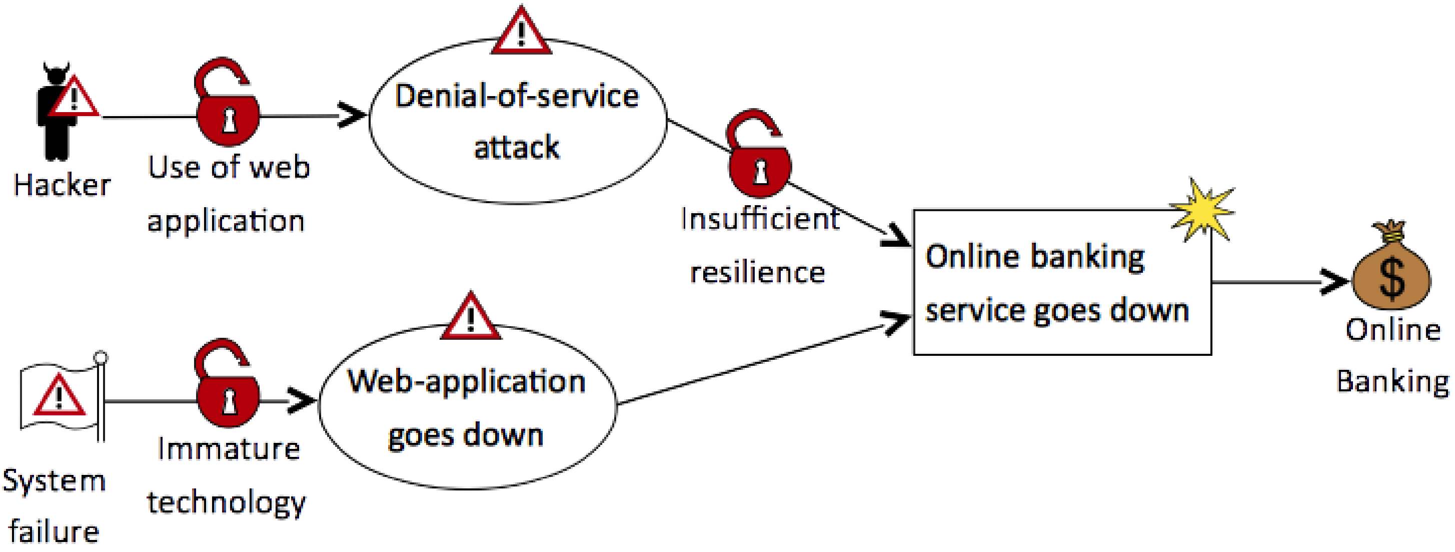
Step 5.4 Identify Vulnerabilities

- Which vulnerabilities make it possible?


Hacker
Poor security awareness
Customer's browser infected by Trojan
Weak malware protection
Hacker alters transaction data
Unauthorized transaction via web application
$
Compliance
Cyber criminal
Insufficient detection of spyware
Keylogger installed on computer
Poor security awareness
Spear-phishing attack on customers
Sniffing of customer credentials
Unauthorized access to customer account via web application
$
Customer DB

Step 5.4 Identify Vulnerabilities

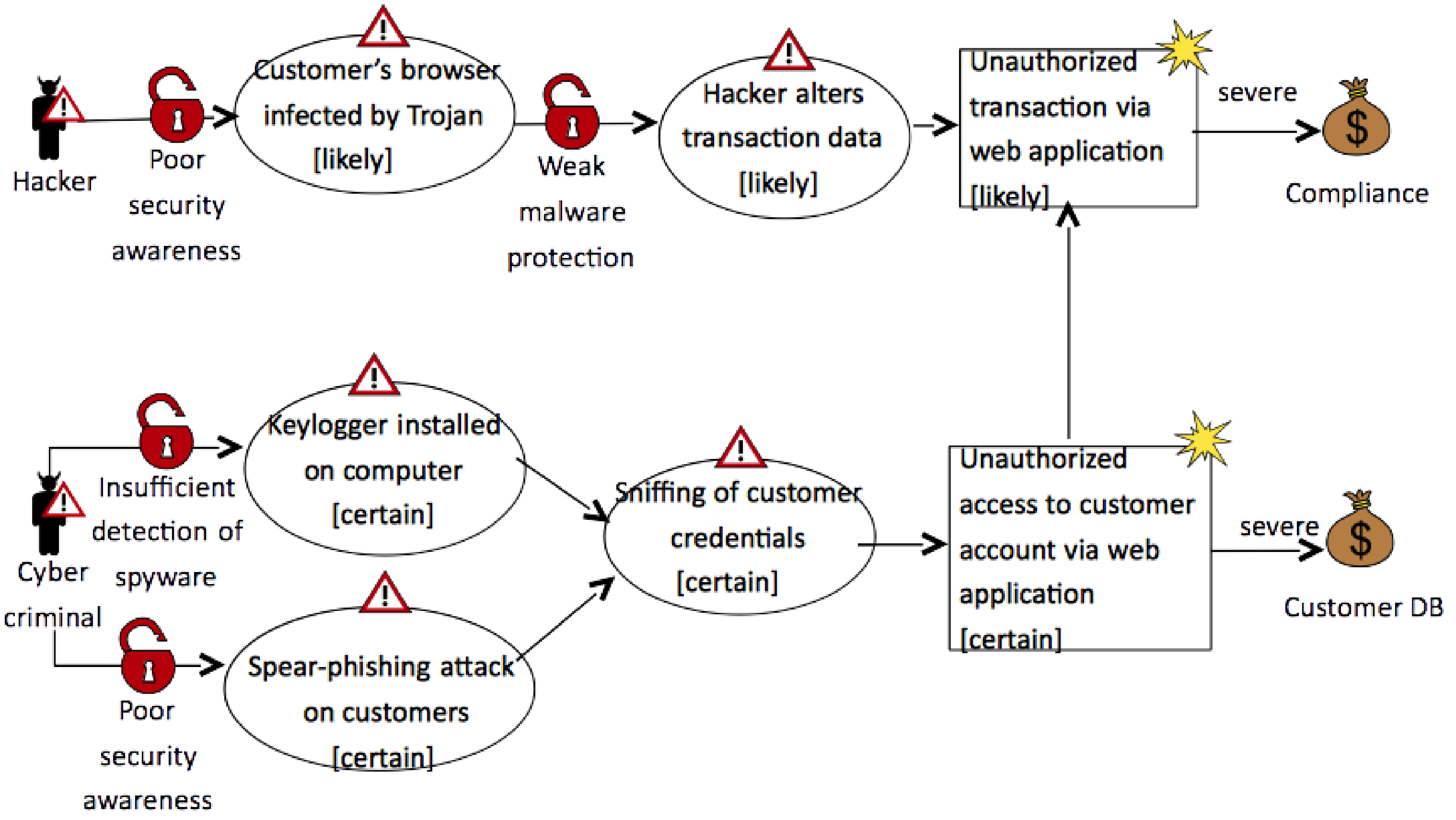
- Which vulnerabilities make it possible?



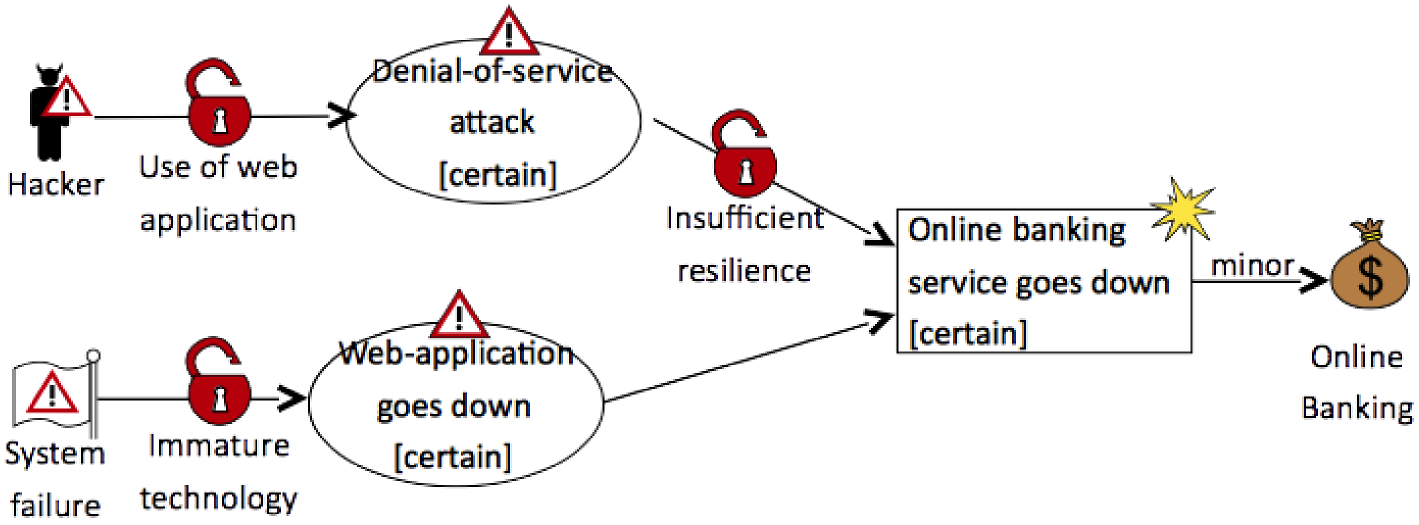
Step 6 Risk estimation

- **Objective**
  - determine level of the identified risks
- **Tasks**
  - Assign likelihood estimated for each Threat Scenario
  - Assign likelihood estimated for each Unwanted Incidents
  - Assign consequence caused by each Unwanted Incidents on each Asset (the consequence is denoted on “impact” relation)
- **Artifacts**
  - Threat diagrams with likelihood and consequences assigned

Example: Assign Likelihood and Consequence


Hacker
Poor security awareness
Customer's browser infected by Trojan [likely]
Weak malware protection
Hacker alters transaction data [likely]
Unauthorized transaction via web application [likely]
severe
Compliance
Cyber criminal
Insufficient detection of spyware
Keylogger installed on computer [certain]
Poor security awareness
Spear-phishing attack on customers [certain]
Sniffing of customer credentials [certain]
Unauthorized access to customer account via web application [certain]
severe
Customer DB

Example: Assign Likelihood and Consequence


Hacker
Use of web application
Denial-of-service attack [certain]
Insufficient resilience
Online banking service goes down [certain]
minor
Online Banking
System failure
Immature technology
Web-application goes down [certain]

Step 7 Risk evaluation

- **Objective**
  - Identify acceptable risks and risks that have to be treated
- **Tasks**
  - Map the risks into the Risk Function (from step 4)
  - Evaluate which risks are acceptable and which are not
  - Summarize the risk picture by Risk Diagram
- **Artifacts**
  - Completed Risk Function
  - Risk Diagram with evaluation result

Example: Risk Evaluation Matrix

Risk Function (Compliance)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Severe	Catastrophic
Rare	🟩	🟩	🟨	🟨	🟨
Unlikely	🟩	🟩	🟨	🟨	🟥
Possible	🟩	🟩	🟨	🟨	🟥
Likely	🟩	🟨	🟨	🟨 R1: Unauthorized transaction via web application	🟥
Certain	🟩	🟨	🟨	🟥	🟥

Example: Risk Evaluation Matrix

Risk Function (Customer DB)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Severe	Catastrophic
Rare	🟩	🟩	🟨	🟥	🟥
Unlikely	🟩	🟩	🟨	🟥	🟥
Possible	🟩	🟩	🟨	🟥	🟥
Likely	🟩	🟨	🟨	🟥	🟥
Certain	🟩	🟨	🟥	🟥 R2: Unauthorized access to customer account via web application	🟥

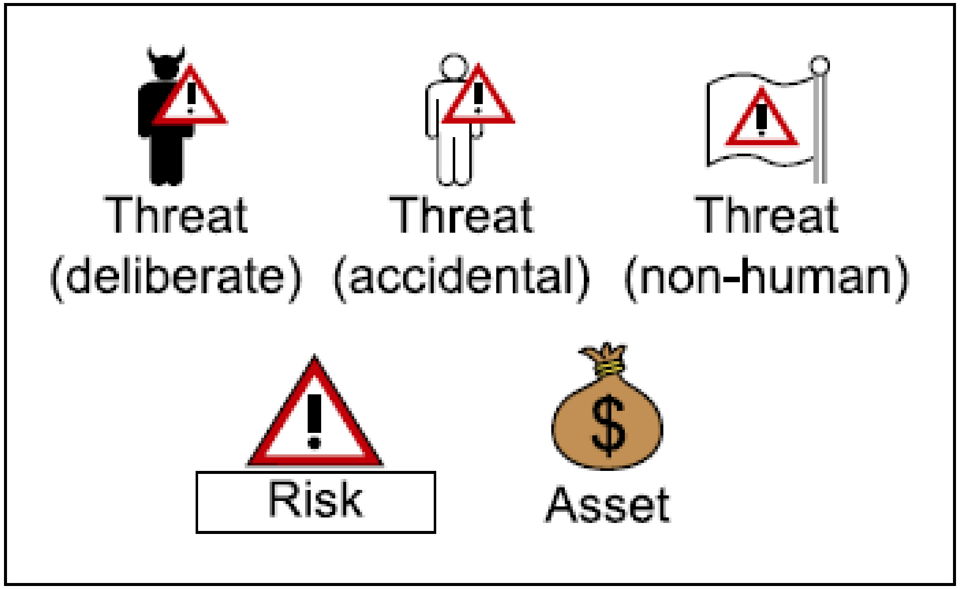
Example: Risk Evaluation Matrix

Risk Function (Online Banking)					
Consequence/ Likelihood	**Insignificant**	**Minor**	**Moderate**	**Severe**	**Catastrophic**
Rare	🟩	🟩	🟨	🟨	🟥
Unlikely	🟩	🟩	🟨	🟨	🟥
Possible	🟩	🟩	🟨	🟥	🟥
Likely	🟩	🟨	🟨	🟥	🟥
Certain	🟩	R3: Online Banking Service Goes Down	🟥	🟥	🟥

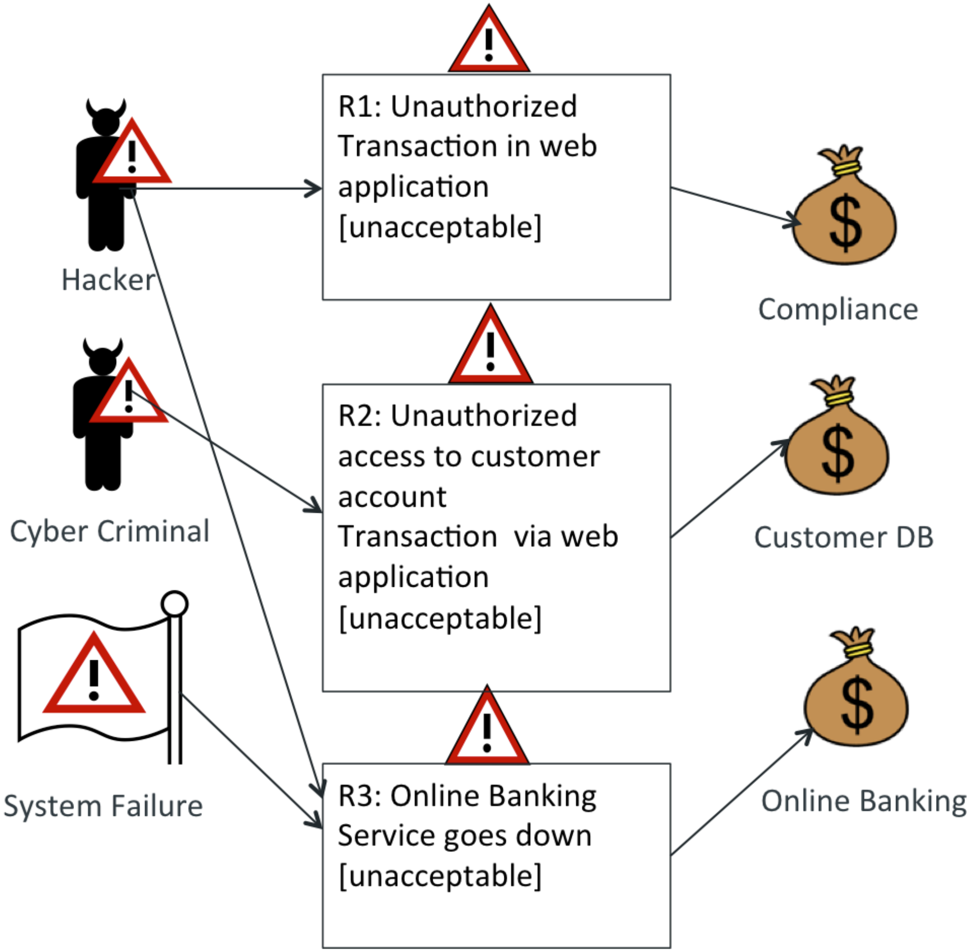
Summarizing the Risk picture

- We use Risk diagram to show how Threats pose Risks to the Assets

- Notations to be used in Risk diagram:



Example: Risk Diagram



R1: Unauthorized Transaction in web application [unacceptable]

R2: Unauthorized access to customer account Transaction via web application [unacceptable]

R3: Online Banking Service goes down [unacceptable]

Step 8 Risk treatment

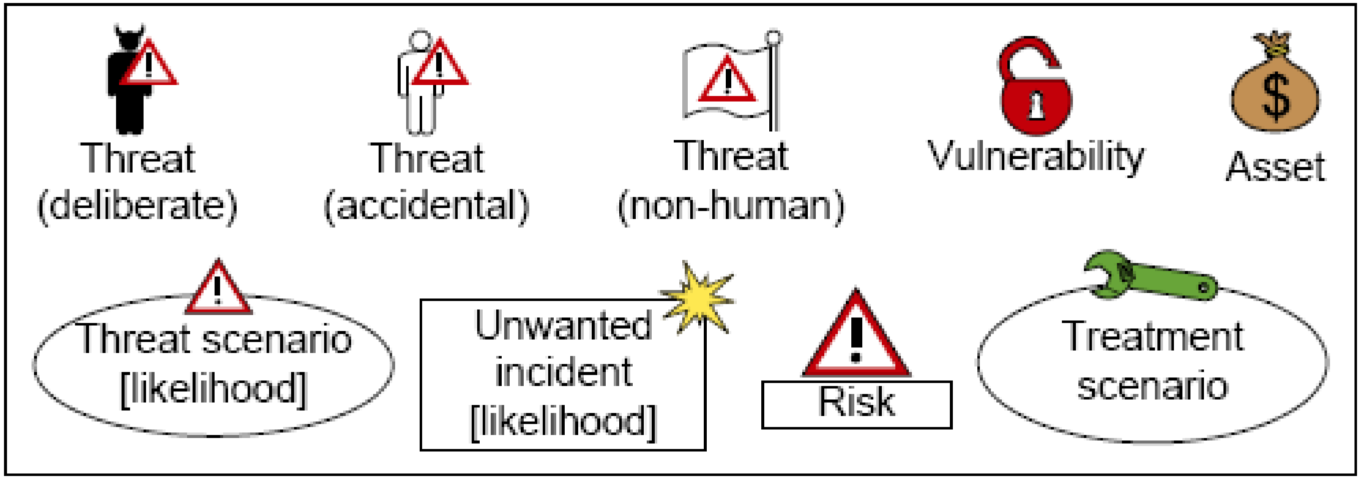
- **Objective**
  - identify cost effective treatments for the unacceptable risks
- **Task**
  - Identify Treatment Scenario for unacceptable risks
  - Create Treatment diagram
  - Summarize by Treatment Overview diagram
  - Estimate the cost-benefit of each treatment
- **Artifacts**
  - Treatment diagram (Threat diagram with Treatment added)

Step 8 Risk treatment

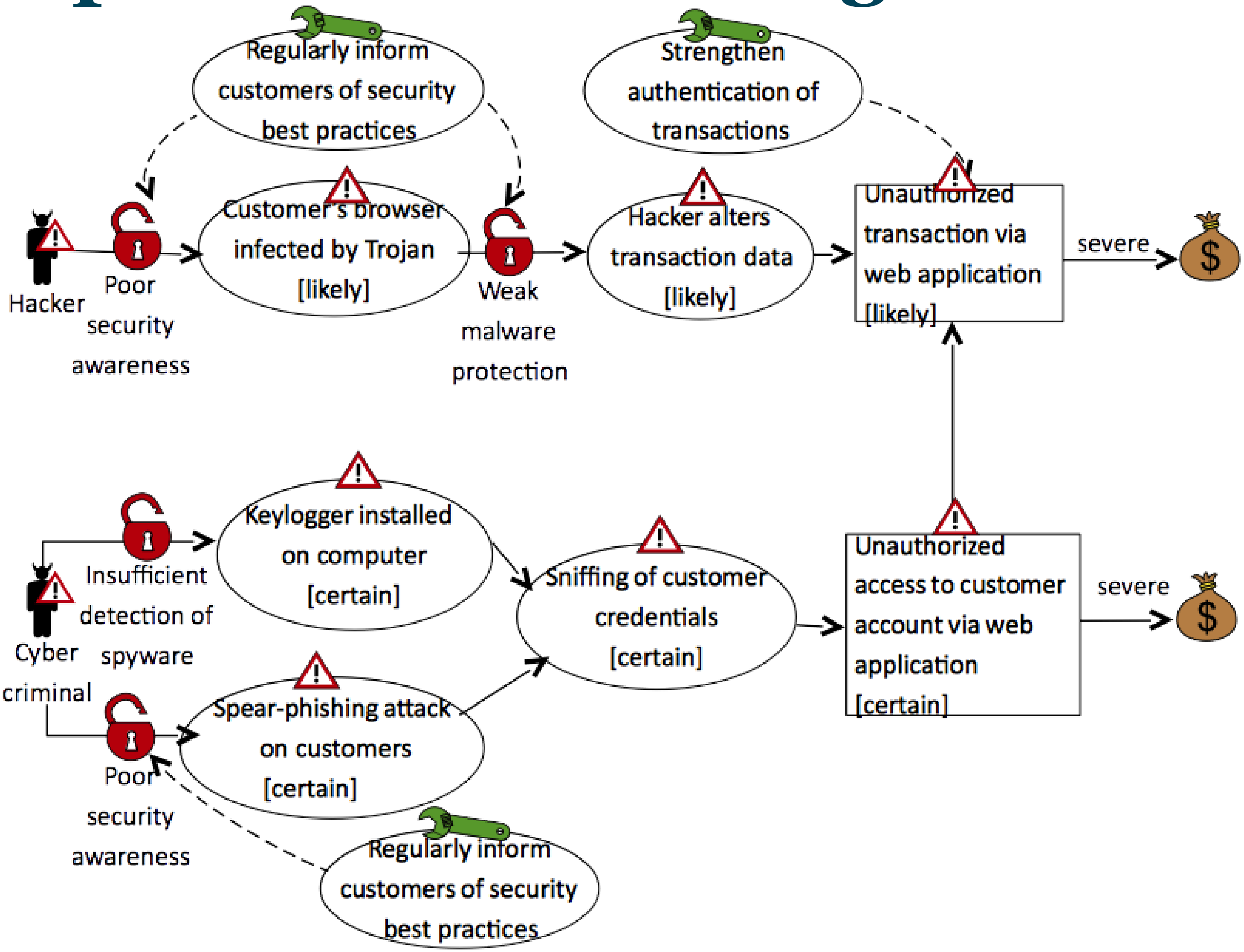
- Type of Treatments
  - **Administrative**
    - Define security responsibilities, security awareness training, audit
  - **Technical**
    - Authentication, access control, encryption, anti-virus
  - **Physical**
    - Locks, fences, alarm systems

Step 8 Risk treatment

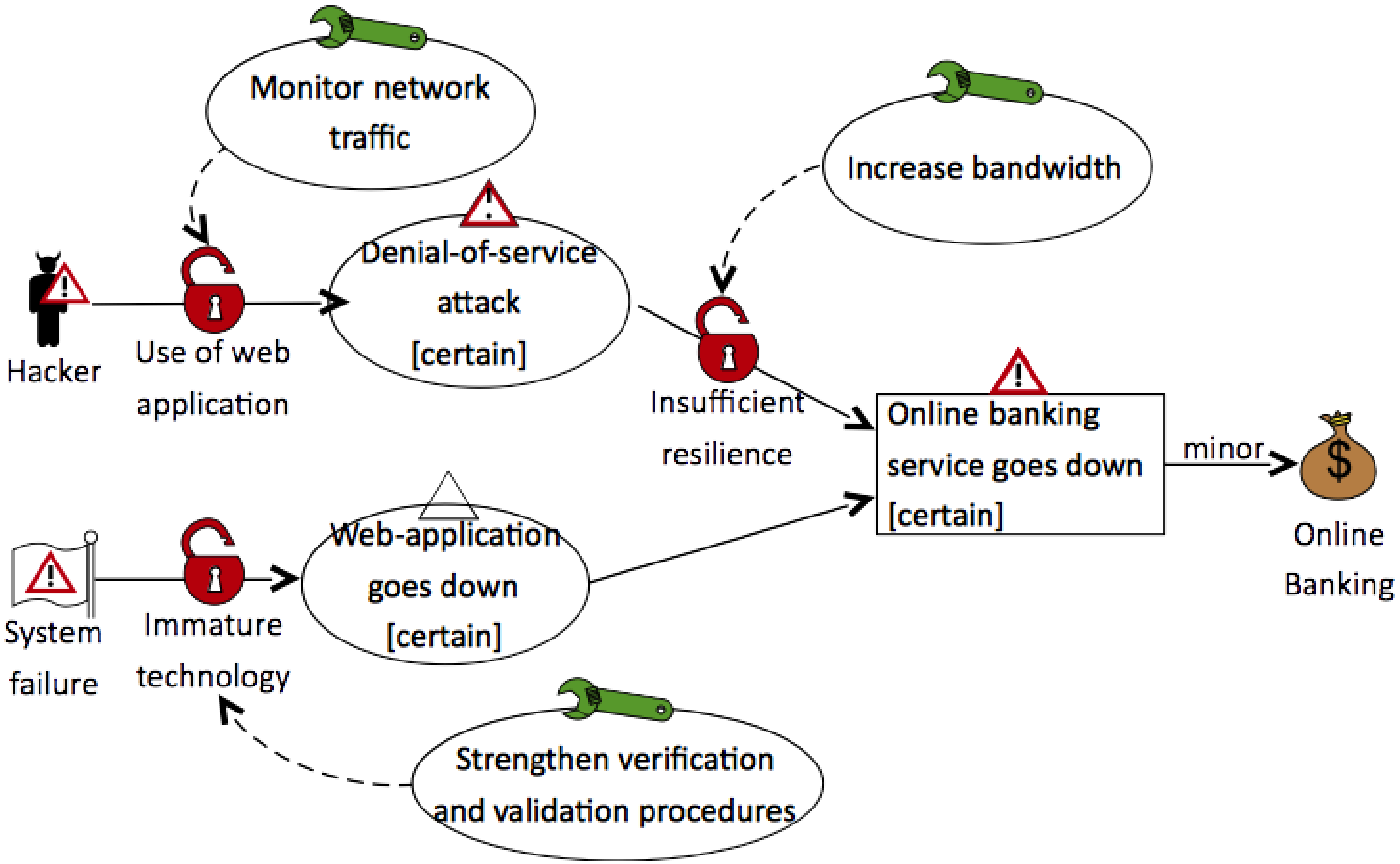
- Notations to be used in Treatment Diagram



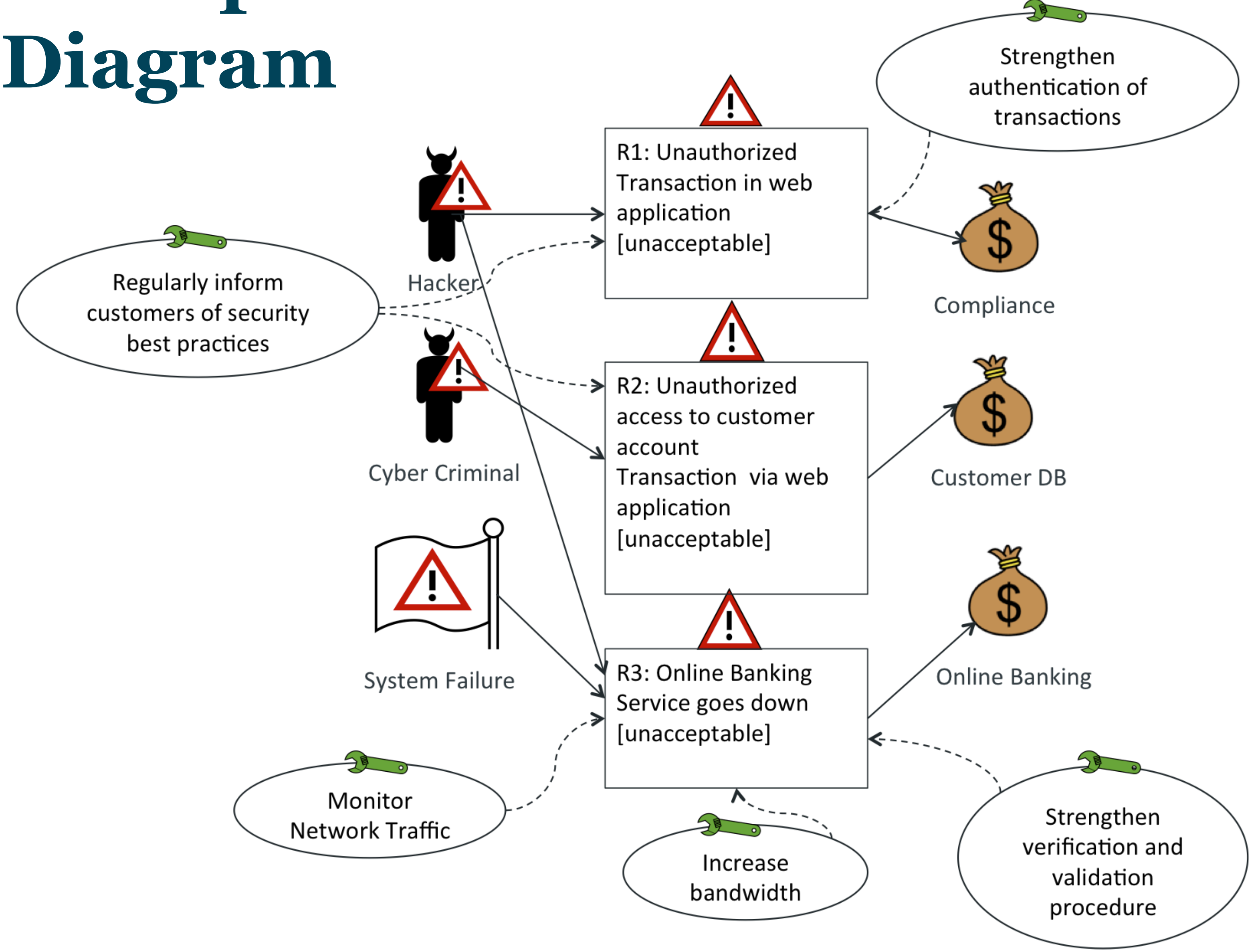
Example: Treatment Diagram


Regularly inform customers of security best practices
Strengthen authentication of transactions
Hacker
Poor security awareness
Customer's browser infected by Trojan [likely]
Weak malware protection
Hacker alters transaction data [likely]
Unauthorized transaction via web application [likely]
severe
$
Cyber criminal
Insufficient detection of spyware
Keylogger installed on computer [certain]
Sniffing of customer credentials [certain]
Unauthorized access to customer account via web application [certain]
severe
$
Poor security awareness
Spear-phishing attack on customers [certain]
Regularly inform customers of security best practices

Example: Treatment Diagram


Monitor network traffic
Increase bandwidth
Hacker
Use of web application
Denial-of-service attack [certain]
Insufficient resilience
Online banking service goes down [certain]
minor
Online Banking
System failure
Immature technology
Web-application goes down [certain]
Strengthen verification and validation procedures

Example: Treatment Overview Diagram



Strengthen authentication of transactions

R1: Unauthorized Transaction in web application [unacceptable]

Compliance

Regularly inform customers of security best practices

R2: Unauthorized access to customer account Transaction via web application [unacceptable]

Customer DB

R3: Online Banking Service goes down [unacceptable]

Online Banking

Monitor Network Traffic

Increase bandwidth

Strengthen verification and validation procedure

Treatment Evaluation

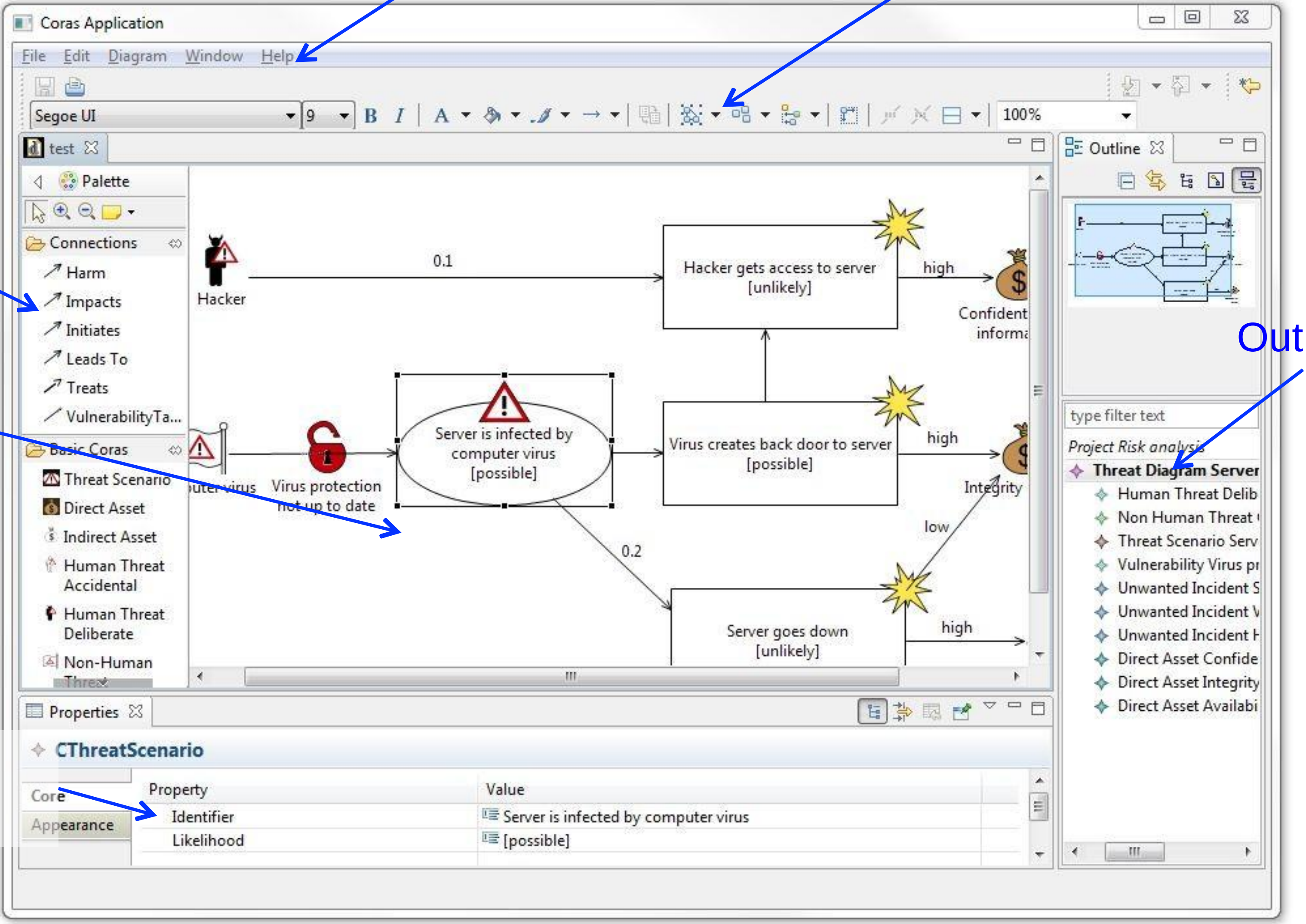
- Estimate the cost-benefit of each treatment and decide which ones to implement

Treatment	Cost	Risk	Risk reduction	Select to implement
….	…	…	…	…
…	…	…	…	…
…	…	…	…	…

Example: Treatment Evaluation

Treatment	Cost	Risk	Risk reduction	Select to implement
Strengthen Authentication of Transaction	Low	R1	Unacceptable to Monitor	No
Regularly Inform Customers of Security Best Practices	Low	R1	Unacceptable to Acceptable	Yes
		R2	Unacceptable to Acceptable	
Monitor Traffic	High	R3	Unacceptable to Acceptable	Yes
Increase bandwidth	Medium	R3	Unacceptable to Acceptable	Yes
Strengthen validation and verification procedure	Medium	R3	Unacceptable to Monitor	No

CORAS Tool



Pull-down menu

Tool bar

Palette

Canvas

Outline

Properties window

CThreatScenario

Property	Value
Identifier	Server is infected by computer virus
Likelihood	[possible]

Summary

- CORAS consists of three parts
  - Method
  - Language
  - Tool
- Model-driven and asset-driven
- Concrete guidelines for how to conduct risk analysis in practice
- Based on internationally established standards

Reading Material

- M.Lund, B.Solhaug, K.Stolen, Model-Driven Risk Analysis: The CORAS approach. Springer 2011.

  Chapter 3 – A Guided Tour of the CORAS Method.

Available for download from the module notes wiki