The CORAS approach to model-driven risk analysis

RISE presentation

May 13, 2011

Atle Refsdal, SINTEF

Outline

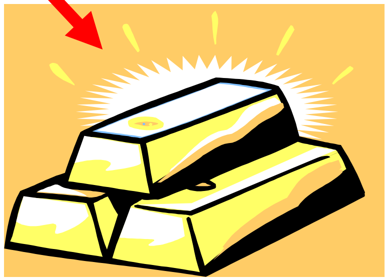
- General introduction
  - what is risk analysis, definition of terms, …
- Overview of the CORAS process and risk modeling language
- The eight steps of a CORAS risk analysis
- Small demo/exercise?

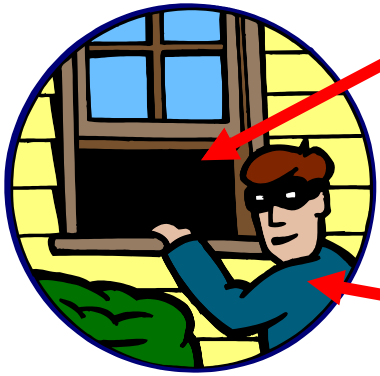
What is risk analysis?

- Determining what can happen, why and how
- Systematic use of available information to determine the level of risk
- Prioritisation by comparing the level of risk against predetermined criteria
- Selection and implementation of appropriate options for dealing with risk

Terms

asset, something of value





vulnerability

threat

reduced security risk

Risk with respect to security

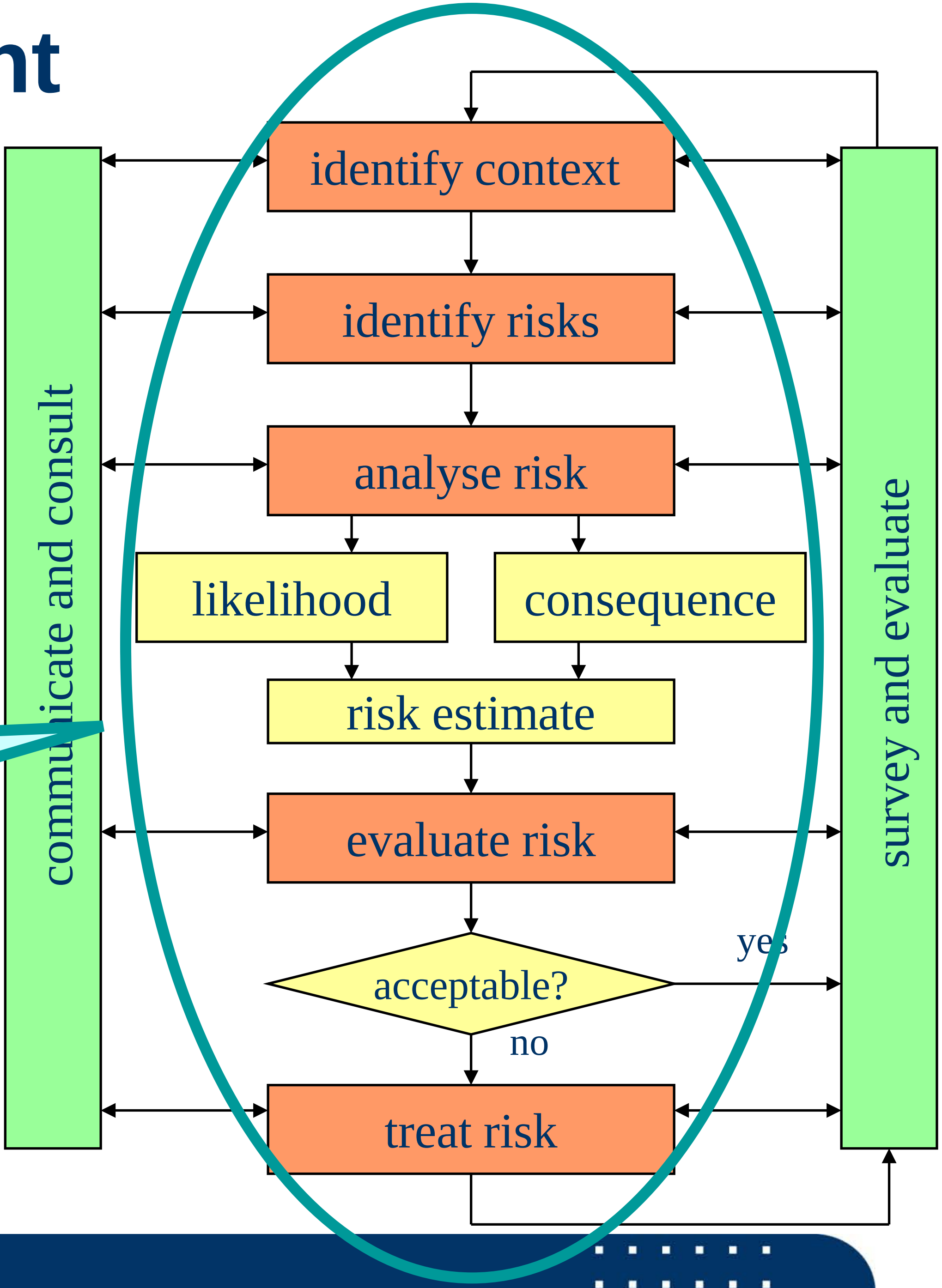
need to introduce security mechanisms

Definition of Terms

- **Asset:** Something to which a party assigns value and hence for which the party requires protection
- **Consequence:** The impact of an unwanted incident on an asset in terms of harm or reduced asset value
- **Likelihood:** The frequency or probability of something to occur
- **Party:** An organization, company, person, group or other body on whose behalf a risk analysis is conducted
- **Risk:** The likelihood of an unwanted incident and its consequence for a specific asset
- **Threat:** A potential cause of an unwanted incident
- **Threat scenario:** A chain or series of events that is initiated by a threat and that may lead to an unwanted incident
- **Treatment:** An appropriate measure to reduce risk level
- **Unwanted incident:** An event that harms or reduces the value of an asset
- **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

Risk management

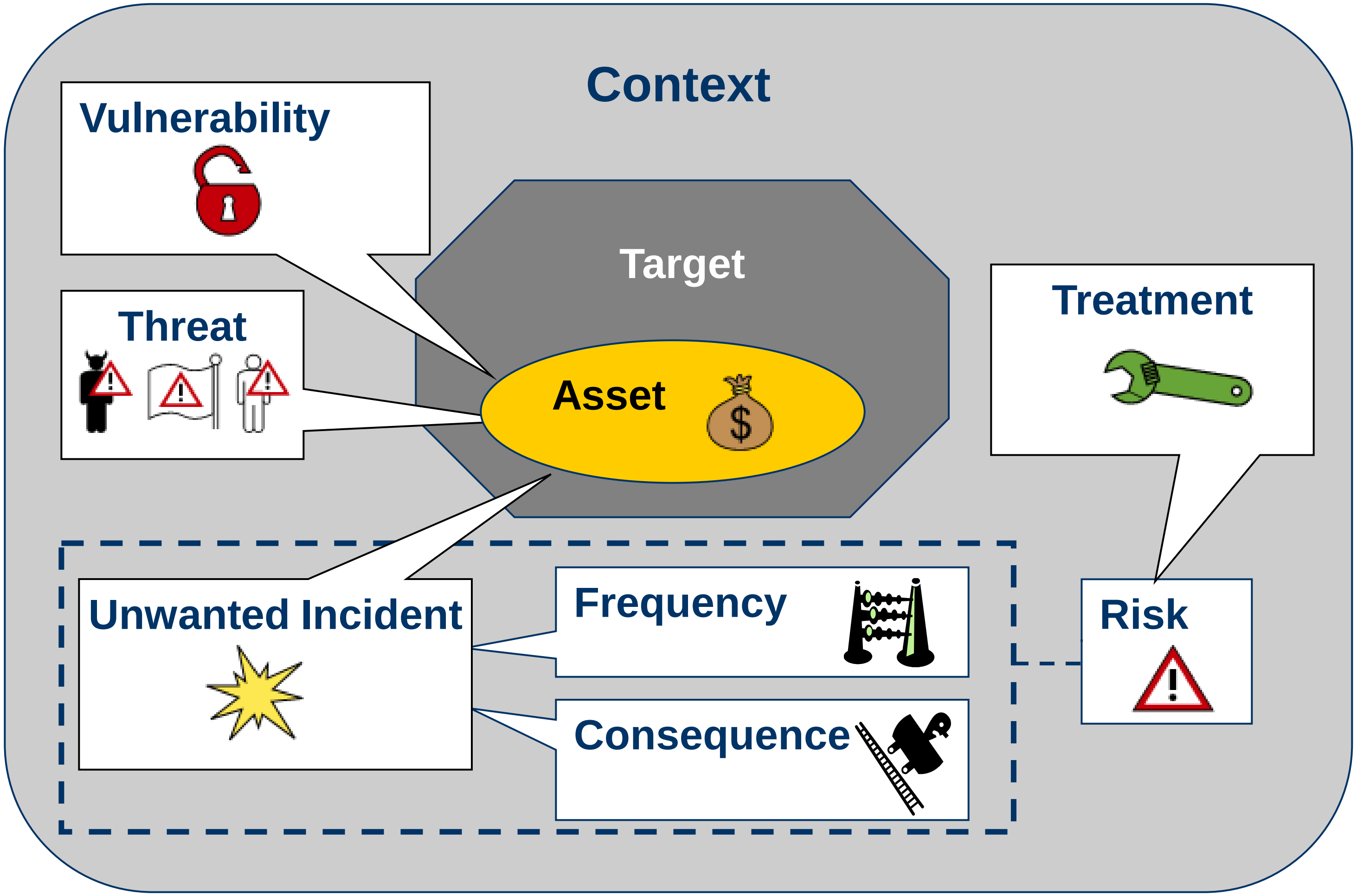
Risk management is the culture, processes and structures that are directed towards
realizing potential opportunities whilst managing adverse effects



Our focus:

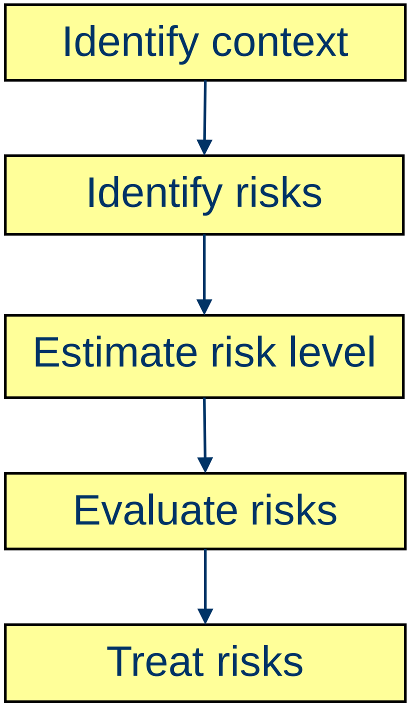
Risk Analysis

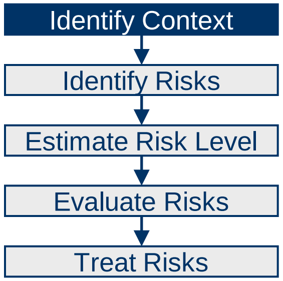
Elements of risk analysis



The CORAS process

- Risk management process based on **ISO 31000: Risk Management – Principles and Guidelines**
- Provides *process* and *guidelines* for risk analysis




Identify Context

Identify Risks

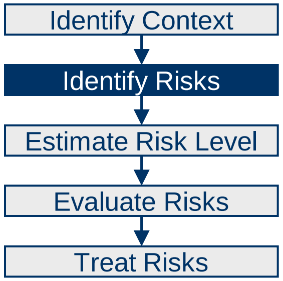
Estimate Risk Level

Evaluate Risks

Treat Risks

Context identification

- Characterise target of analysis
  - What is the focus and scope of the analysis?
- Identify and value assets
  - Asset-driven risk analysis process
  - Business oriented, e.g. availability of services generating revenue
- Specify risk evaluation criteria
  - There will always be risks, but what losses can the client tolerate?
  - Similar to requirements in system development



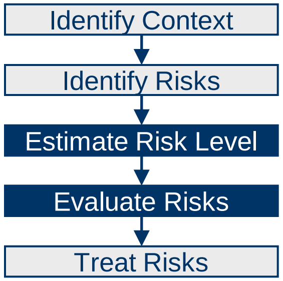
Risk identification

- Identify threats to assets through structured brainstorming
  - Hazard and Operability analysis (HazOp)
  - Involving system owners, users, developers, domain experts, risk analysis experts, etc. (typically 5-7 people)

- Identify vulnerabilities of assets
  - Questionnaires and checklists

Equipment physical security

- Is equipment properly physically protected against unauthorised access to data or loss of data?
- Are power supplies handled in a manner that prevents loss of data and ensures availability?
- …

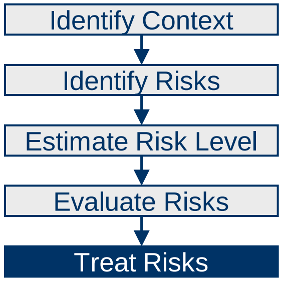


Risk evaluation

- We cannot completely eliminate all risks
- Determine which risks need treatment
  - We need to know how serious they are so we can prioritise

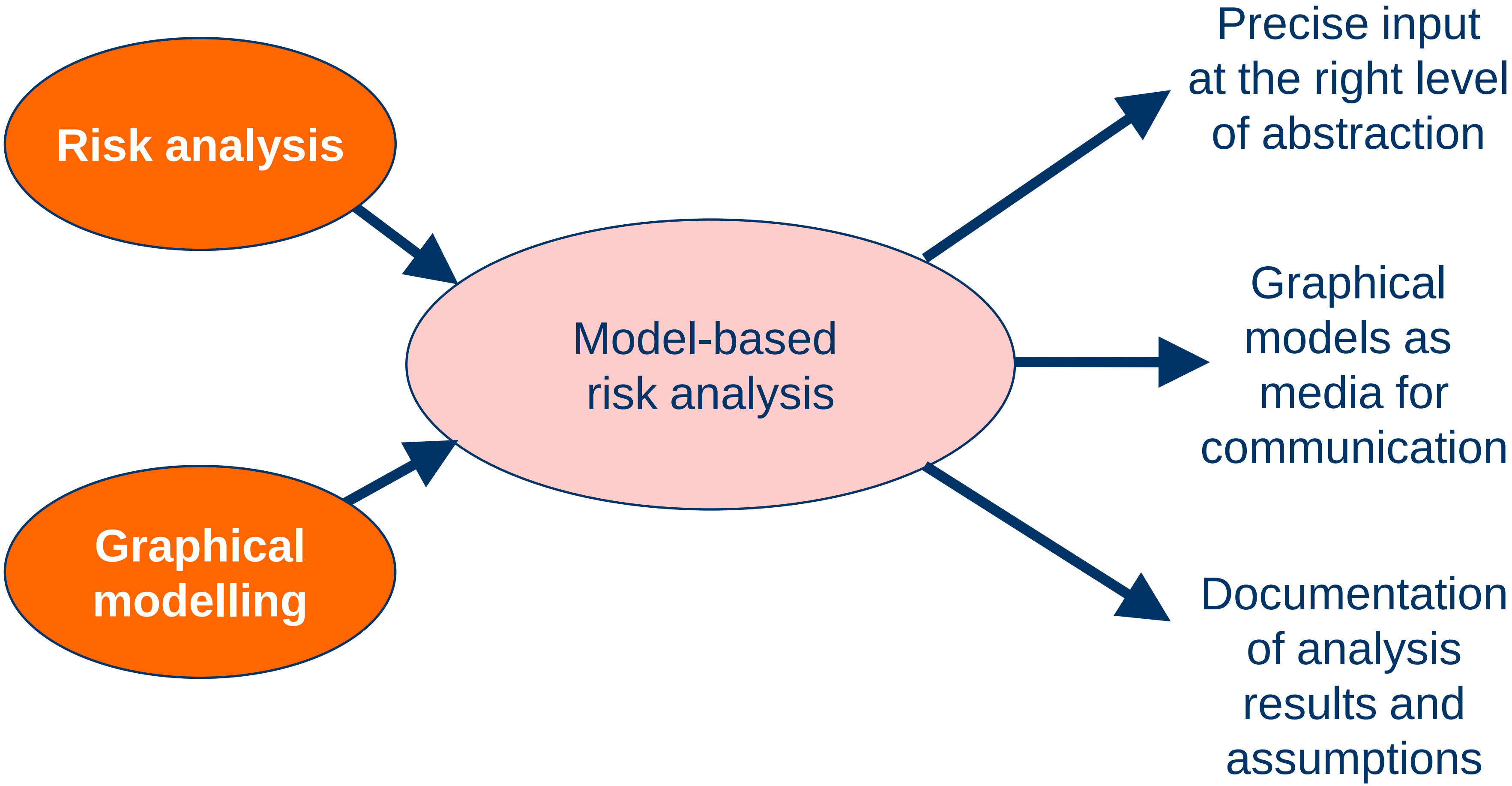
- Risk level is determined based on analysis of the likelihood and consequence of the unwanted incident
  - Quantitative values: e.g., loss of 1M€, 25% chance per year
  - Qualitative values: e.g., high, medium, low

Risk treatment



- Identify treatments for unaccepted risks
- Evaluate and prioritise different treatments

Model-based risk analysis



Risk analysis

Graphical modelling

Model-based risk analysis

Precise input at the right level of abstraction

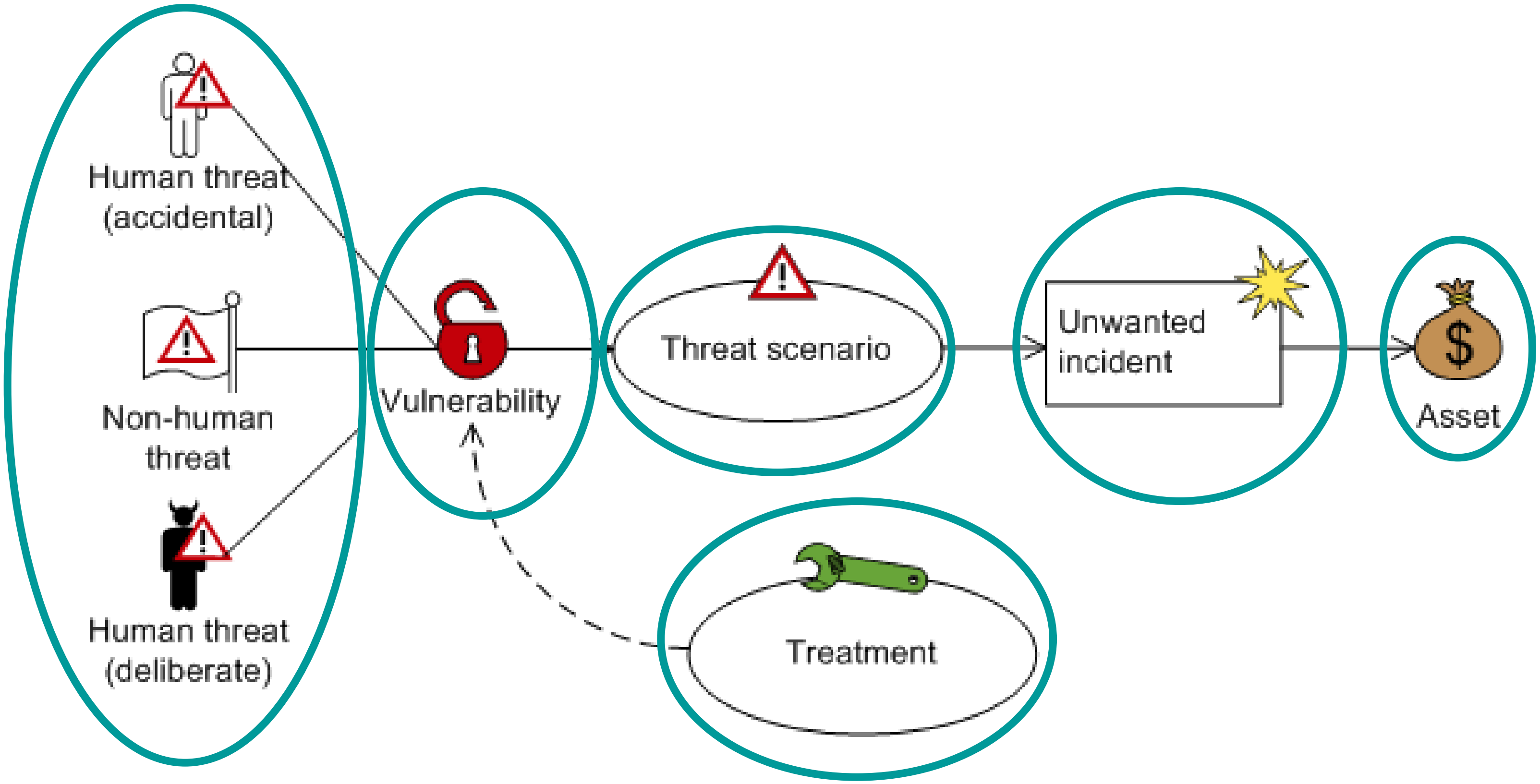
Graphical models as media for communication

Documentation of analysis results and assumptions

What is CORAS?

- The CORAS process
  - A process for security risk analysis
- The CORAS language (diagrams)
  - A graphical language that supports the analysis process
  - Basis for communication, documentation and analysis
- The CORAS semantics
  - A schematic translation of any CORAS diagram into English
- The CORAS guideline
  - A guideline for best use of the language within the process
- The CORAS tool
  - A computerized tool supporting the above

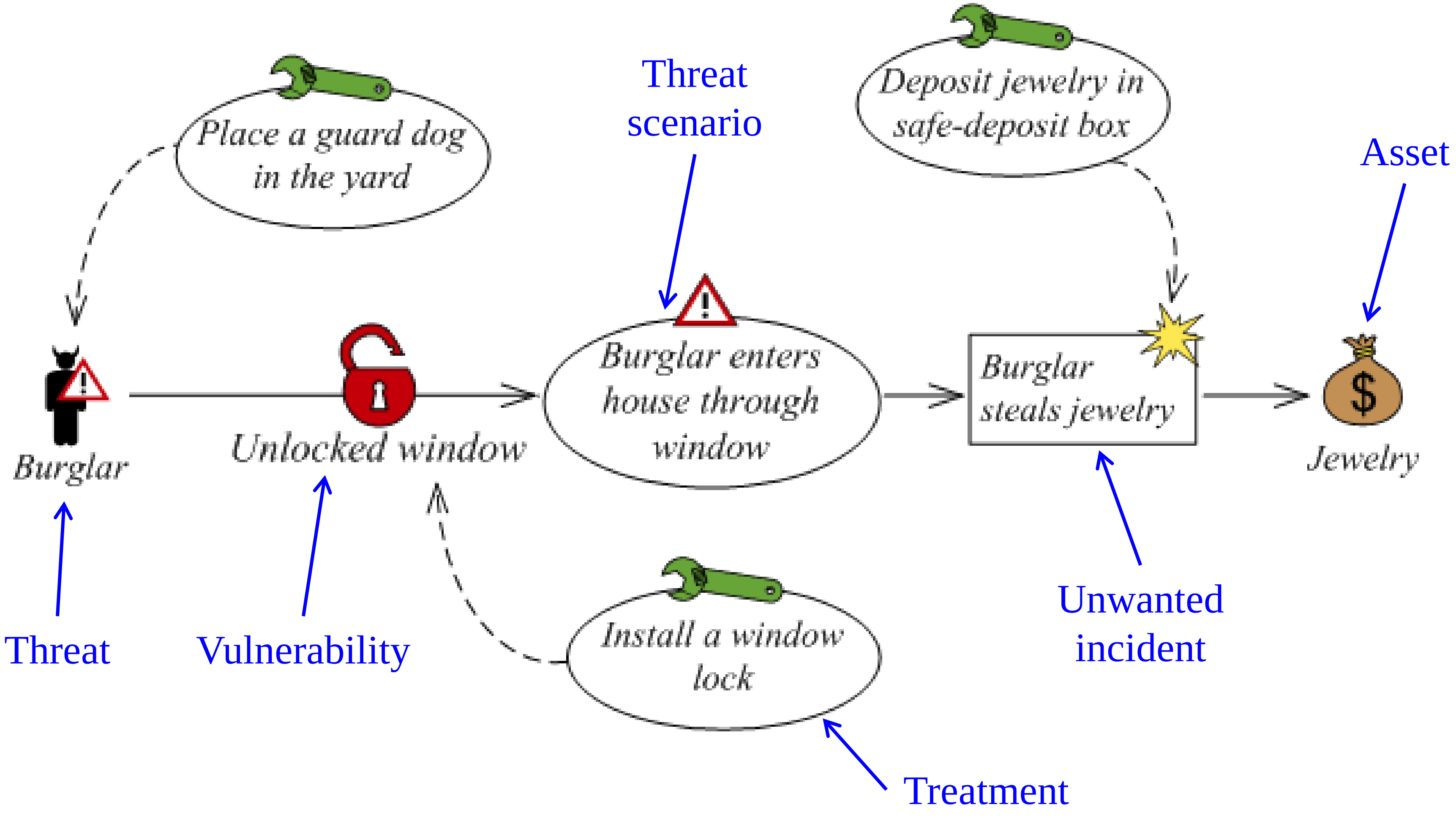
The CORAS language



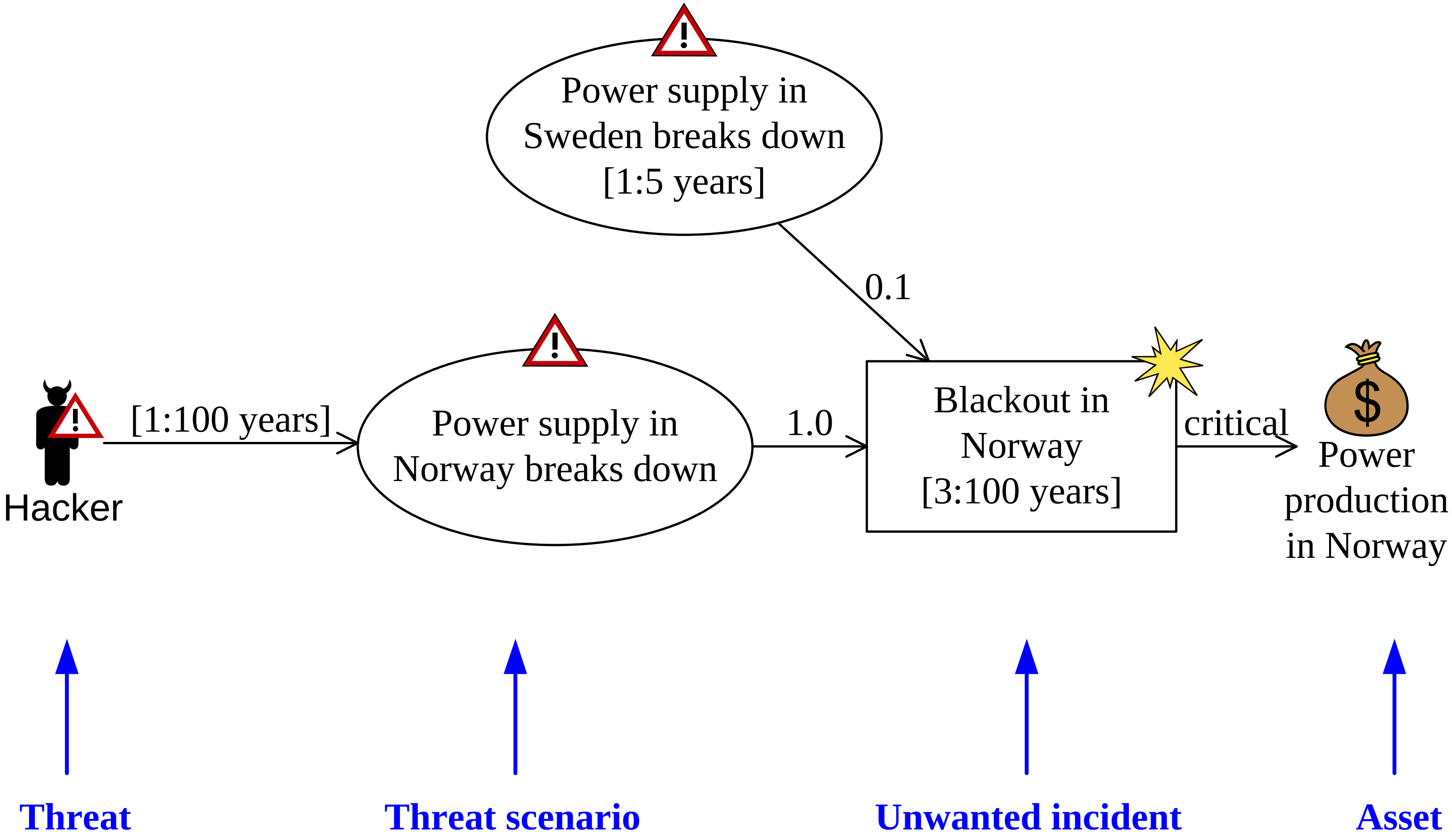
The CORAS diagrams

- **Asset diagrams**
  Describes the focus of the analysis
- **Threat diagrams**
  Describes scenarios which may cause harm to the assets
- **Risk diagrams**
  Summarises the risks presented in threat diagrams
- **Treatment diagrams**
  Adds proposed treatments to threat diagrams
- **Treatment overview diagrams**
  Adds proposed treatments to risk diagrams

Threat Diagram – Example 1



Threat Diagram – Example 2



Power supply in Sweden breaks down [1:5 years]

0.1

Hacker

[1:100 years]

Power supply in Norway breaks down

1.0

Blackout in Norway [3:100 years]

critical

Power production in Norway

Threat

Threat scenario

Unwanted incident

Asset

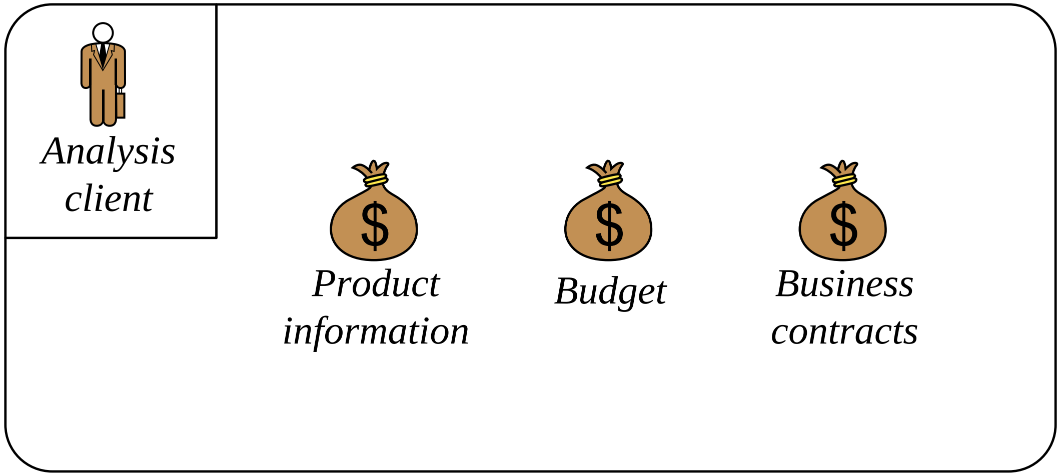
Semantics: Translation into English

- Vertices
  - *Hacker* is a deliberate human threat.
  - Threat scenario *Power supply in Norway breaks down* occurs with undefined likelihood.
  - Threat scenario *Power supply in Sweden breaks down* occurs with likelihood *1:5 years*.
  - Unwanted incident *Blackout in Norway* occurs with likelihood *3:100 years*.
  - *Power production in Norway* is a direct asset.

- Relations
  - *Hacker* initiates *Power supply in Norway breaks down* with likelihood *1:100 years*.
  - *Power supply in Norway breaks down* leads to *Blackout in Norway* with conditional likelihood *1.0*.
  - *Power supply in Sweden breaks down* leads to *Blackout in Norway* with conditional likelihood *0.1*.
  - *Blackout in Norway* impacts *Power production in Norway* with consequence *critical*.

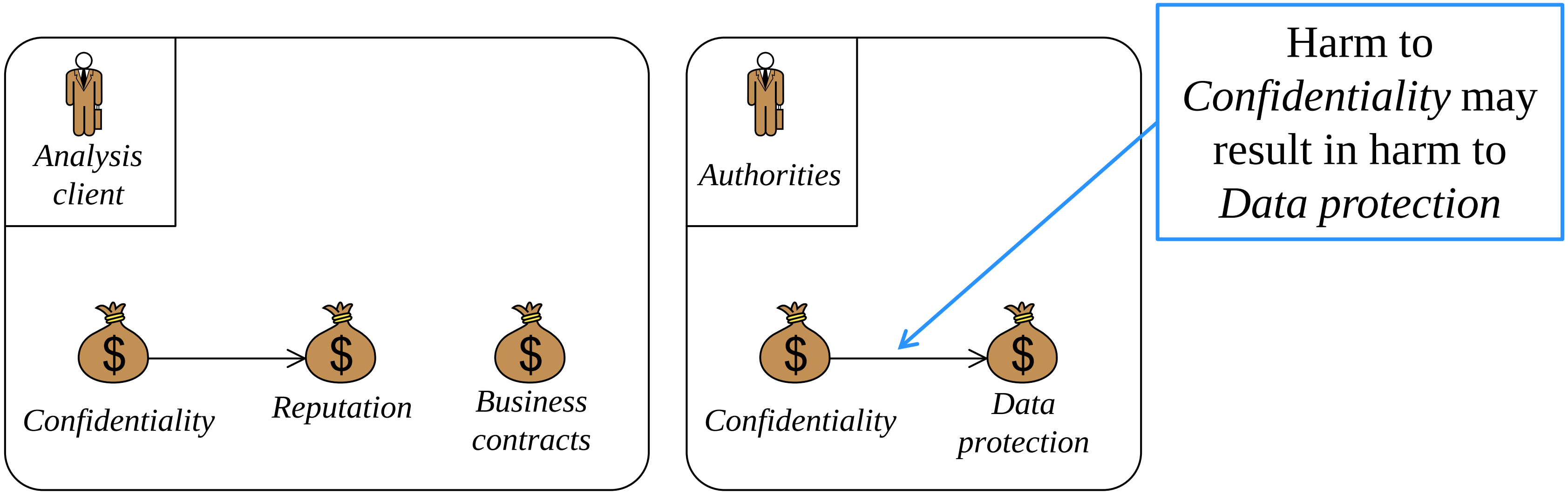
Identifying and documenting assets

- Asset: *Something to which a party assigns value and hence for which the party requires protection*
- The client specifies its assets and risk acceptance levels
- Difficult, - faults may jeopardize the whole analysis
  - wrong focus
  - wrong level of details



Identifying and documenting assets

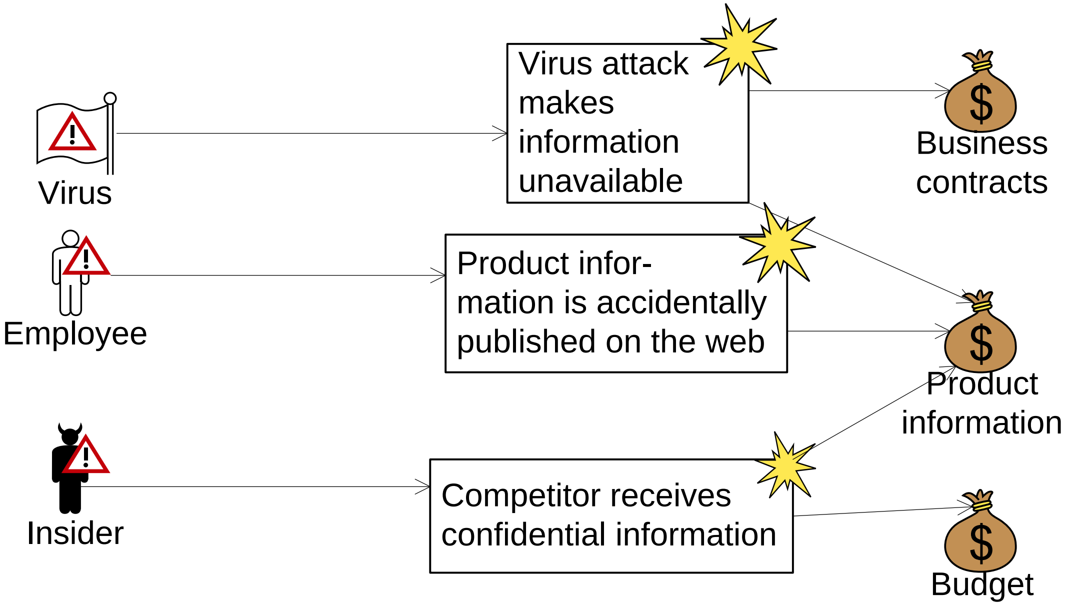
- One may also specify other interested parties than the client
  - Different parties may have different assets
  - Two parties may assign value to the same parts or aspects (e.g. confidentiality), but possibly with different priority (asset value) and different protection requirements
- Possible to specify how assets can depend on other assets
  - company reputation
  - income



Harm to *Confidentiality* may result in harm to *Data protection*

Identifying and documenting threats and unwanted incidents in threat diagrams

- **Threat**: *A potential cause of an unwanted incident*
- **Unwanted incident**: *An event that harms or reduces the value of an asset*

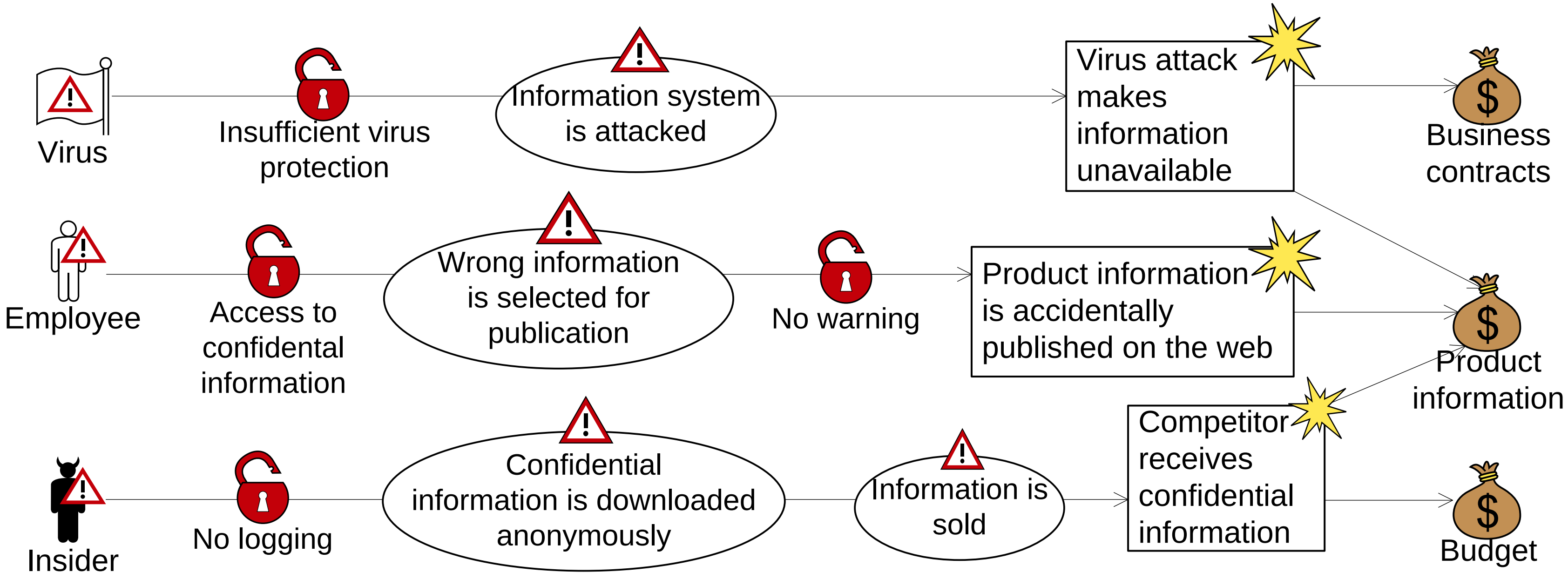


Virus
Employee
Insider
Virus attack makes information unavailable
Product information is accidentally published on the web
Competitor receives confidential information
Business contracts
Product information
Budget

Threat	*Unwanted incident*	*Asset damaged*
Virus	Virus attack makes information unavailable	Business contracts
Virus	Virus attack makes information unavailable	Product information
Employee	Product information is accidentally published on the web	Product information
Insider	Competitor receives confidential information	Product information
Insider	Competitor receives confidential information	Budget

Identifying and documenting vulnerabilities and threat scenarios

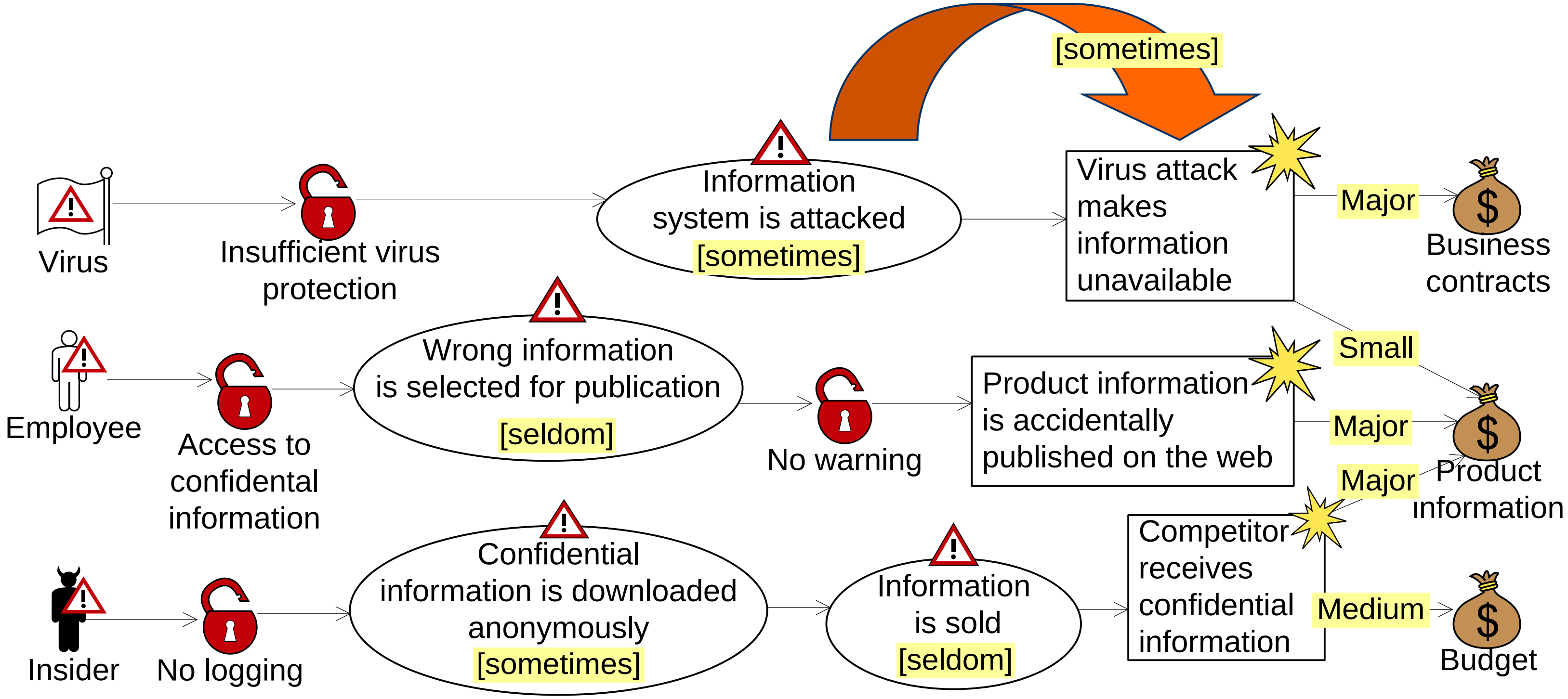
- **Vulnerability**: *A weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset*
- **Threat scenario**: *A chain or series of events that is initiated by a threat and that may lead to an unwanted incident*
- Forces the participants to specify “why” incidents can happen (vulnerabilities) and “how” (threat scenarios)



Virus
Insufficient virus protection
Information system is attacked
Virus attack makes information unavailable
Business contracts
Employee
Access to confidental information
Wrong information is selected for publication
No warning
Product information is accidentally published on the web
Product information
Insider
No logging
Confidential information is downloaded anonymously
Information is sold
Competitor receives confidential information
Budget

Identifying and documenting likelihoods and consequences

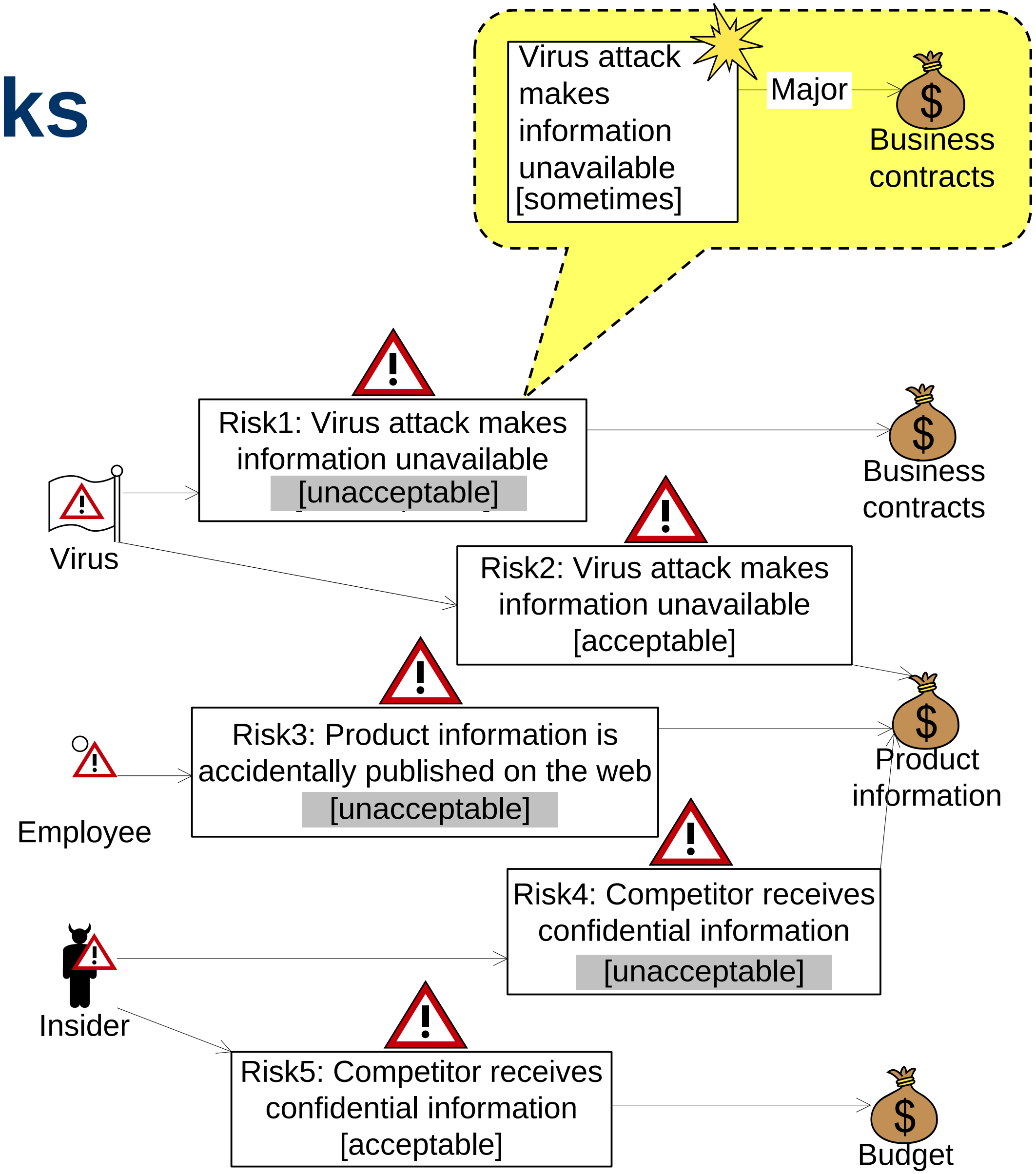
- **Likelihood:** *The frequency or probability of something to occur*
- **Consequence:** *The impact of an unwanted incident on an asset in terms of harm or reduced asset value*



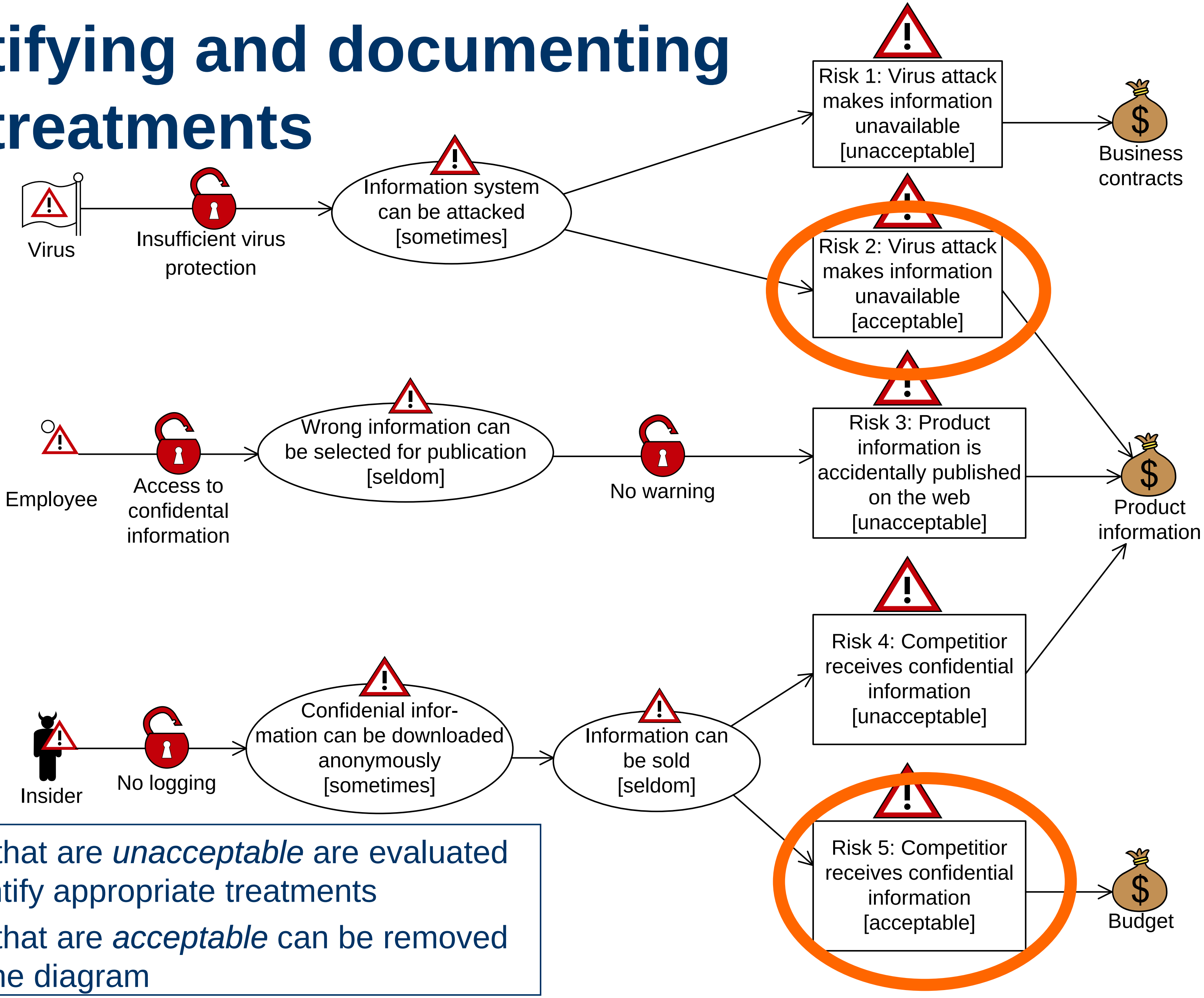
[sometimes]
Virus
Insufficient virus protection
Information system is attacked
[sometimes]
Virus attack makes information unavailable
Major
Business contracts
Small
Employee
Access to confidental information
Wrong information is selected for publication
[seldom]
No warning
Product information is accidentally published on the web
Major
Major
Product information
Insider
No logging
Confidential information is downloaded anonymously
[sometimes]
Information is sold
[seldom]
Competitor receives confidential information
Medium
Budget

Documenting risks

- **Risk**: *The likelihood of an unwanted incident and its consequence for a specific asset*
- Compared to the party's risk acceptance levels
- Acceptable and non-acceptable risks are shown in a risk diagram
  - decision makers
  - planning treatments
  - communicating risks


Virus attack makes information unavailable [sometimes]
Major
Business contracts
Risk1: Virus attack makes information unavailable [unacceptable]
Business contracts
Virus
Risk2: Virus attack makes information unavailable [acceptable]
Risk3: Product information is accidentally published on the web [unacceptable]
Product information
Employee
Risk4: Competitor receives confidential information [unacceptable]
Insider
Risk5: Competitor receives confidential information [acceptable]
Budget

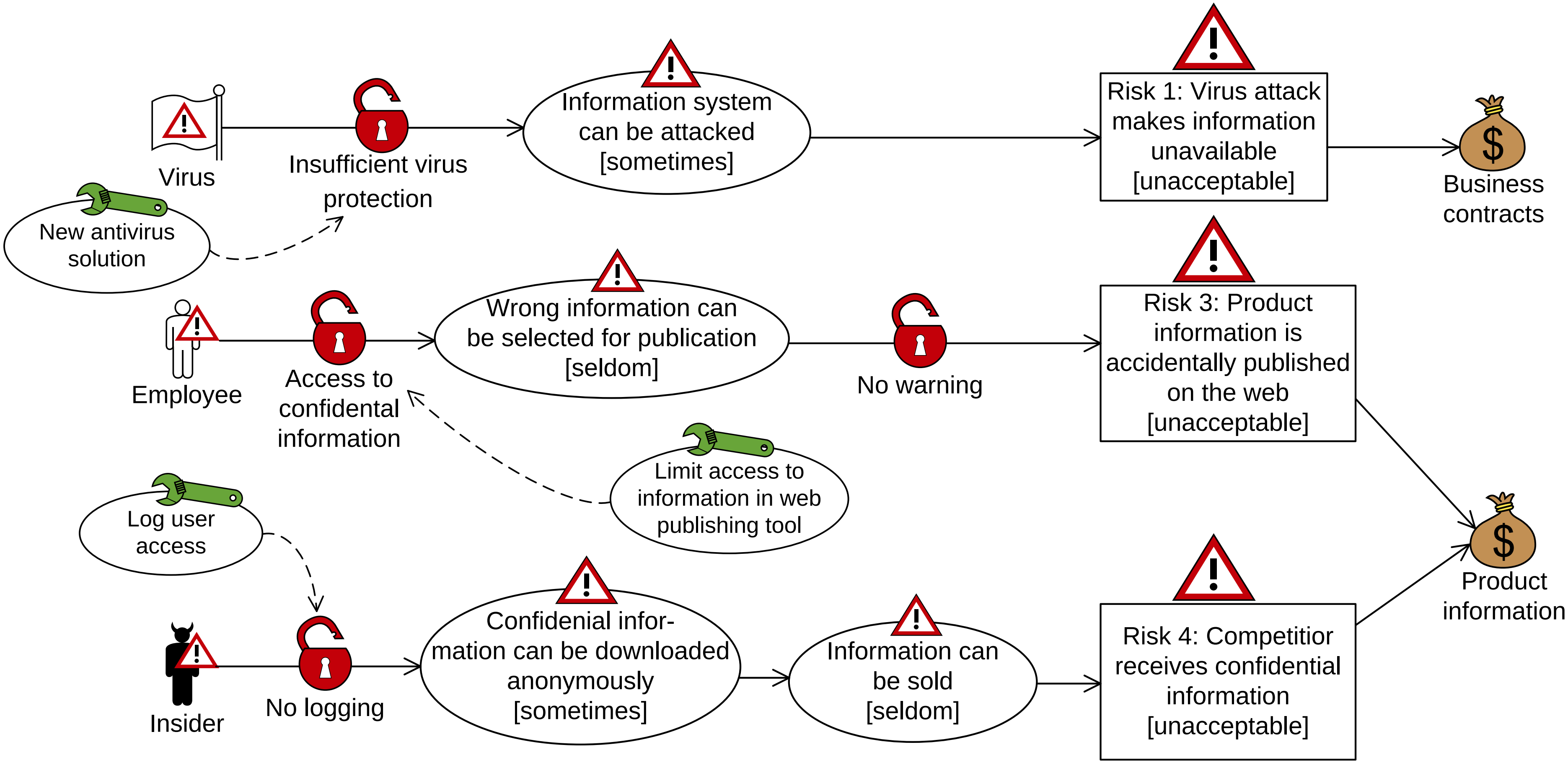
Identifying and documenting risk treatments


Virus
Insufficient virus protection
Information system can be attacked [sometimes]
Risk 1: Virus attack makes information unavailable [unacceptable]
Business contracts
Risk 2: Virus attack makes information unavailable [acceptable]
Employee
Access to confidential information
Wrong information can be selected for publication [seldom]
No warning
Risk 3: Product information is accidentally published on the web [unacceptable]
Product information
Risk 4: Competitior receives confidential information [unacceptable]
Insider
No logging
Confidential infor-mation can be downloaded anonymously [sometimes]
Information can be sold [seldom]
Risk 5: Competitior receives confidential information [acceptable]
Budget

- Risks that are *unacceptable* are evaluated to identify appropriate treatments
- Risks that are *acceptable* can be removed from the diagram

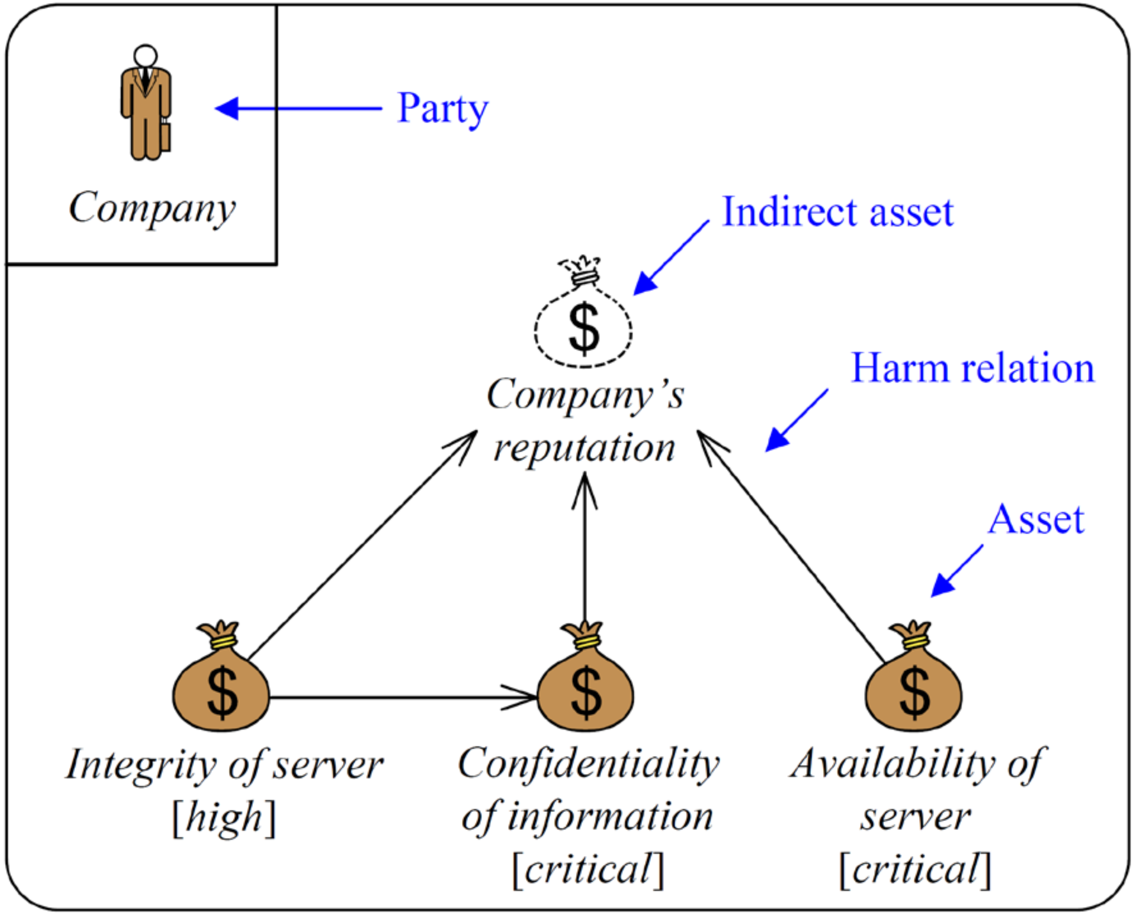
Identifying and documenting risk treatments

- **Risk treatment**: *An appropriate measure to reduce risk level*
- Treatments are added where they should have effect

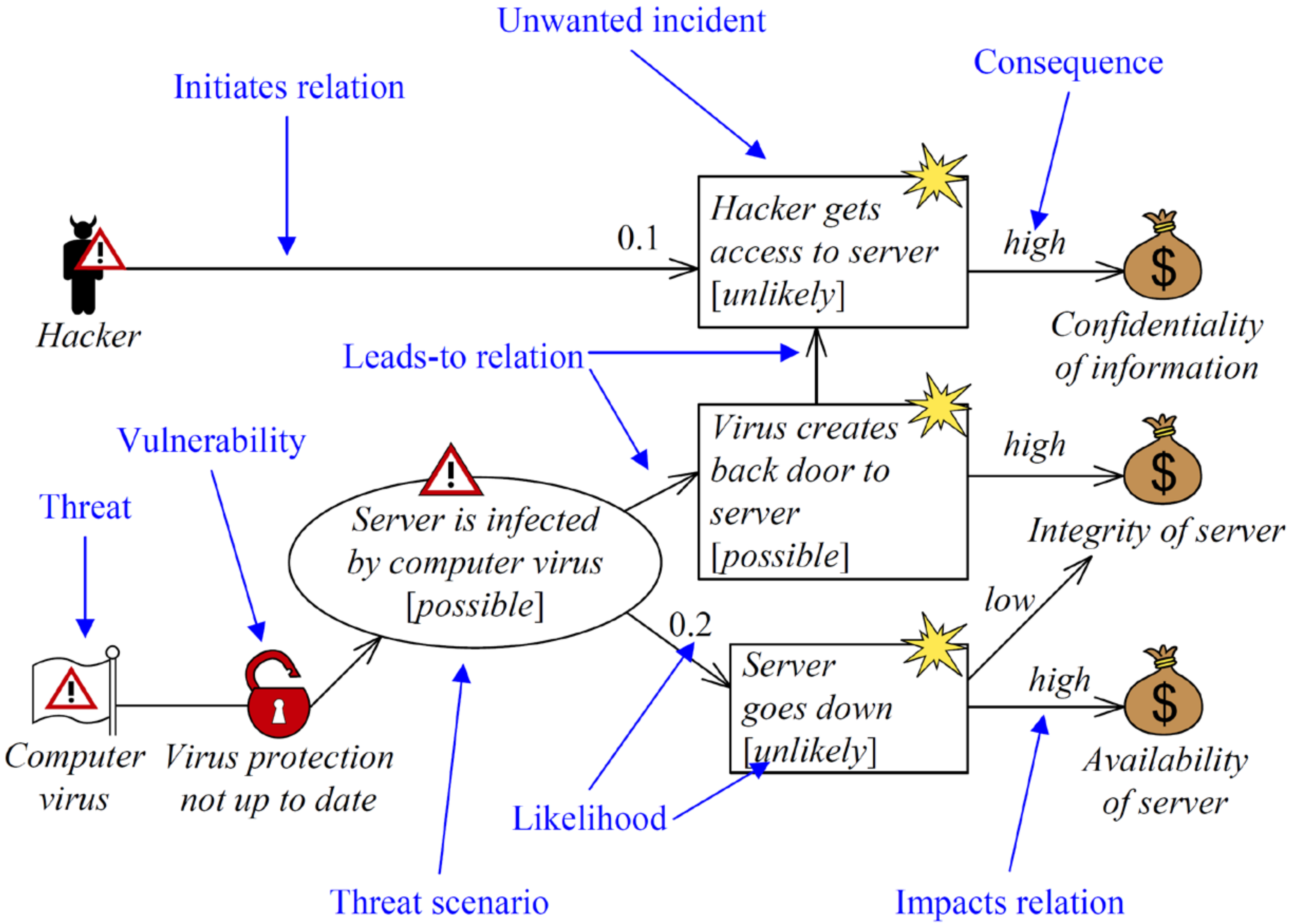

Virus
Insufficient virus protection
Information system can be attacked [sometimes]
Risk 1: Virus attack makes information unavailable [unacceptable]
Business contracts
New antivirus solution
Employee
Access to confidential information
Wrong information can be selected for publication [seldom]
No warning
Risk 3: Product information is accidentally published on the web [unacceptable]
Limit access to information in web publishing tool
Log user access
Insider
No logging
Confidential infor-mation can be downloaded anonymously [sometimes]
Information can be sold [seldom]
Risk 4: Competitior receives confidential information [unacceptable]
Product information

Example CORAS diagrams

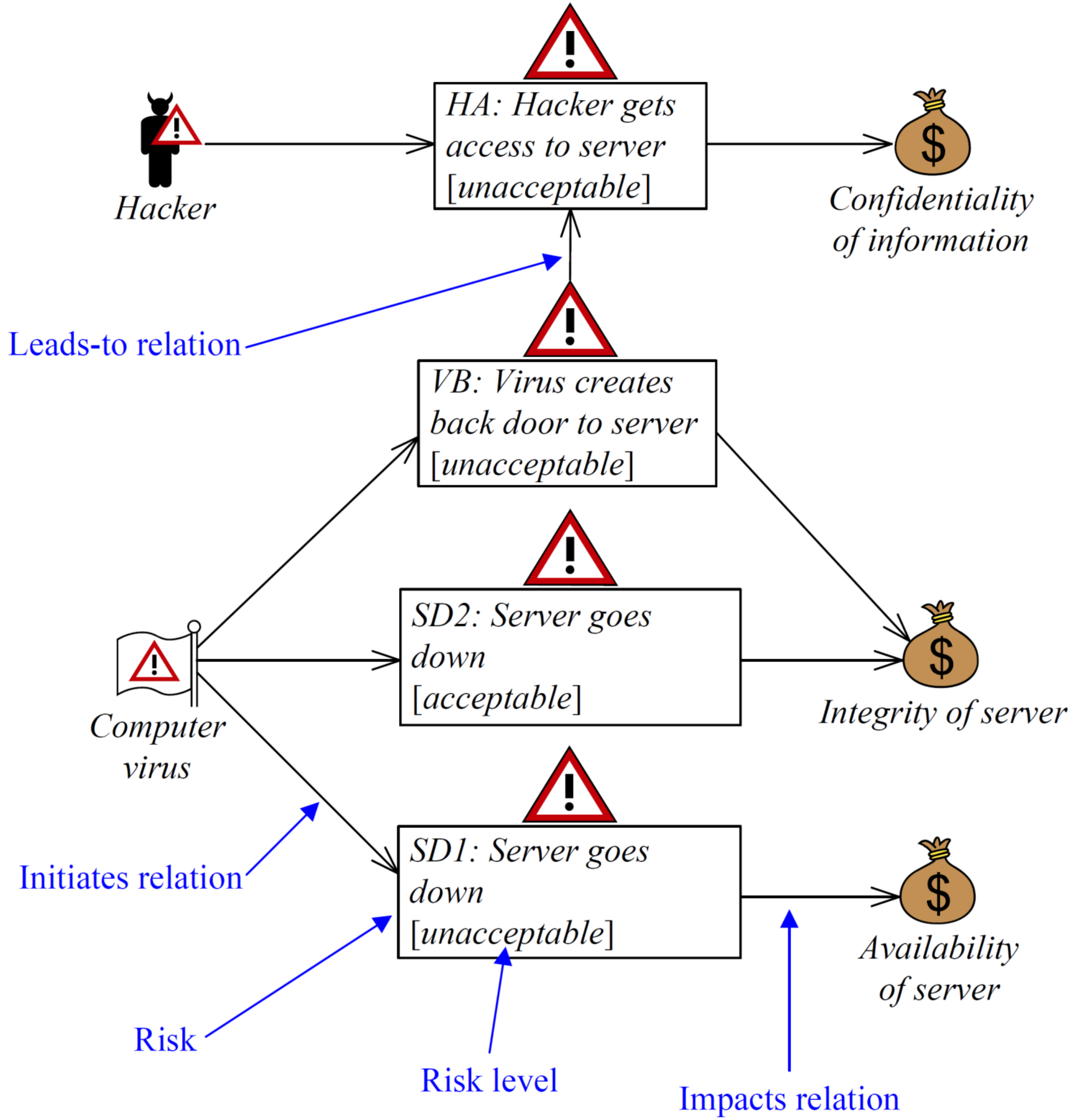
Example asset diagram


Company
Party
Indirect asset
Company's reputation
Harm relation
Asset
Integrity of server [high]
Confidentiality of information [critical]
Availability of server [critical]

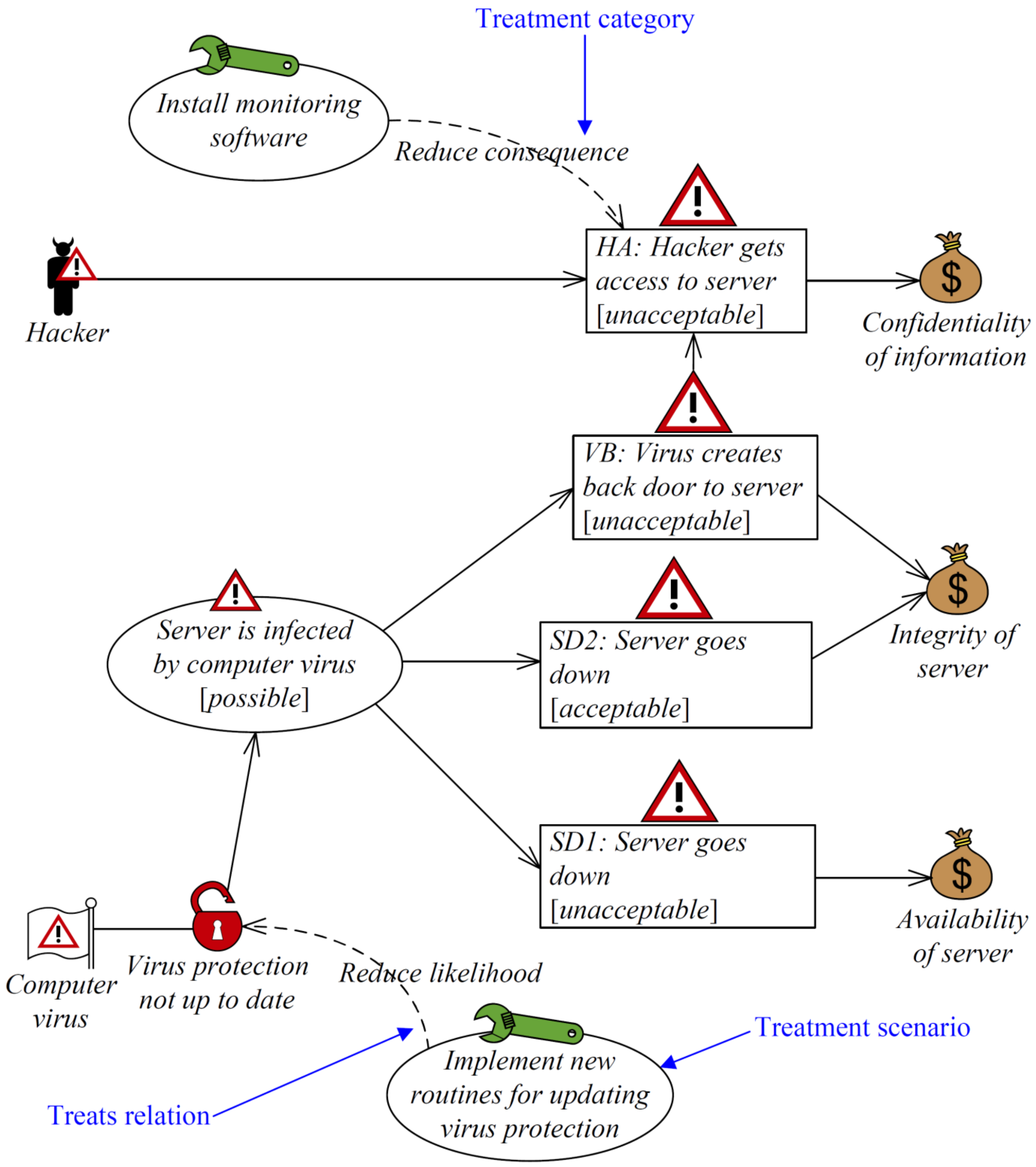
Example threat diagram


Unwanted incident
Initiates relation
Consequence
0.1
Hacker gets access to server [unlikely]
high
Hacker
Confidentiality of information
Leads-to relation
Vulnerability
Virus creates back door to server [possible]
high
Threat
Server is infected by computer virus [possible]
Integrity of server
low
0.2
Server goes down [unlikely]
high
Computer virus
Virus protection not up to date
Availability of server
Likelihood
Threat scenario
Impacts relation

Example risk diagram

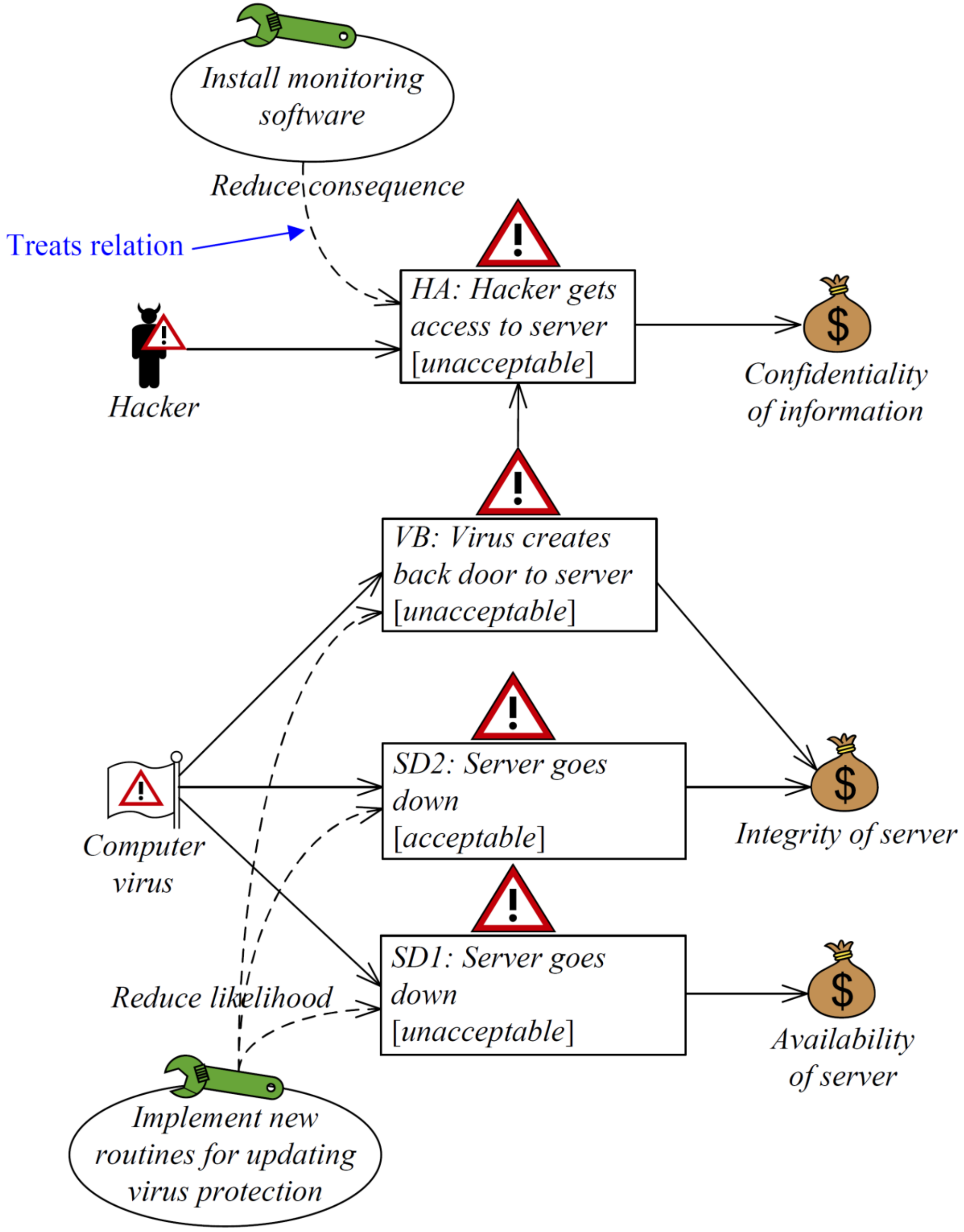

HA: Hacker gets access to server [unacceptable]
Hacker
Confidentiality of information
Leads-to relation
VB: Virus creates back door to server [unacceptable]
SD2: Server goes down [acceptable]
Computer virus
Integrity of server
Initiates relation
SD1: Server goes down [unacceptable]
Availability of server
Risk
Risk level
Impacts relation

Example treatment diagram



Treatment category
Install monitoring software
Reduce consequence
Hacker
HA: Hacker gets access to server [unacceptable]
Confidentiality of information
VB: Virus creates back door to server [unacceptable]
Server is infected by computer virus [possible]
SD2: Server goes down [acceptable]
Integrity of server
SD1: Server goes down [unacceptable]
Availability of server
Computer virus
Virus protection not up to date
Reduce likelihood
Treatment scenario
Implement new routines for updating virus protection
Treats relation

Example treatment overview diagram


Install monitoring software
Reduce consequence
Treats relation
HA: Hacker gets access to server [unacceptable]
Hacker
Confidentiality of information
VB: Virus creates back door to server [unacceptable]
SD2: Server goes down [acceptable]
Computer virus
Integrity of server
SD1: Server goes down [unacceptable]
Reduce likelihood
Availability of server
Implement new routines for updating virus protection

Building a threat diagram (1)

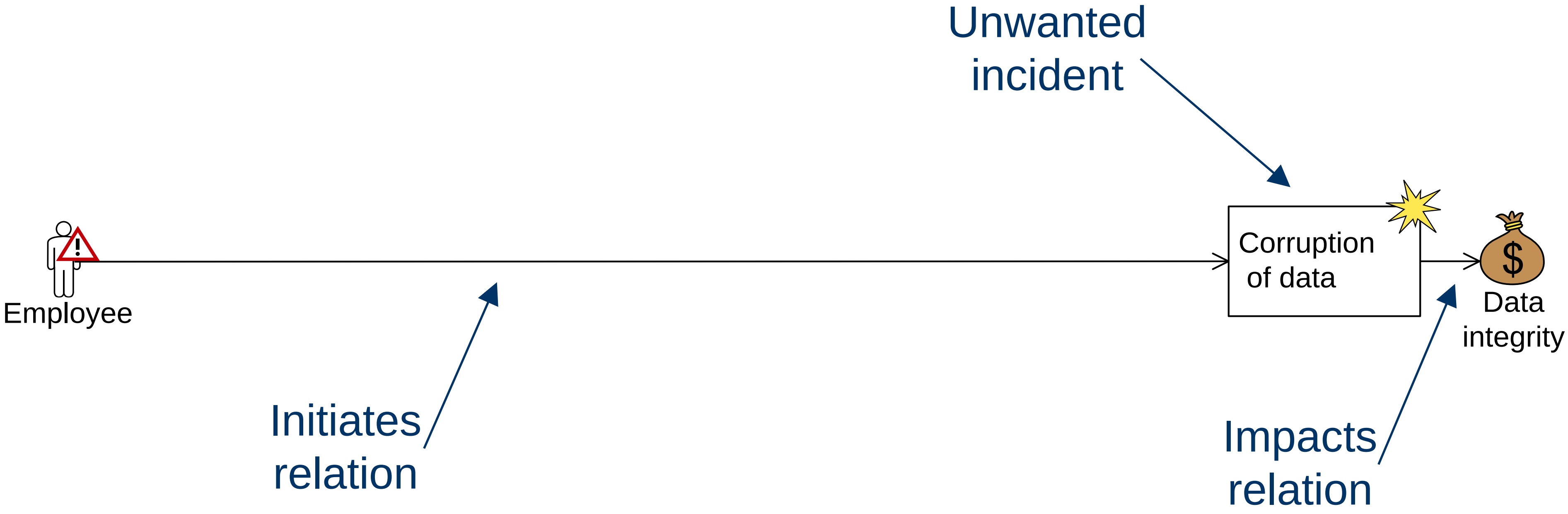
Threat

Asset

Employee

Data integrity

Building a threat diagram (2)

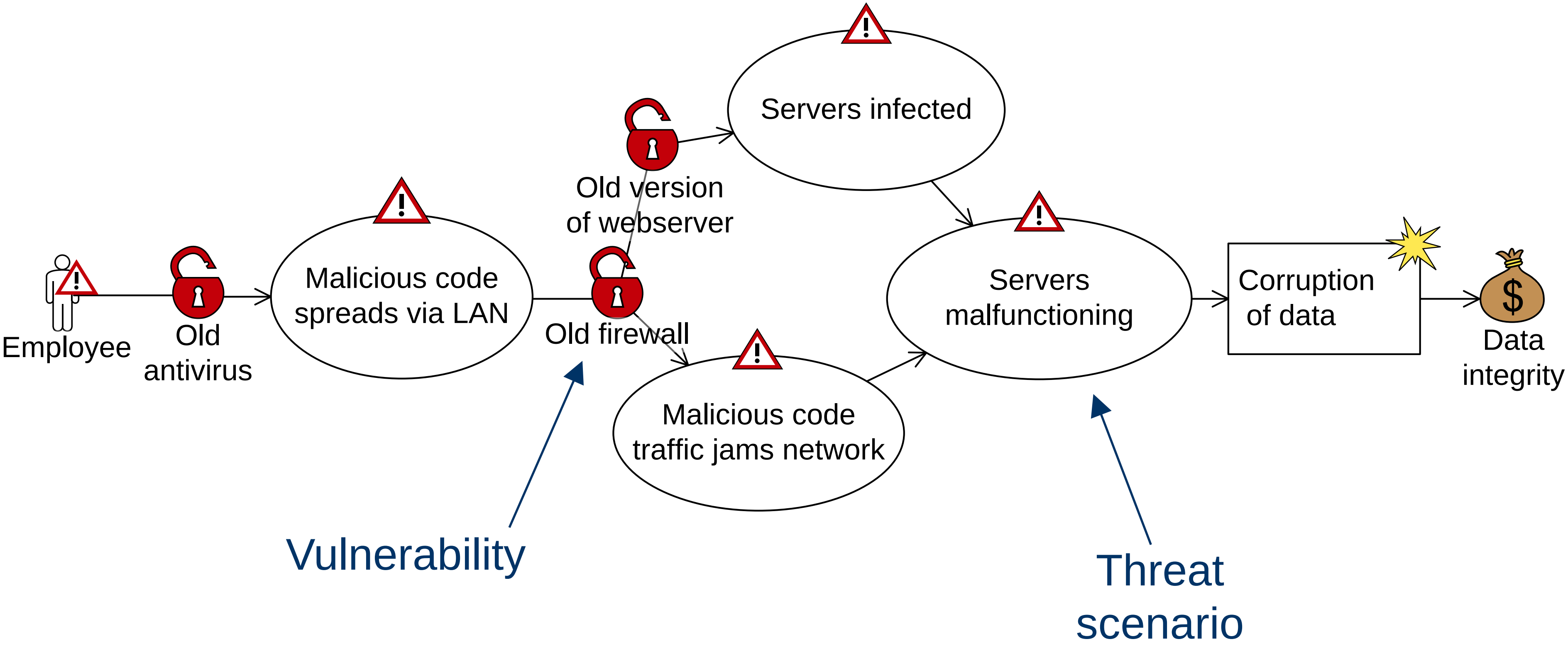


Unwanted incident

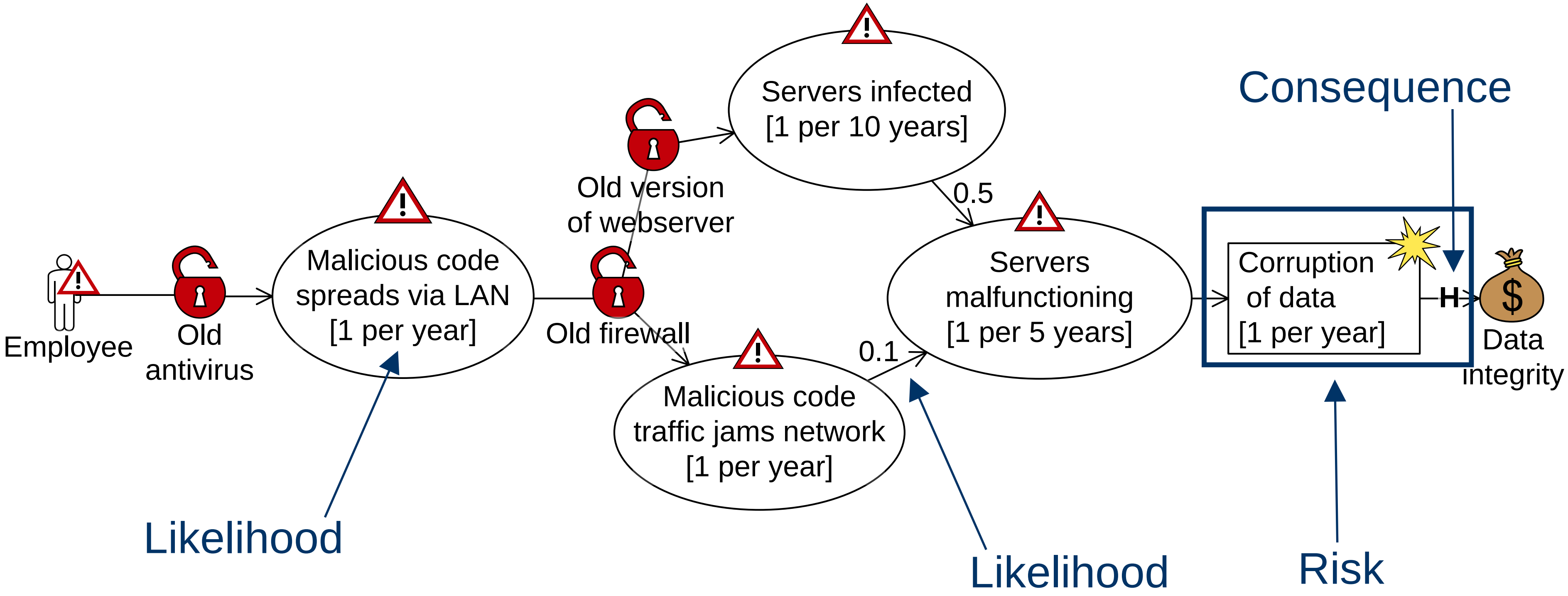
Initiates relation

Impacts relation

Building a threat diagram (3)



Building a threat diagram (4)


Employee
Old antivirus
Malicious code spreads via LAN [1 per year]
Old version of webserver
Old firewall
Servers infected [1 per 10 years]
0.5
Malicious code traffic jams network [1 per year]
0.1
Servers malfunctioning [1 per 5 years]
Corruption of data [1 per year]
H
$
Data integrity

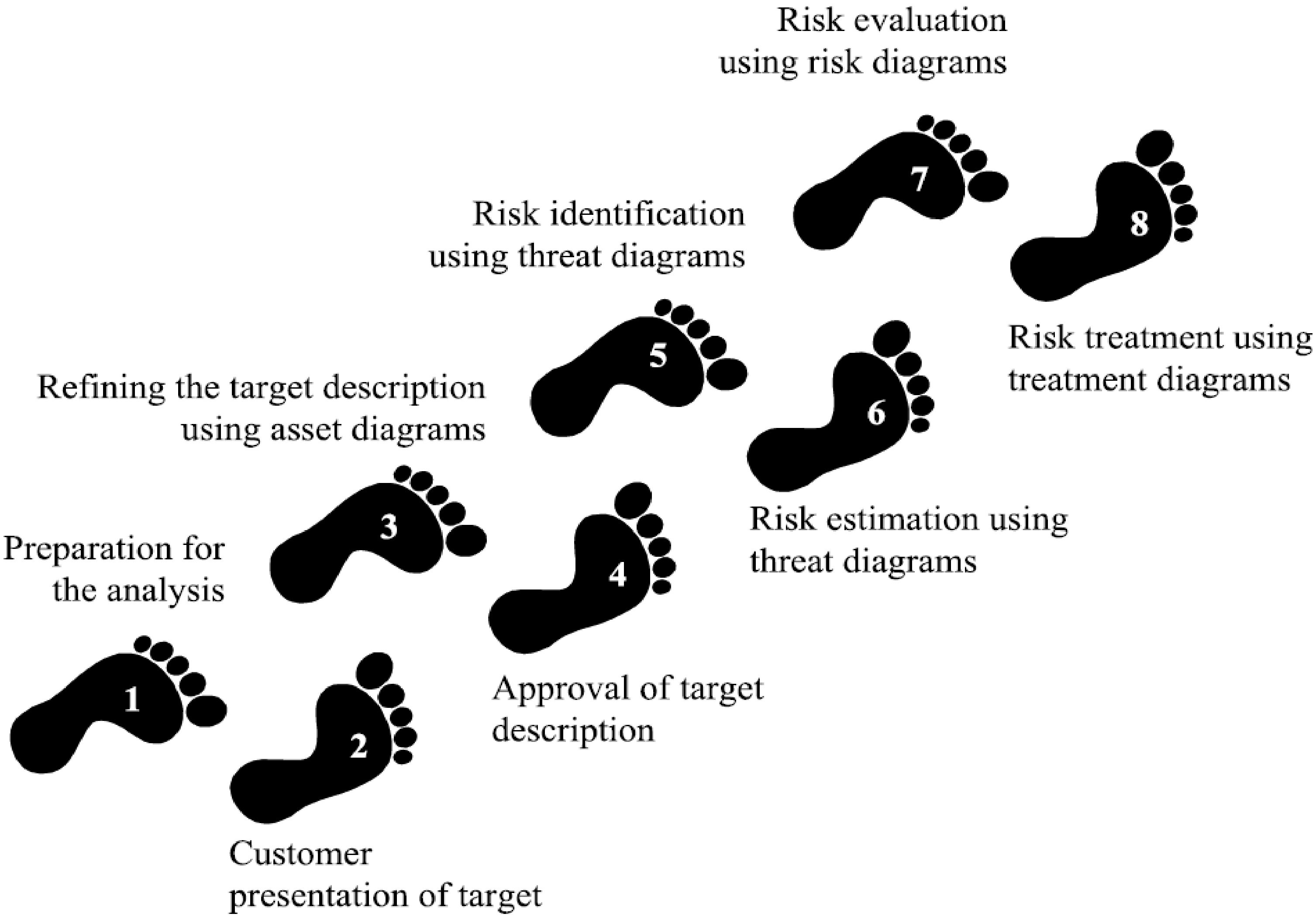
Consequence

Likelihood

Likelihood

Risk

The eight steps of a CORAS risk analysis



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

Step 1: Preparation

- The purpose of Step 1 is to do the necessary initial preparations prior to the actual startup of the analysis
- This includes
  - roughly setting the scope and focus
  - informing the customer of its responsibilities

Step 2: Customer presentation

- The second step involves an introductory meeting
- The main item on the agenda for this meeting is to get the representatives of the client to present their overall goals of the analysis and the target they wish to have analysed
- Hence, during the initial step the analysts will gather information based on the customer's presentations and discussions

Tasks

- The security analysis method is introduced
- The customer presents the goals and the target of the analysis
- The focus and scope of the analysis is set
- The meetings and workshops are planned

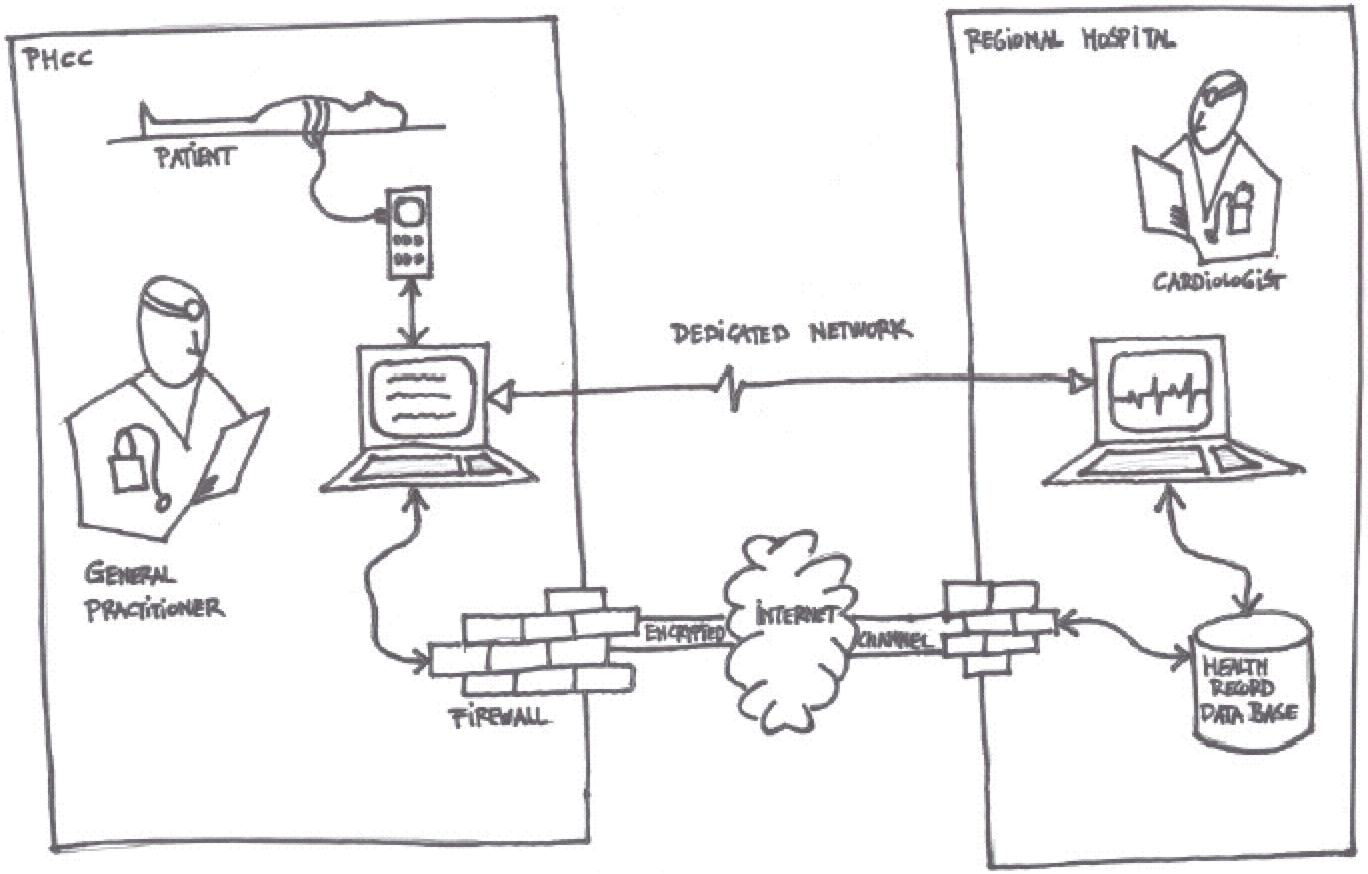
People that should participate

- Analysis leader (required)
- Analysis secretary (required)
- Representatives of the customer:
  - Decision makers (required)
  - Technical expertise (optional)
  - Users (optional)

Modelling guideline

- At this early stage of the analysis it can be useful to describe the target with informal drawings, pictures or sketches on a blackboard
- The presentation can later be supplemented with more formal modelling techniques such as UML or data flow-diagram

Telemedicine case



Step 3: Refining the target

- The third step also involves a separate meeting with representatives of the customer
- However, this time the analysts will present their understanding of what they learned at the first meeting and from studying documentation that has been made available to them by the client
- The third step also involves a rough, high-level security analysis
- During this analysis the first threats, vulnerabilities, threat scenarios and unwanted incidents are identified
- They will be used to help directing and scoping the more detailed analysis still to come

Tasks

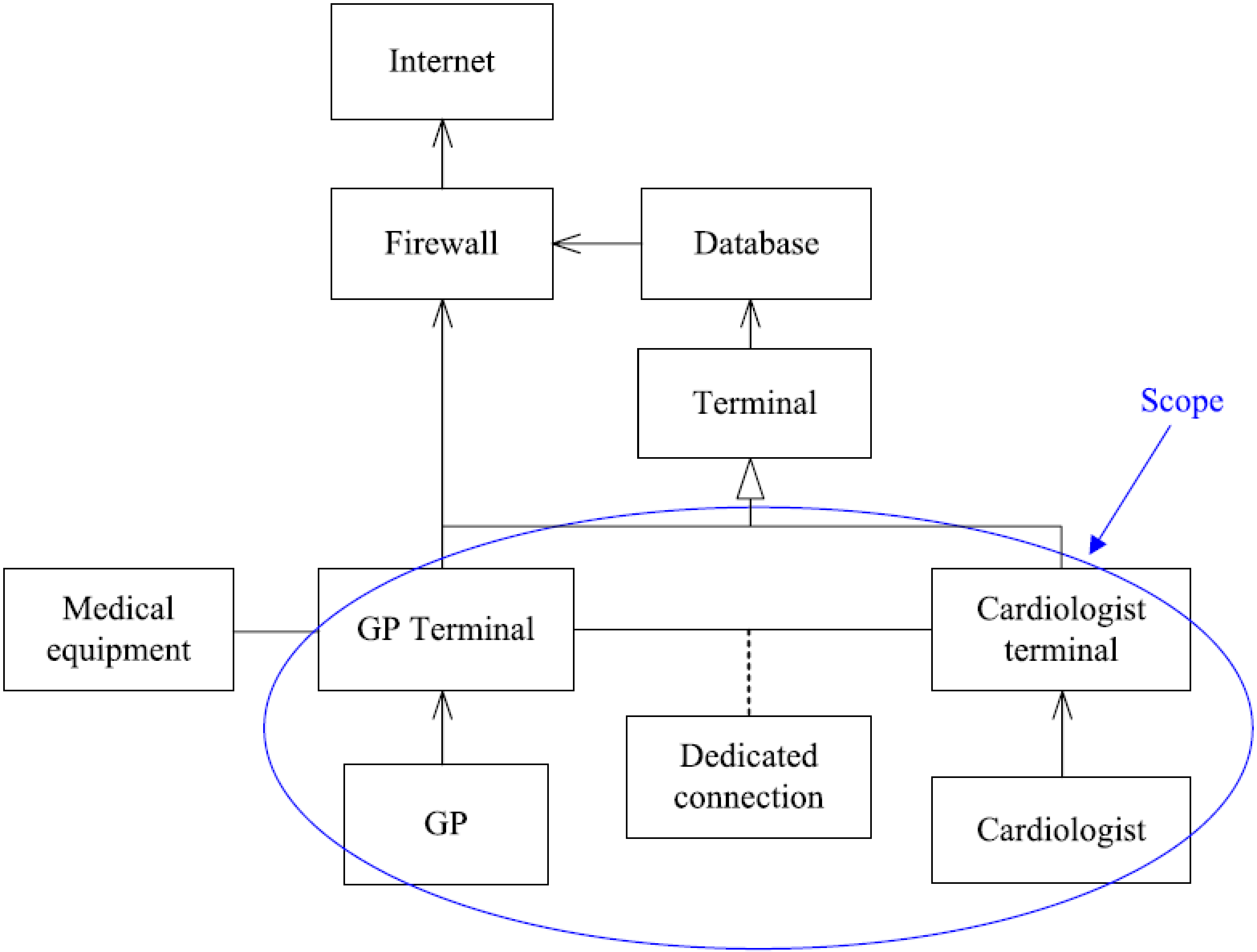
- The target as understood by the analysts is presented
- The assets are identied
- A high-level analysis is conducted

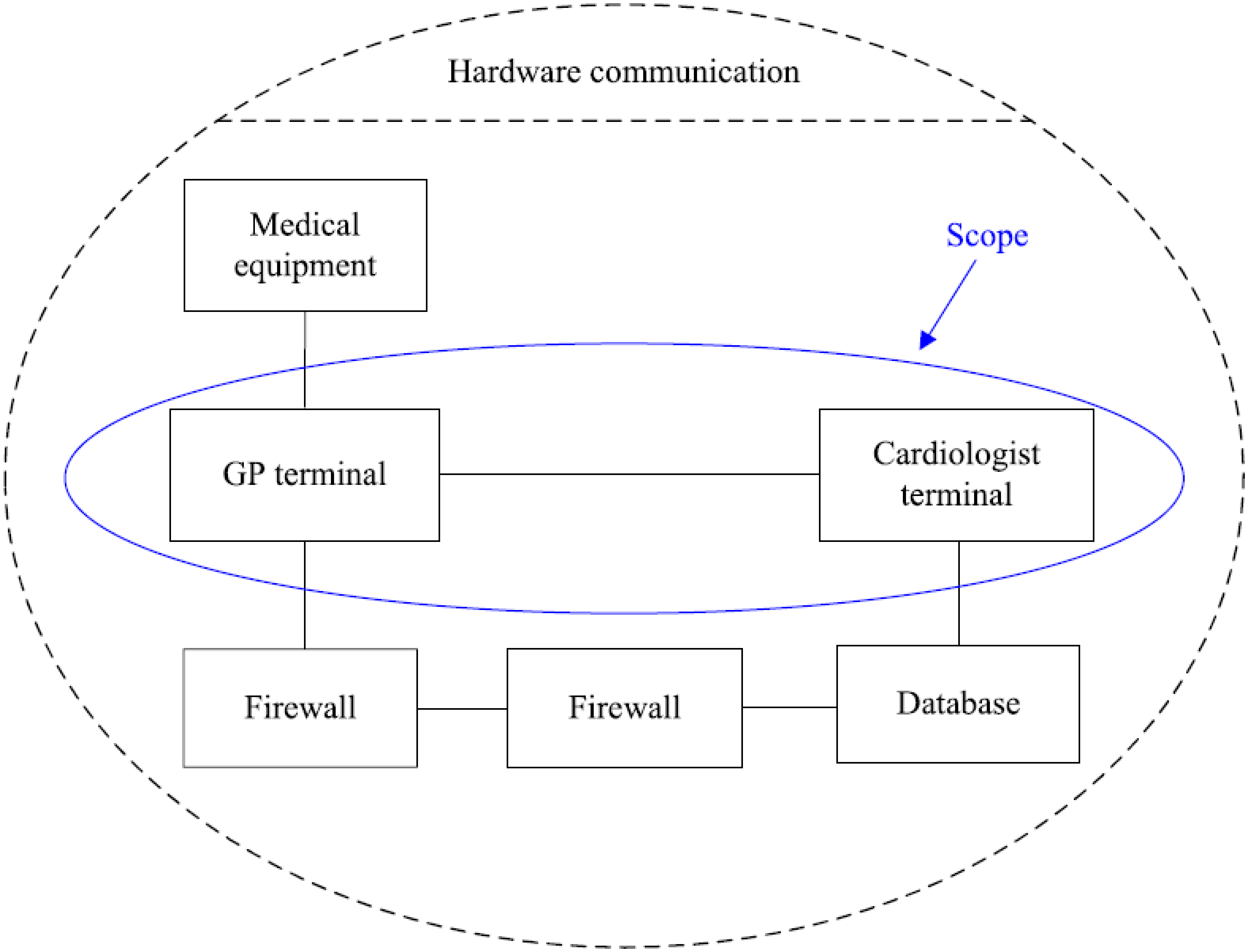
People that should participate

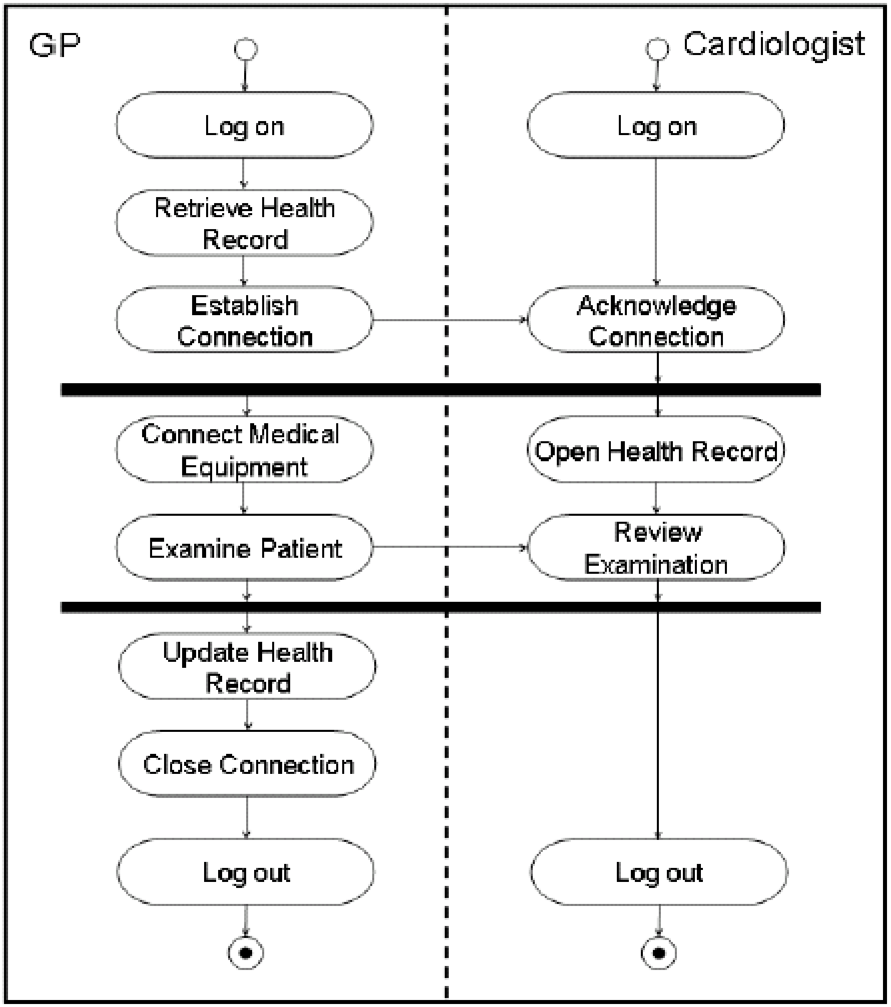
- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the customer:
  - Decision makers (required)
  - Technical expertise (required)
  - Users (optional)

Modelling guideline for the target description

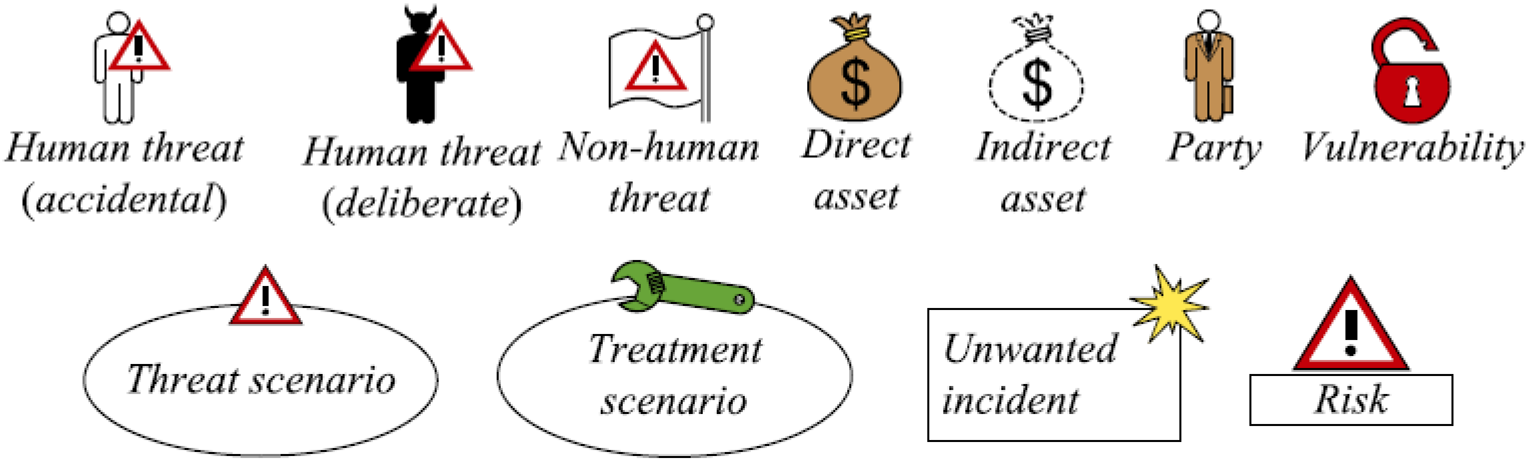
- Use a formal or standardised notation such as UML, but ensure that the notation is explained thoroughly so that the participants understand it.
- Create models of both the static and the dynamic features of the target.
- Static may be hardware configurations, network design etc., while dynamic may be work processes, information flow etc.
- For the static parts of the description UML class diagrams and UML collaboration diagrams (or similar notations) are recommended.
- For the dynamic parts we recommend UML activity diagrams and UML sequence diagrams (or similar notations)


Internet
Firewall
Database
Terminal
Scope
Medical equipment
GP Terminal
Cardiologist terminal
Dedicated connection
GP
Cardiologist

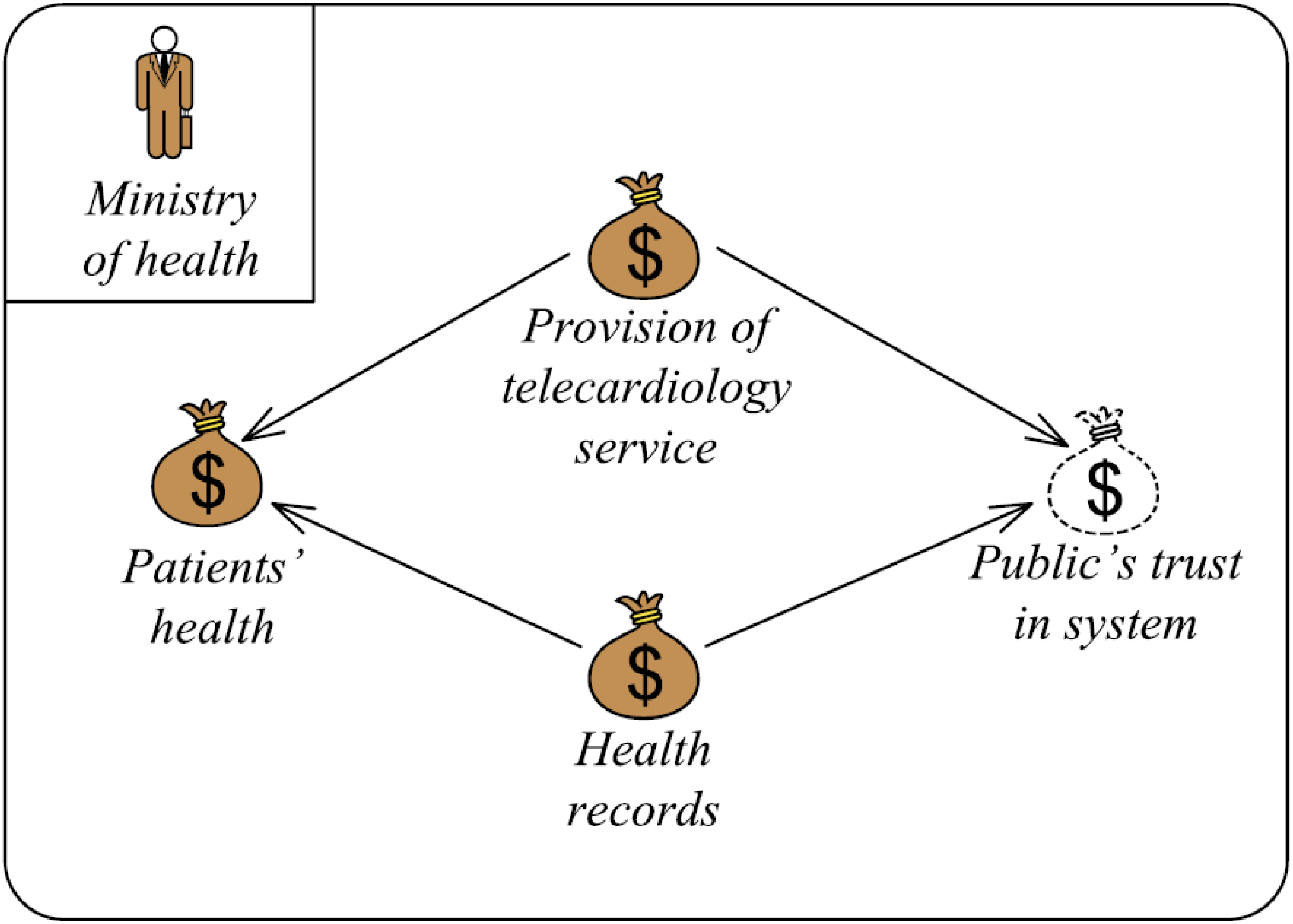

Hardware communication
Medical equipment
Scope
GP terminal
Cardiologist terminal
Firewall
Firewall
Database


GP
Cardiologist
Log on
Log on
Retrieve Health Record
Establish Connection
Acknowledge Connection
Connect Medical Equipment
Open Health Record
Examine Patient
Review Examination
Update Health Record
Close Connection
Log out
Log out

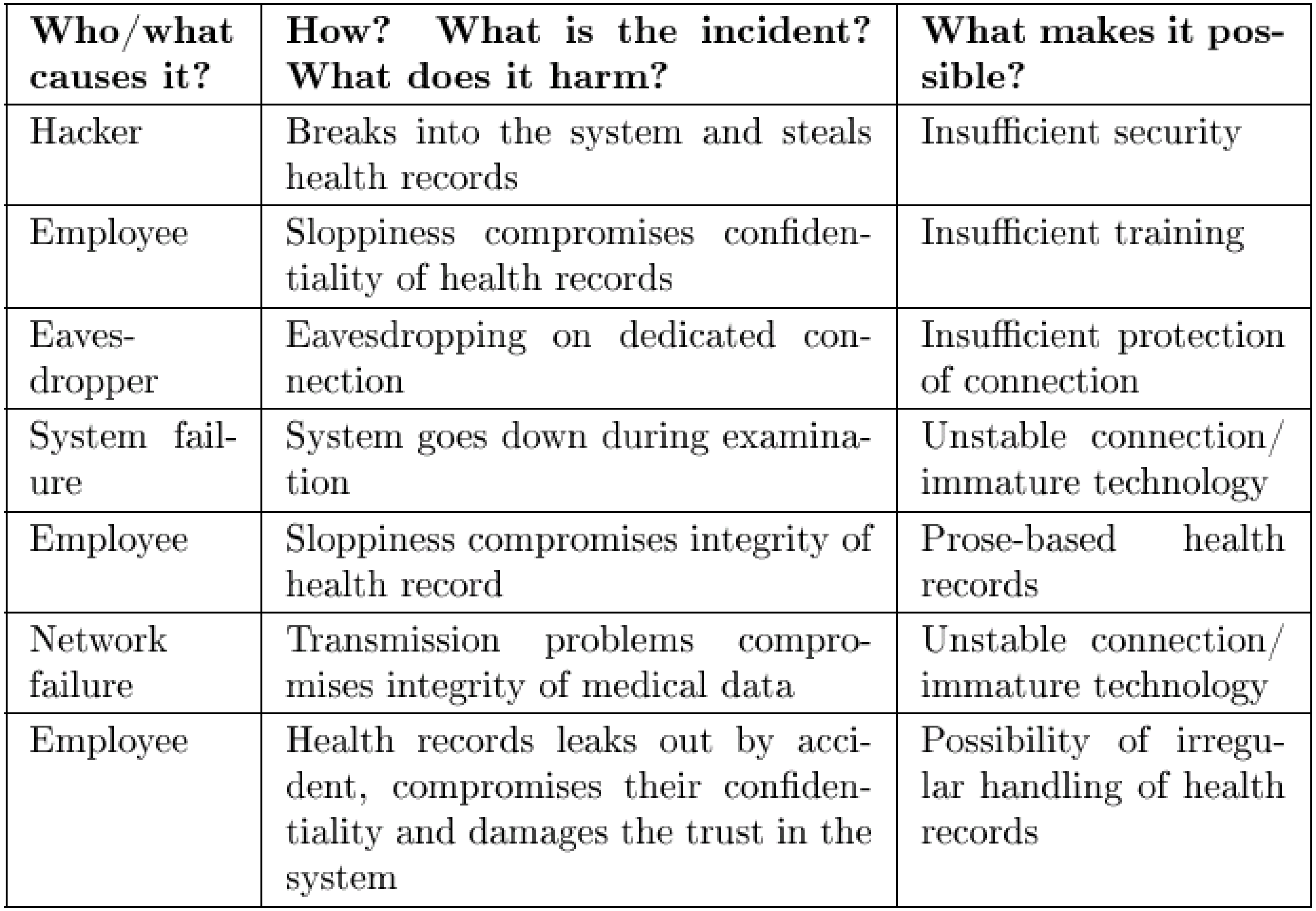
Symbols from the CORAS risk modelling language



Asset diagram



High-level risk table



Who/what causes it?	How? What is the incident? What does it harm?	What makes it possible?
Hacker	Breaks into the system and steals health records	Insufficient security
Employee	Sloppiness compromises confidentiality of health records	Insufficient training
Eavesdropper	Eavesdropping on dedicated connection	Insufficient protection of connection
System failure	System goes down during examination	Unstable connection/ immature technology
Employee	Sloppiness compromises integrity of health record	Prose-based health records
Network failure	Transmission problems compromises integrity of medical data	Unstable connection/ immature technology
Employee	Health records leaks out by accident, compromises their confidentiality and damages the trust in the system	Possibility of irregular handling of health records

Step 4: Approval

- The fourth step involves a more refined description of the target to be analysed, and also
  - all assumptions being made and
  - other preconditions made
- Step 4 is terminated once all this documentation has been approved by the customer

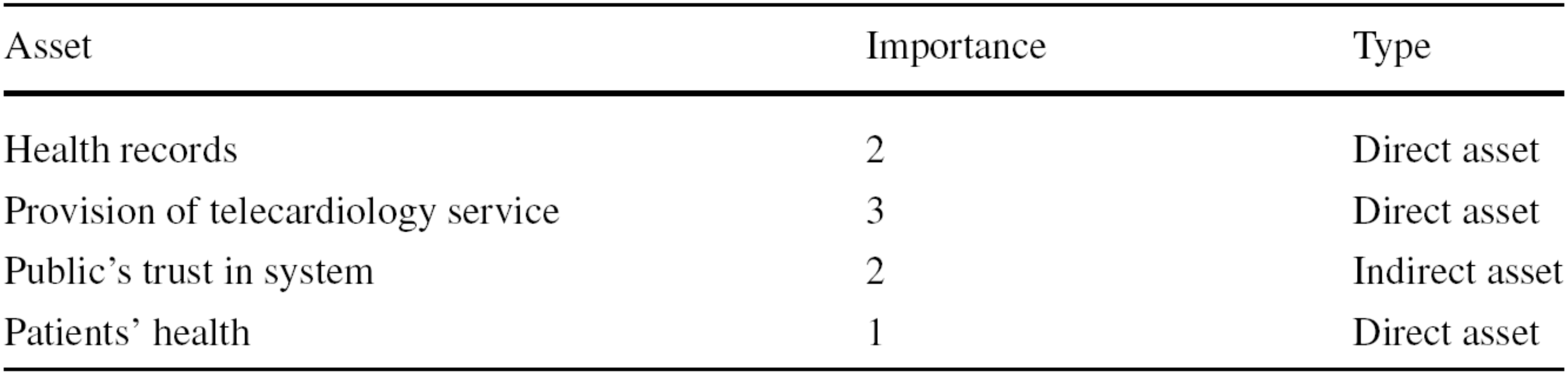
Tasks

- The client approves target descriptions and asset descriptions
- The assets should be ranked according to importance.
- Consequence scales must be set for each asset within the scope of the analysis
- A likelihood scale must be defined
- The client must decide risk evaluation criteria for each asset within the scope of the analysis

People that should participate

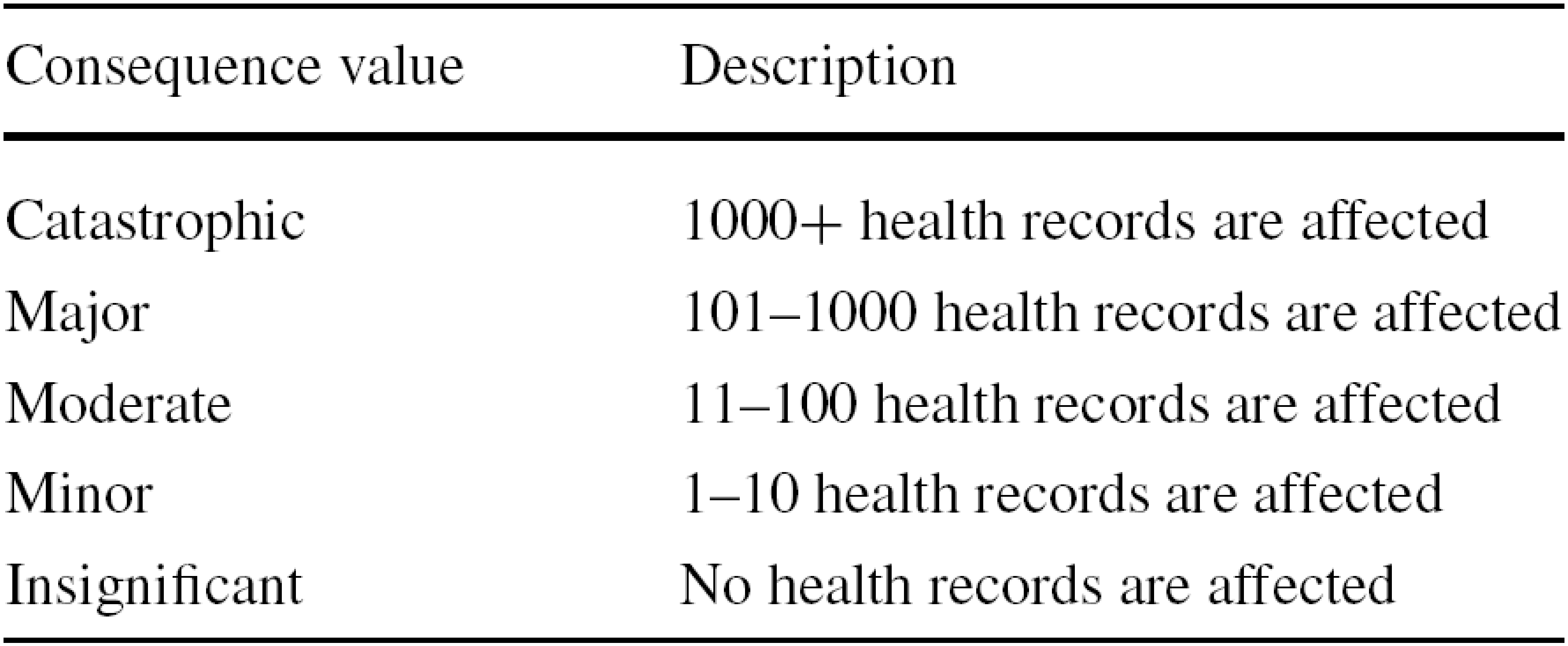
- The same as in the previous meeting, but since this step sets the boundaries for the further analysis it is important that the relevant decision-makers are present

Asset table



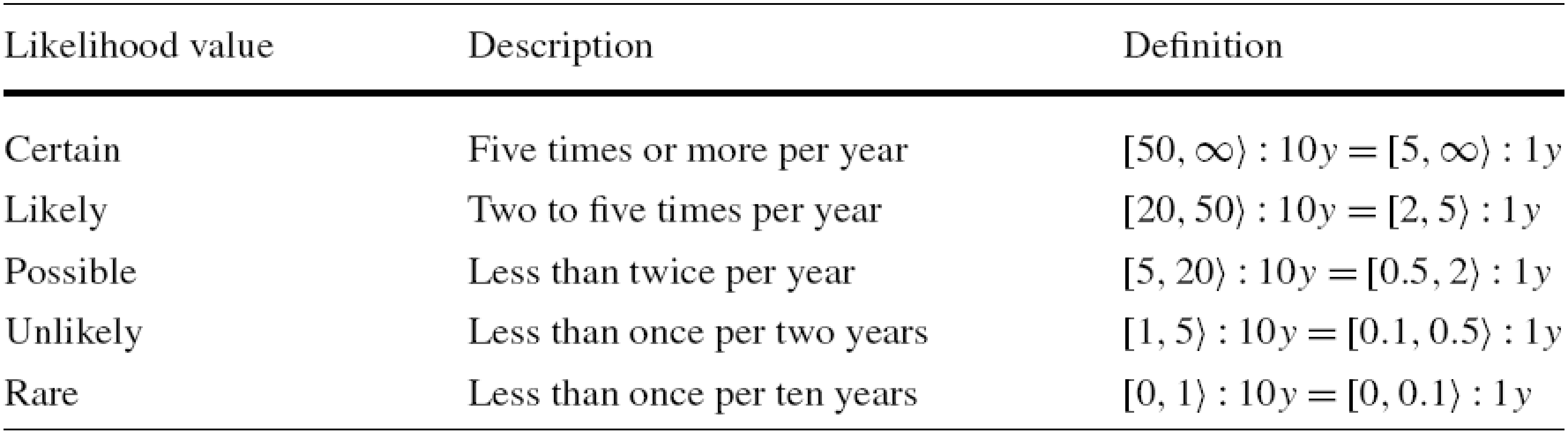
Asset	Importance	Type
Health records	2	Direct asset
Provision of telecardiology service	3	Direct asset
Public’s trust in system	2	Indirect asset
Patients’ health	1	Direct asset

Consequence scale for health records



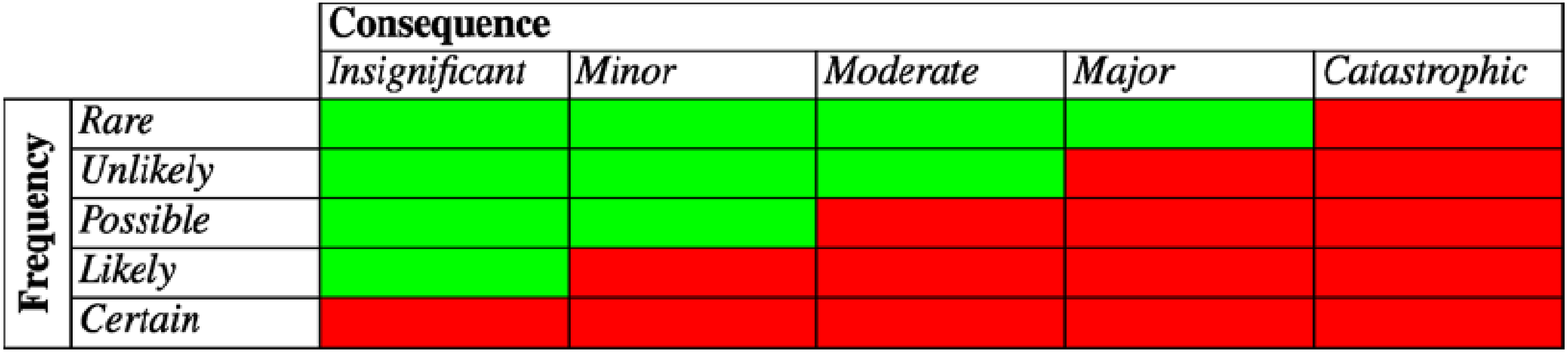
Consequence value	Description
Catastrophic	1000+ health records are affected
Major	101–1000 health records are affected
Moderate	11–100 health records are affected
Minor	1–10 health records are affected
Insignificant	No health records are affected

Likelihood scale



Likelihood value	Description	Definition
Certain	Five times or more per year	$[50, \infty\rangle : 10y = [5, \infty\rangle : 1y$
Likely	Two to five times per year	$[20, 50\rangle : 10y = [2, 5\rangle : 1y$
Possible	Less than twice per year	$[5, 20\rangle : 10y = [0.5, 2\rangle : 1y$
Unlikely	Less than once per two years	$[1, 5\rangle : 10y = [0.1, 0.5\rangle : 1y$
Rare	Less than once per ten years	$[0, 1\rangle : 10y = [0, 0.1\rangle : 1y$

Risk evaluation matrix



		Consequence				
		Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Frequency	*Rare*	🟩	🟩	🟩	🟩	🟥
	Unlikely	🟩	🟩	🟩	🟥	🟥
	Possible	🟩	🟩	🟥	🟥	🟥
	Likely	🟩	🟥	🟥	🟥	🟥
	Certain	🟥	🟥	🟥	🟥	🟥

Step 5: Risk identification

- This step is organised as a workshop gathering people with expertise on the target of evaluation.
- The goal is to identify as many potential unwanted incidents as possible, as well as threats, vulnerabilities and threat scenarios.

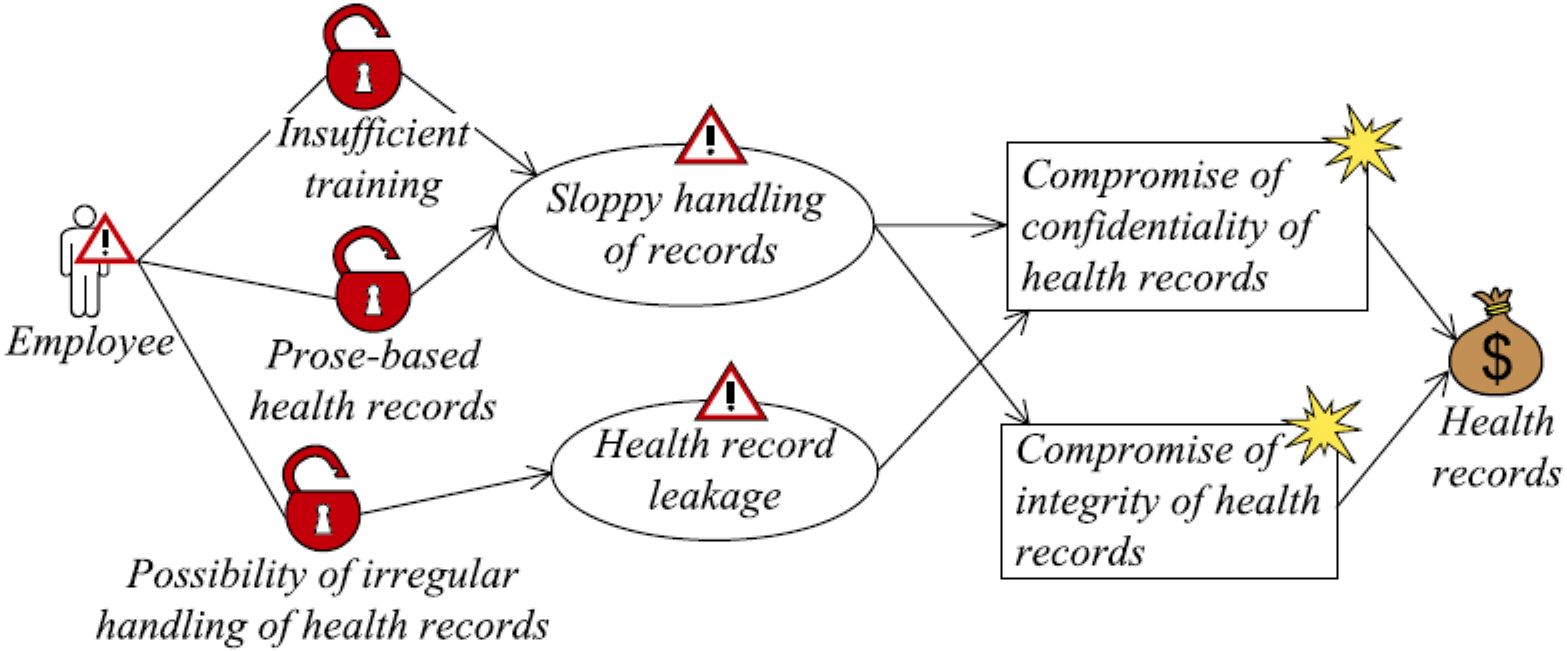
Tasks

- The initial threat diagrams should be completed with identified threats, vulnerabilities, threat scenarios and unwanted incidents.

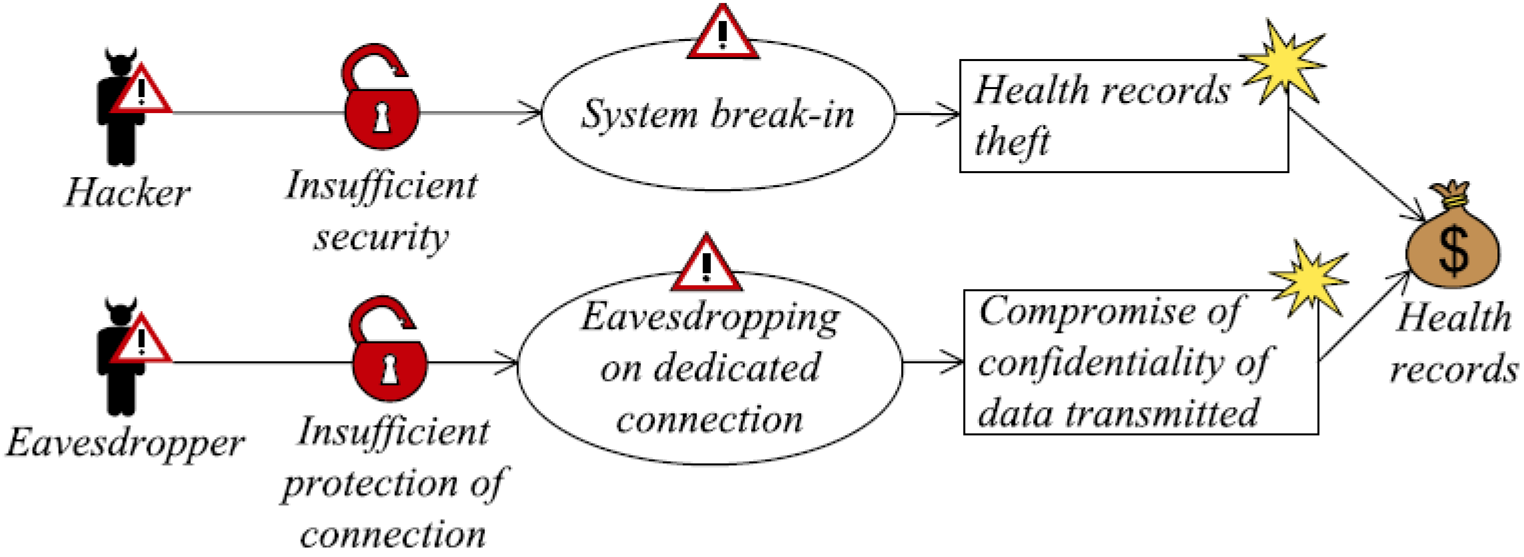
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (optional)
  - Technical expertise (required)
  - Users (required)

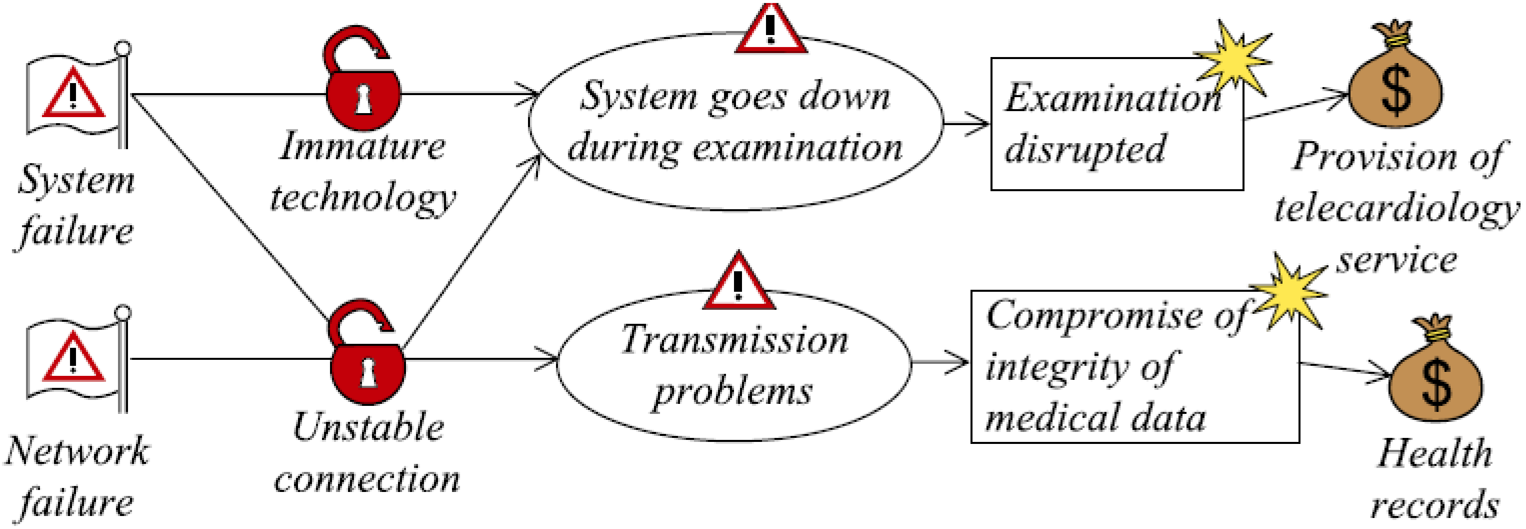
Initial threat diagram: accidental actions


Insufficient training
Employee
Prose-based health records
Possibility of irregular handling of health records
Sloppy handling of records
Health record leakage
Compromise of confidentiality of health records
Compromise of integrity of health records
Health records

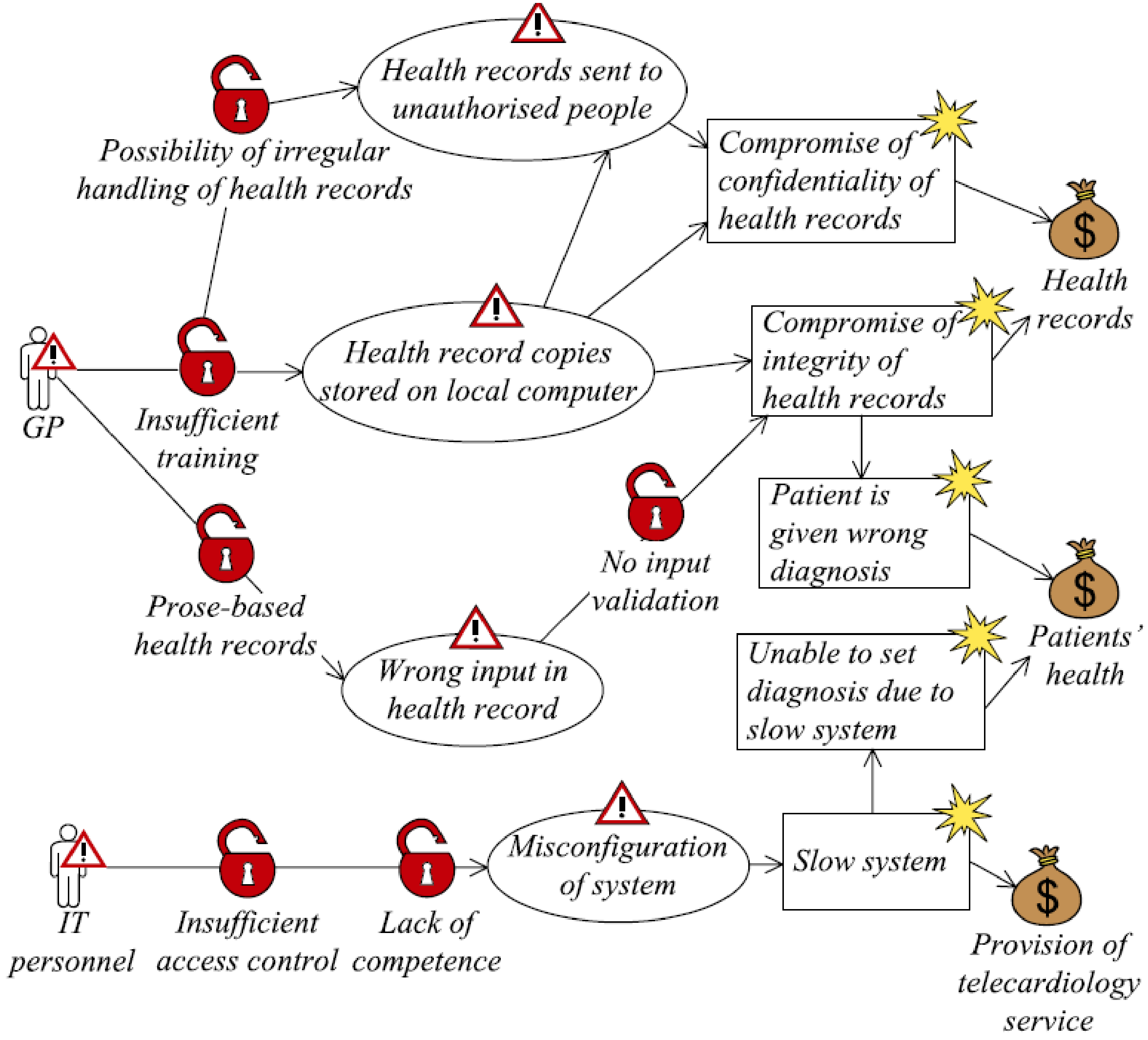
Initial threat diagram: deliberate actions


Hacker
Insufficient security
System break-in
Health records theft
Eavesdropper
Insufficient protection of connection
Eavesdropping on dedicated connection
Compromise of confidentiality of data transmitted
Health records

Initial threat diagram: non-human threats



Final threat diagram: accidental actions


Health records sent to unauthorised people
Possibility of irregular handling of health records
Compromise of confidentiality of health records
Health records
Health record copies stored on local computer
Compromise of integrity of health records
GP
Insufficient training
No input validation
Patient is given wrong diagnosis
Prose-based health records
Wrong input in health record
Patients' health
Unable to set diagnosis due to slow system
Misconfiguration of system
Slow system
IT personnel
Insufficient access control
Lack of competence
Provision of telecardiology service

Step 6: Risk estimation

- The sixth step is also organised as a workshop
- This time with focus on estimating consequences and likelihood values for each of the identied unwanted incidents

Tasks

- Threat scenarios must be given a likelihood estimate and likelihoods for unwanted incidents are based on these
- Every relation between an unwanted incident and an asset must be given a consequence estimate

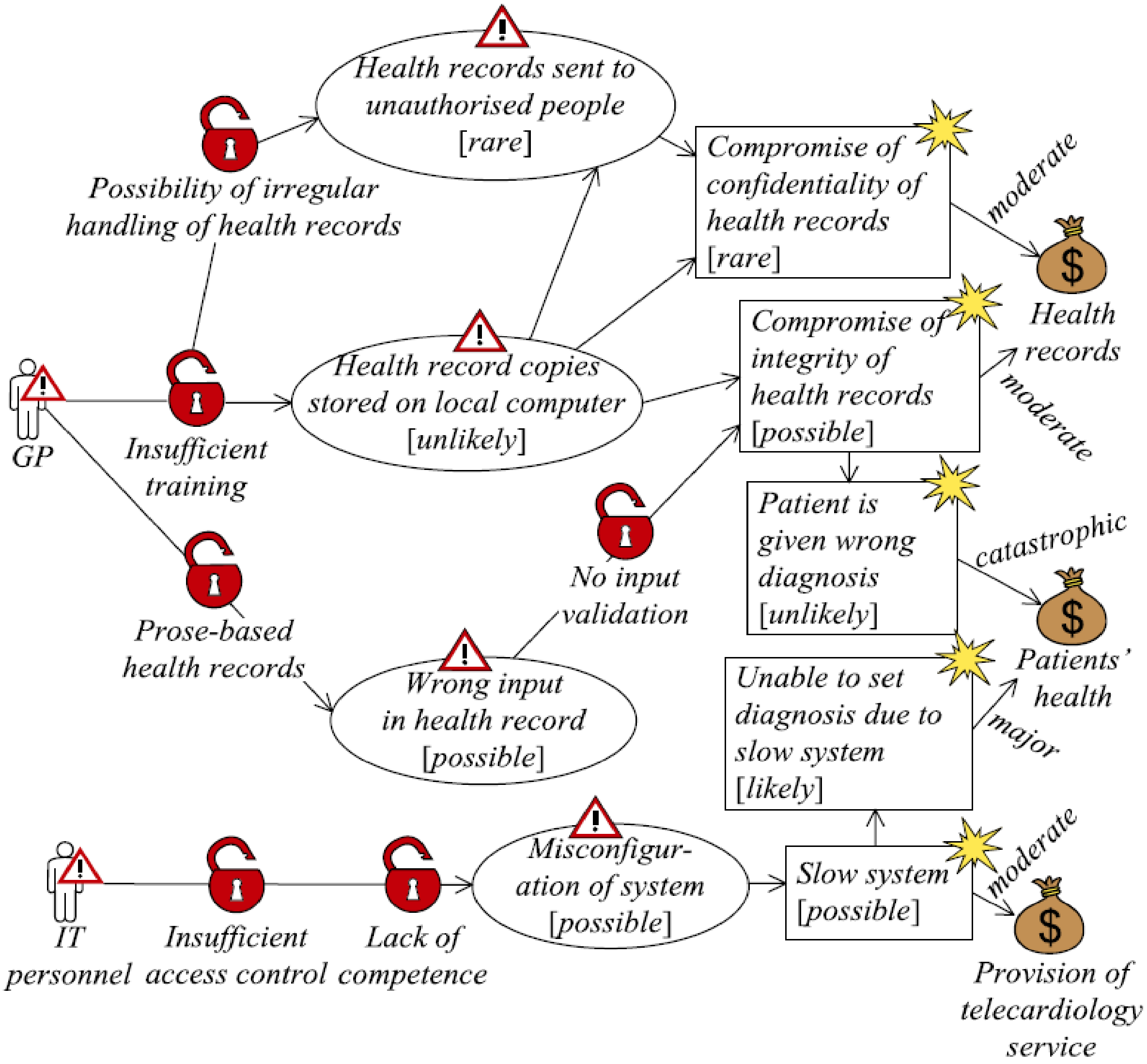
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise regarding the target (required)
  - Users (required)

Modelling guideline

- Risk estimation on threat diagrams:
  - Add likelihood estimates to the threat scenarios.
  - Add likelihood estimates to the unwanted incidents, based on the threat scenarios.
  - Annotate each unwanted incident-asset relation with a consequence taken from the respective asset's consequence scale.

Threat diagram with estimates



Health records sent to unauthorised people [rare]

Possibility of irregular handling of health records

Compromise of confidentiality of health records [rare]

moderate

Health records

GP

Insufficient training

Health record copies stored on local computer [unlikely]

Compromise of integrity of health records [possible]

moderate

Patient is given wrong diagnosis [unlikely]

catastrophic

No input validation

Prose-based health records

Wrong input in health record [possible]

Unable to set diagnosis due to slow system [likely]

Patients' health

major

IT personnel

Insufficient access control

Lack of competence

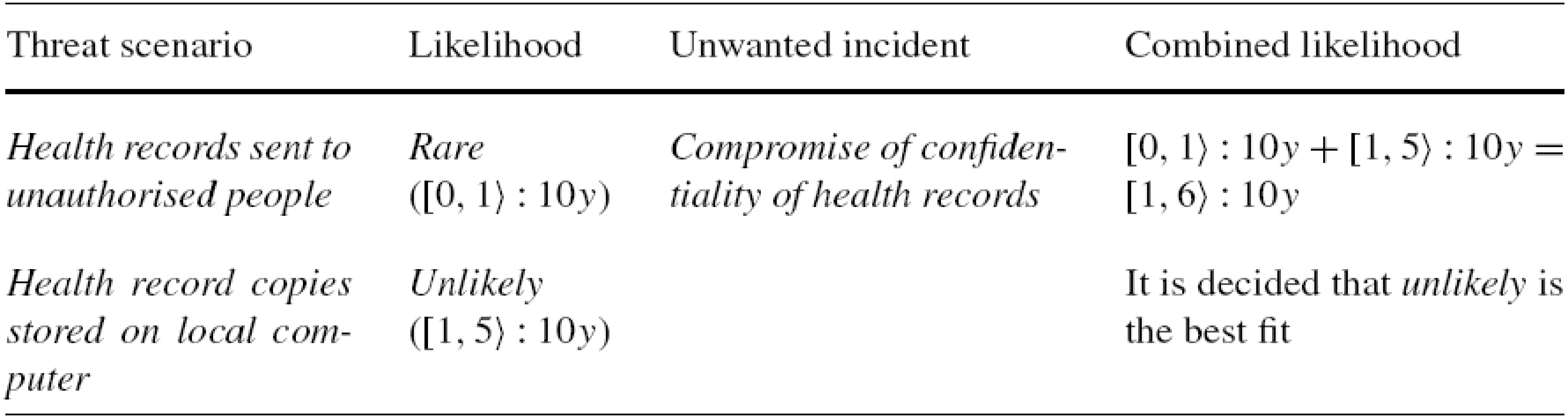
Misconfigur-ation of system [possible]

Slow system [possible]

moderate

Provision of telecardiology service

Combined likelihood estimates



Threat scenario	Likelihood	Unwanted incident	Combined likelihood
Health records sent to unauthorised people	*Rare* ($[0, 1\rangle : 10y$)	*Compromise of confidentiality of health records*	$[0, 1\rangle : 10y + [1, 5\rangle : 10y = [1, 6\rangle : 10y$
Health record copies stored on local computer	*Unlikely* ($[1, 5\rangle : 10y$)		It is decided that *unlikely* is the best fit

Step 7: Risk evaluation

- This step involves giving the client the first overall risk picture
- This will typically trigger some adjustments and corrections

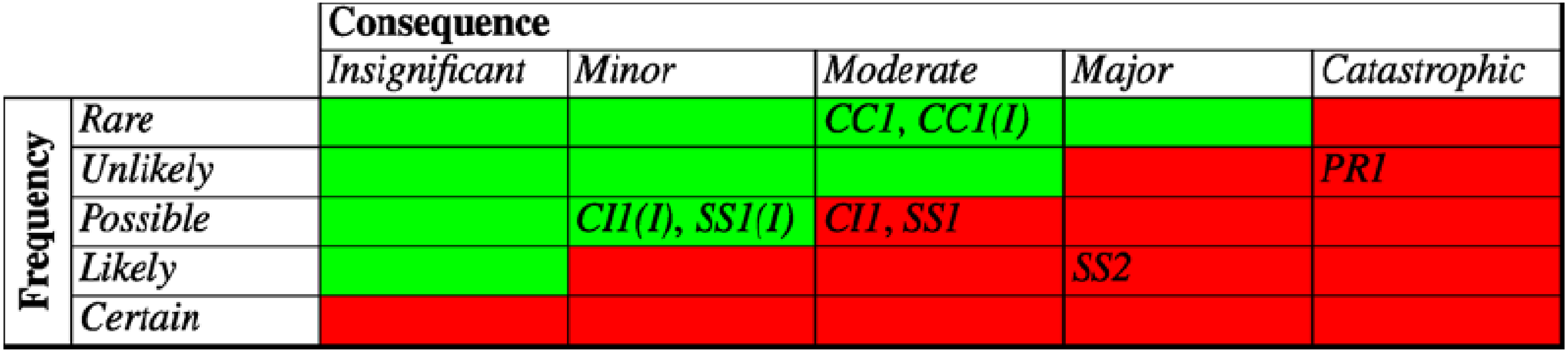
Tasks

- Likelihood and consequence estimates should be confirmed or adjusted
- The final adjustments of the acceptable area in the risk matrices should be made (if needed)
- An overview of the risks may be given in a risk diagram

People that should participate

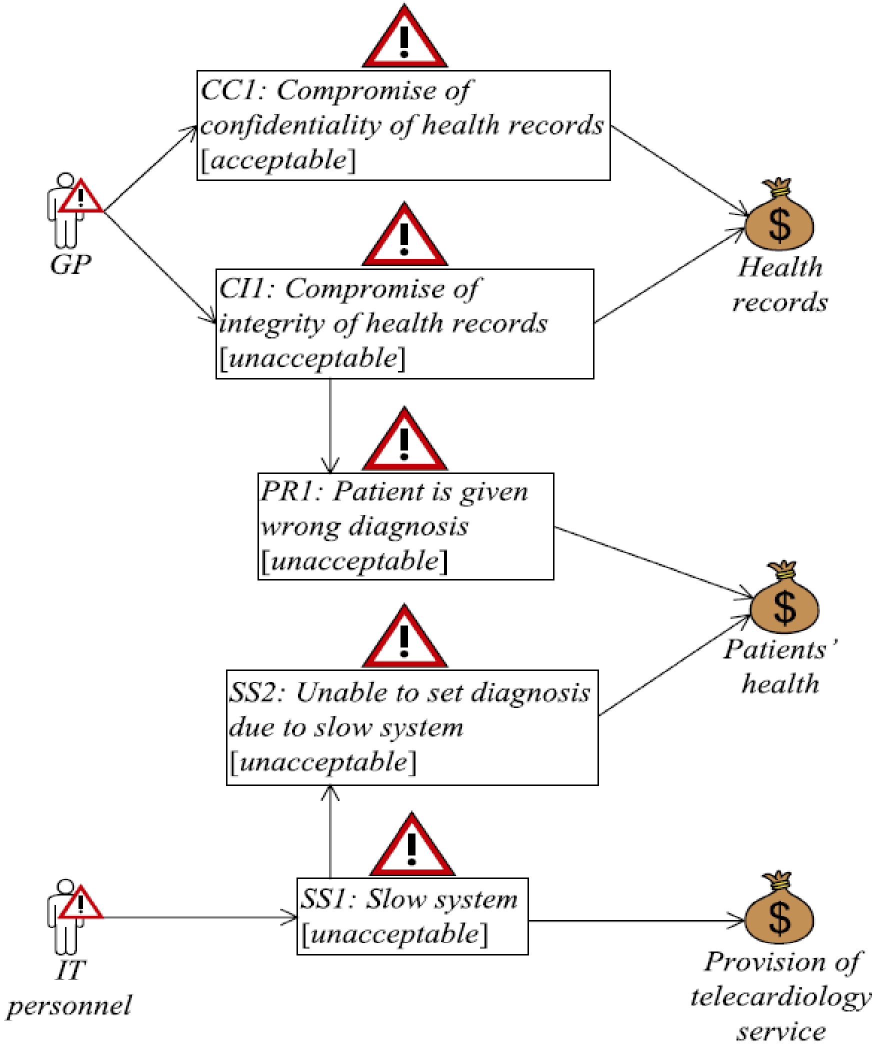
- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise regarding the target (optional)
  - Users (optional)

Risk evaluation matrix with risks



		Consequence				
		Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Frequency	*Rare*	🟩	🟩	🟩 *CC1, CC1(I)*	🟩	🟥
	Unlikely	🟩	🟩	🟩	🟥	🟥 *PR1*
	Possible	🟩	🟩 *CI1(I), SS1(I)*	🟥 *CI1, SS1*	🟥	🟥
	Likely	🟩	🟥	🟥	🟥 *SS2*	🟥
	Certain	🟥	🟥	🟥	🟥	🟥

Risk overview diagram



CC1: Compromise of confidentiality of health records [acceptable]

CI1: Compromise of integrity of health records [unacceptable]

PR1: Patient is given wrong diagnosis [unacceptable]

SS2: Unable to set diagnosis due to slow system [unacceptable]

SS1: Slow system [unacceptable]

Step 8: Risk treatment

- The last step is devoted to treatment identication, as well as addressing cost/benefit issues of the treatments
- This step is best organised as a workshop

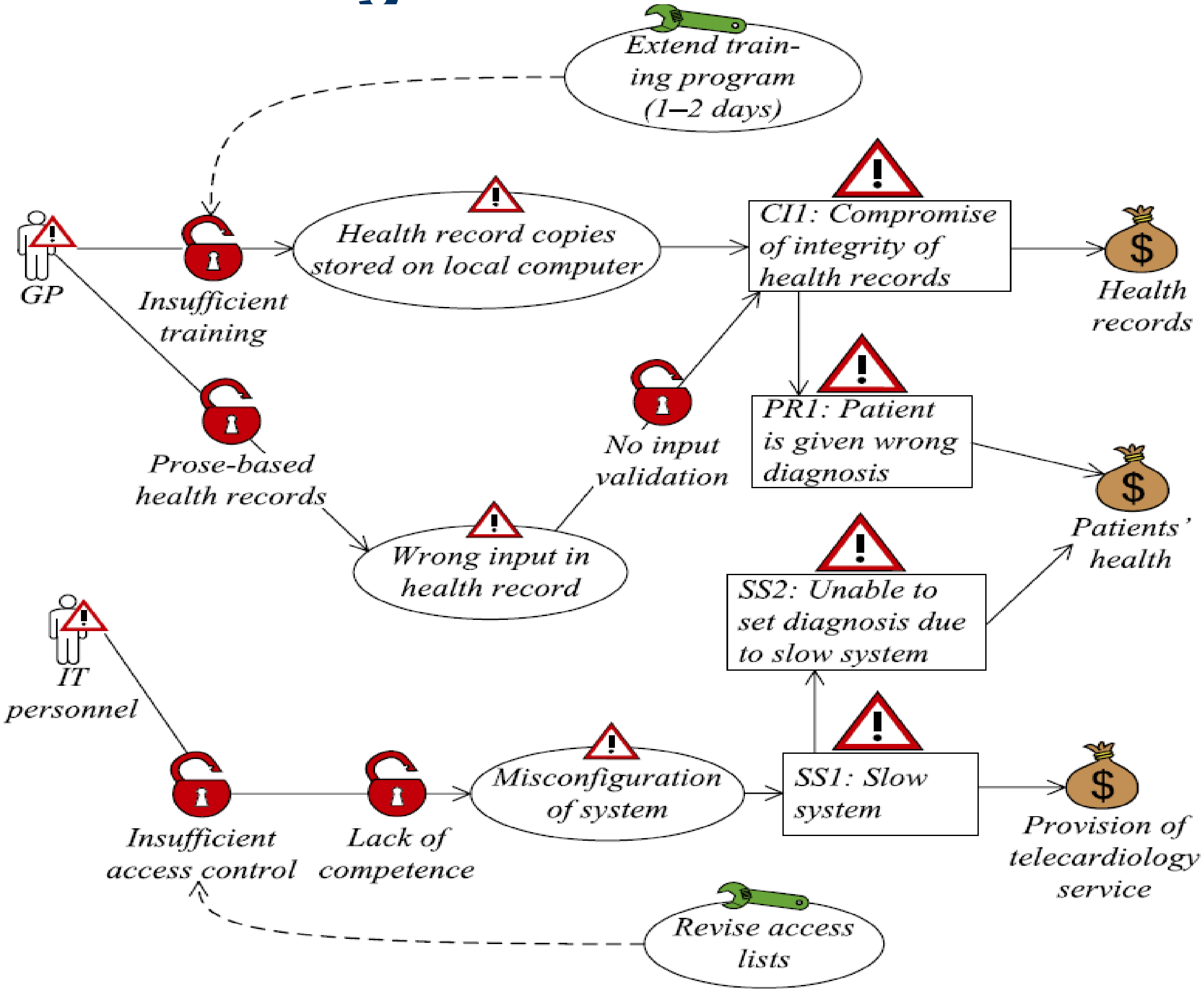
Tasks

- Add treatments to threat diagrams
- Estimate the cost/benefit of each treatment and decide which ones to use
- Show treatments in risk overview diagrams

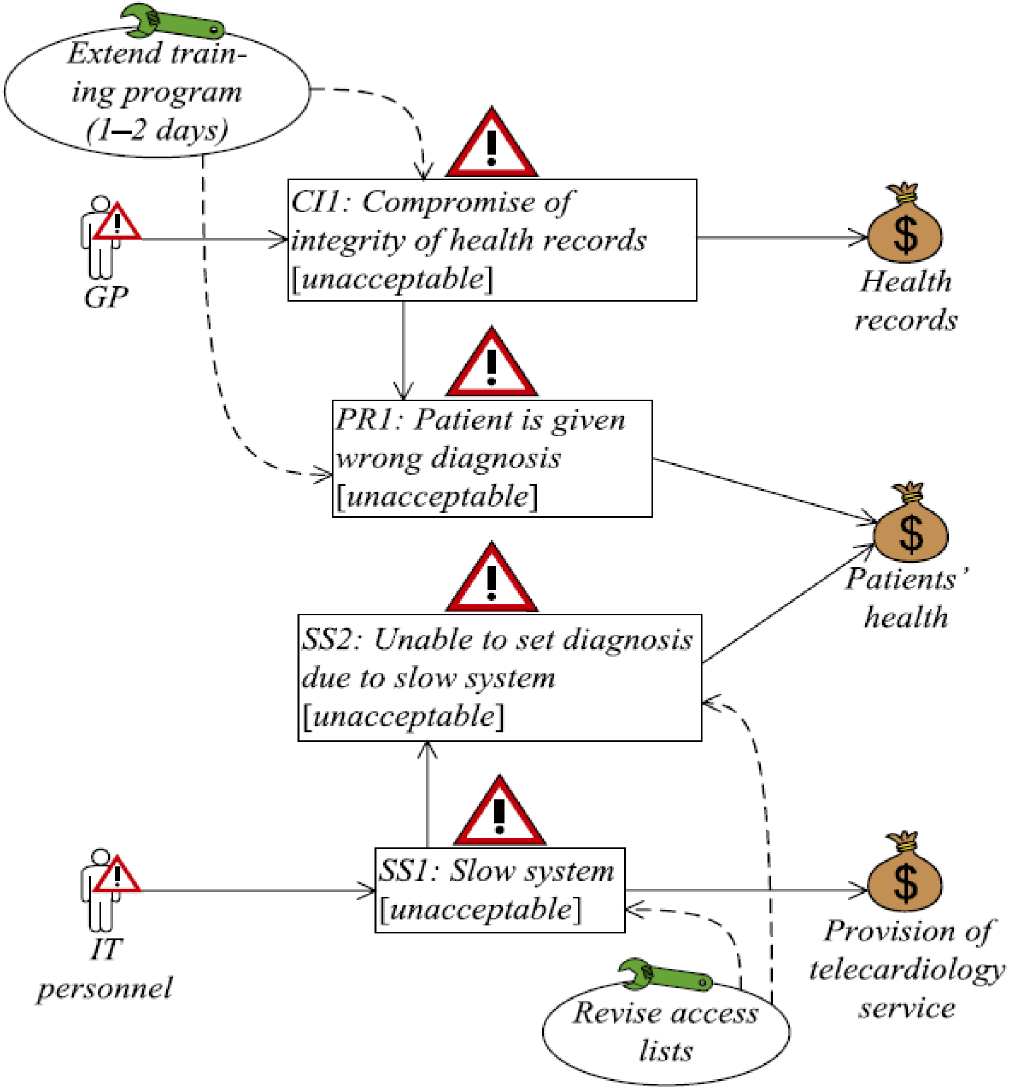
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise (required)
  - Users (required)

Treatment diagram


Extend training program (1–2 days)
GP
Insufficient training
Health record copies stored on local computer
CI1: Compromise of integrity of health records
Health records
Prose-based health records
No input validation
PR1: Patient is given wrong diagnosis
Patients' health
Wrong input in health record
SS2: Unable to set diagnosis due to slow system
IT personnel
Insufficient access control
Lack of competence
Misconfiguration of system
SS1: Slow system
Provision of telecardiology service
Revise access lists

Treatment overview diagram


Extend training program (1–2 days)
GP
CI1: Compromise of integrity of health records [unacceptable]
Health records
PR1: Patient is given wrong diagnosis [unacceptable]
Patients' health
SS2: Unable to set diagnosis due to slow system [unacceptable]
SS1: Slow system [unacceptable]
IT personnel
Provision of telecardiology service
Revise access lists

The CORAS web page

- publications
- tool download

- http://coras.sourceforge.net/