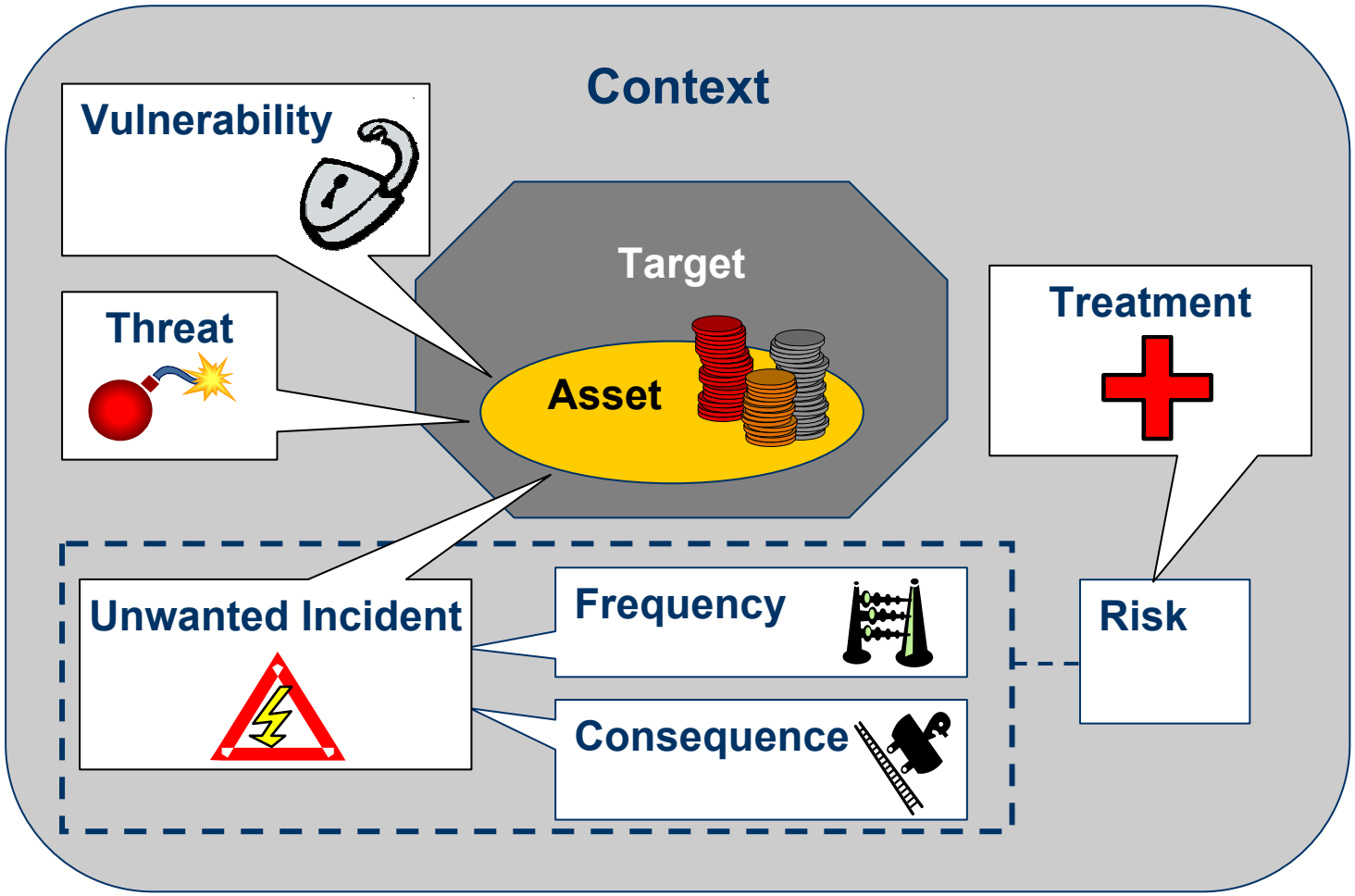
Security analysis — an introduction to CORAS

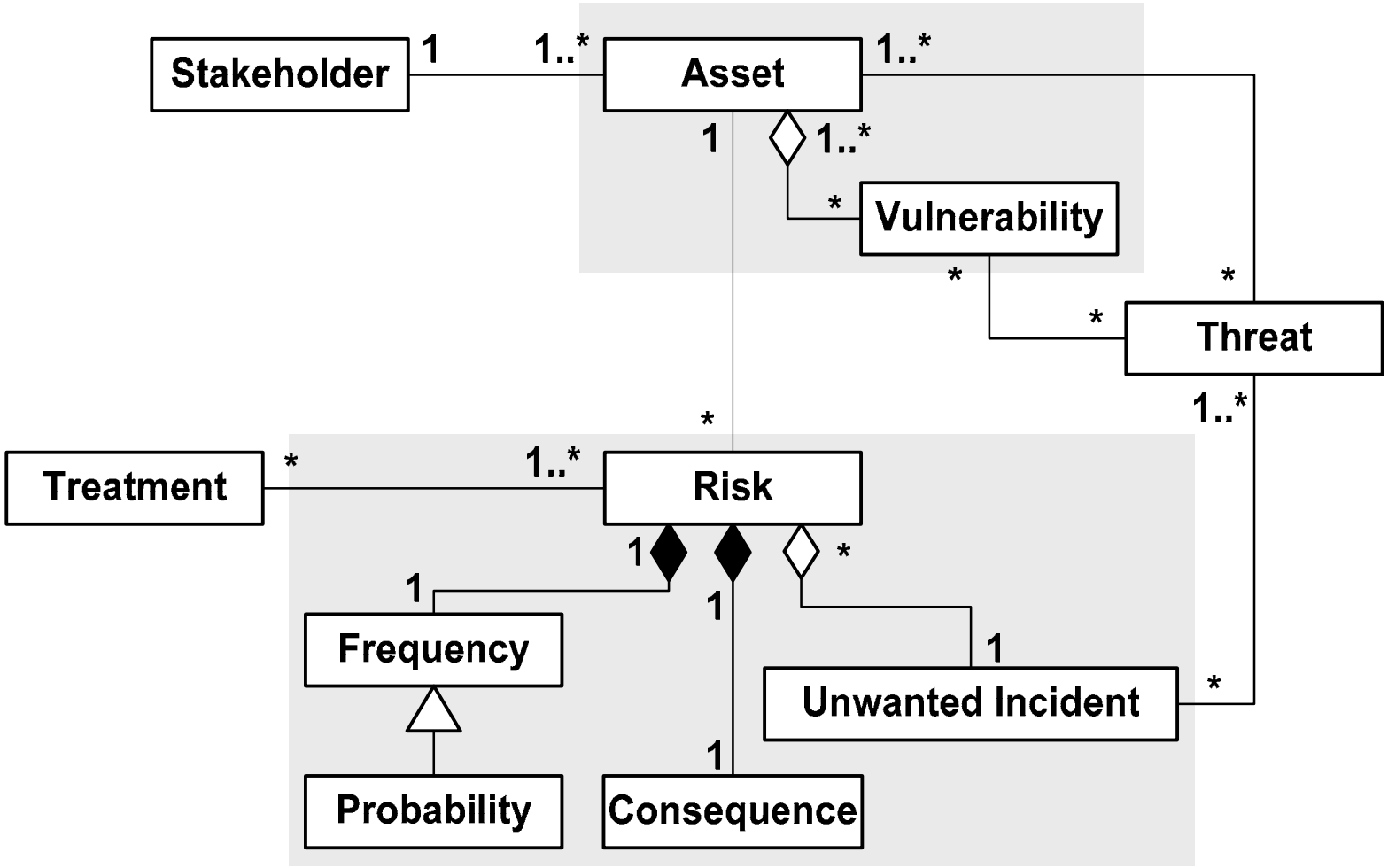
November 3, 2006

Ketil Stølen, SINTEF & UiO

Elements of risk analysis



Conceptual model for risk analysis



CORAS background

- Research and technological development project under the Information Society Technologies (IST) Programme
- January 2001 -> July 2003
- 11 partners from 4 European countries

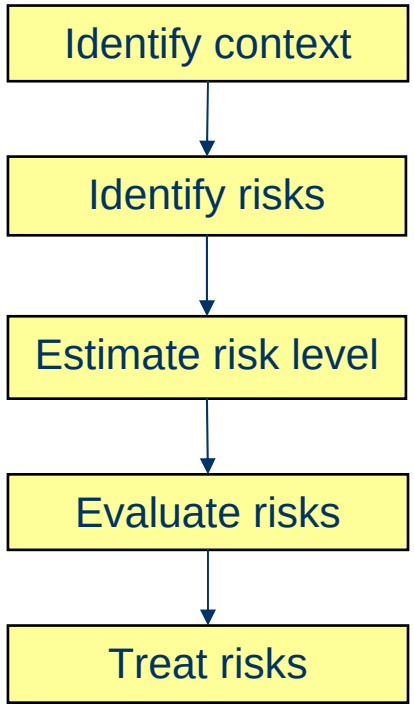
- Goal: Develop an improved methodology for precise, unambiguous, and efficient risk analysis of security critical IT systems

SECURIS - The CORAS follow up project

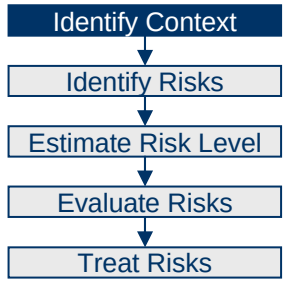
- Funded by the Research Council of Norway (2003-2007)
  - Aims to test security risk analysis methods for IT systems
  - Major industrial partners in field trials:
    - Vessel classification company: a web based information sharing service
    - Telecom company: mobile access to personal information
    - Energy company: a control and supervisory system
    - Metal production company: a web based control and supervisory system

CORAS methodology

- Risk management process based on AS/NZS 4360
- Provides *process* and *guidelines* for risk analysis

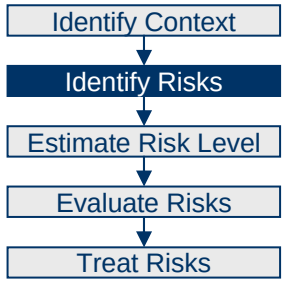


Context identification



- 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 acceptance criteria
  - There will always be risks, but what losses can the client tolerate?
  - Similar to requirements in system development

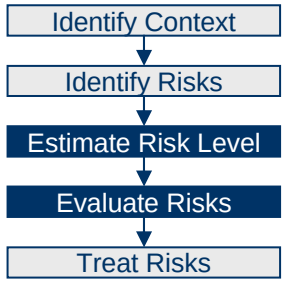
Risk identification



- 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?
- …

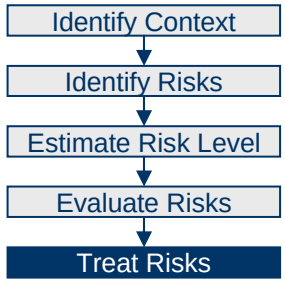
Risk evaluation



- 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 frequency 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

The CORAS Security Risk Modeling Language

- Joint work with Ida Hogganvik
- Has been influences by a number of SINTEF researchers, in particular by Mass Soldal Lund (who designed the first version of the language, the so-called CORAS UML Profile)

- Structure of presentation of the CORAS Language
  - Why do we need a graphical approach in security analysis?
  - Our approach
  - Empirical investigations
    - *Experiences from using the approach in industrial field-trials*
    - *Experiments on which major design decisions have been based*

Background

- Security analysis
  - Structured brainstorming:
    - a step-wise walk through of the analysis object to identify potential threats, vulnerabilities, unwanted incidents, risks.
  - Participants:
    - developers, users, decision makers etc.
    - have thorough knowledge of the analysis object (different parts)
    - often no experience with security analysis
    - often not used to communicate with each other
  - We need a way of supporting the analysis process and documenting their findings

Motivation

- Why is documenting a security analysis so important?
  - Documentation is used ***during*** the analysis to:
    - support the process
    - share and communicate information
    - achieve a common understanding of the target of analysis
  - Documentation is used ***after*** the analysis to:
    - demonstrate that the process was conducted properly
    - provide evidence for a systematic approach
    - keep a record of risks and develop the organization's knowledge base
    - provide the decision makers with a risk management plan
    - facilitate continuous monitoring and review

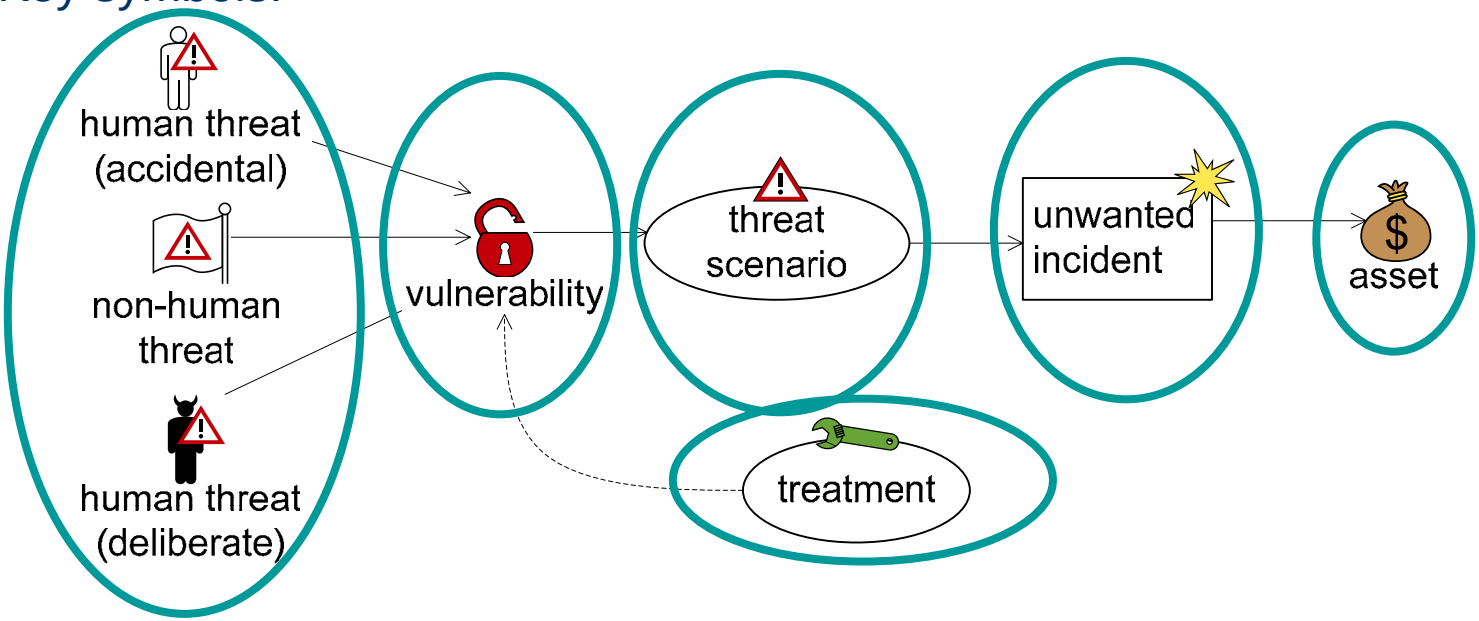
More motivation

- Traditional documentation methods in risk analysis are often only based on text and tables
- We believe graphical models are more useful in structured brainstorming:
  - suitable for capturing information “on-the-fly”
  - understandable for people without technical background
  - can quickly give the reader an overview of the risk picture

Our approach:
the CORAS security risk modeling language

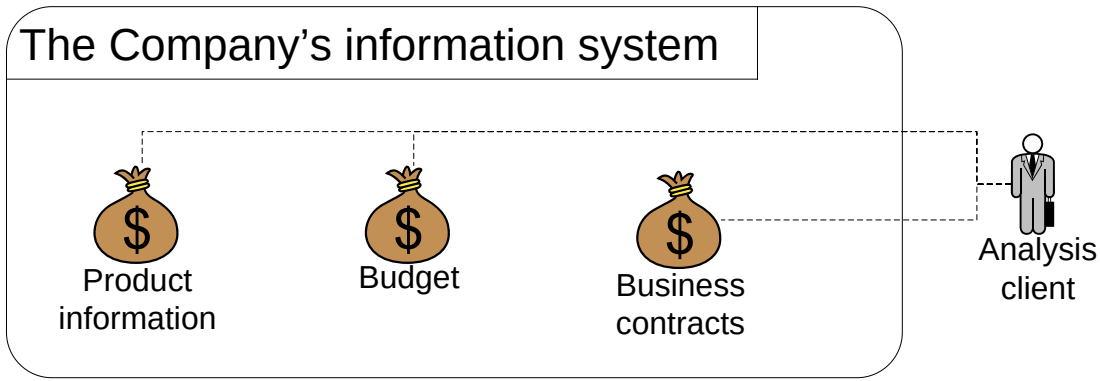
- Specifies a common security risk picture for the object analyzed:
  - shows potential unwanted incidents, threats, vulnerabilities
  - supports estimation of risks (how often may the risk occur and how serious is it?)
- Developed iteratively in the SECURIS project based on:
  - experiences from field trials
  - results from empirical experiments

- Key symbols:



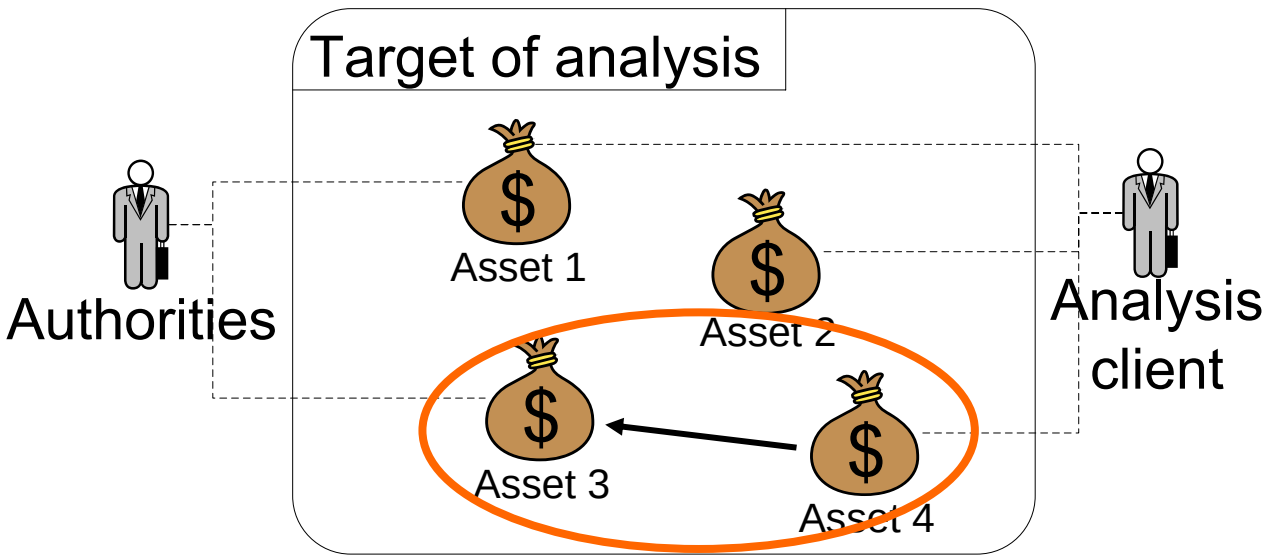
Identifying and documenting assets:

- Asset: *something of value that needs protection*
- The client specifies its assets and risk acceptance levels
- Difficult, - faults may jeopardize the whole analysis
  - wrong focus
  - wrong level of details



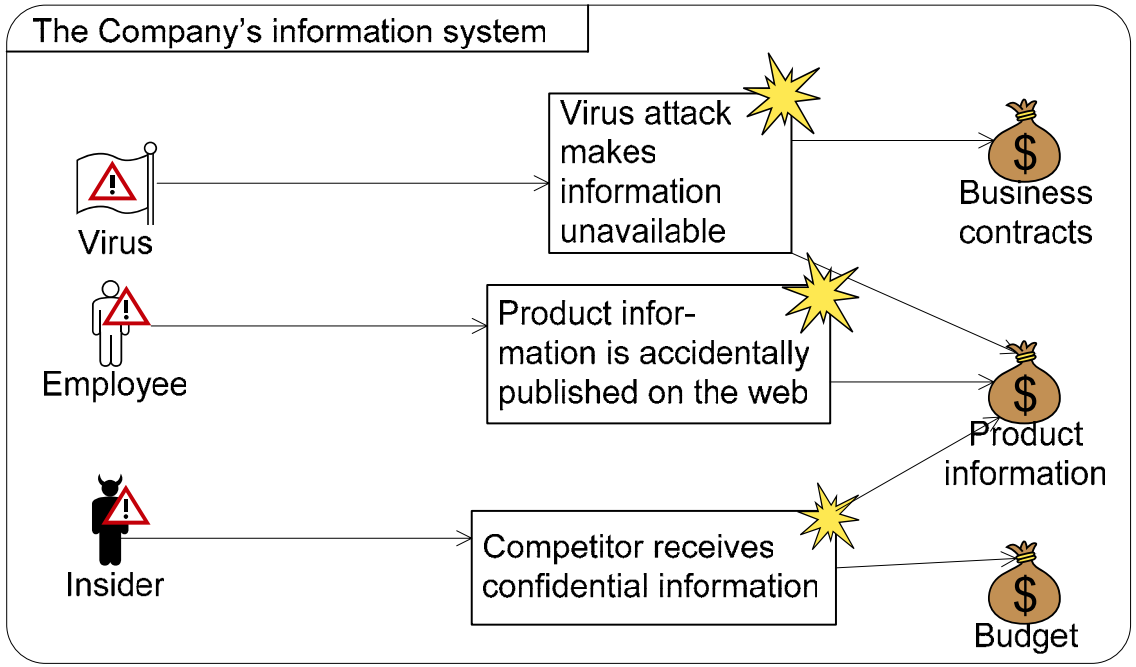
Identifying and documenting assets:

- One may also specify other interested parties than the client
- Possible to specify how assets can depend on other assets
  - company reputation
  - income



Identifying and documenting threats and unwanted incidents in threat diagrams:

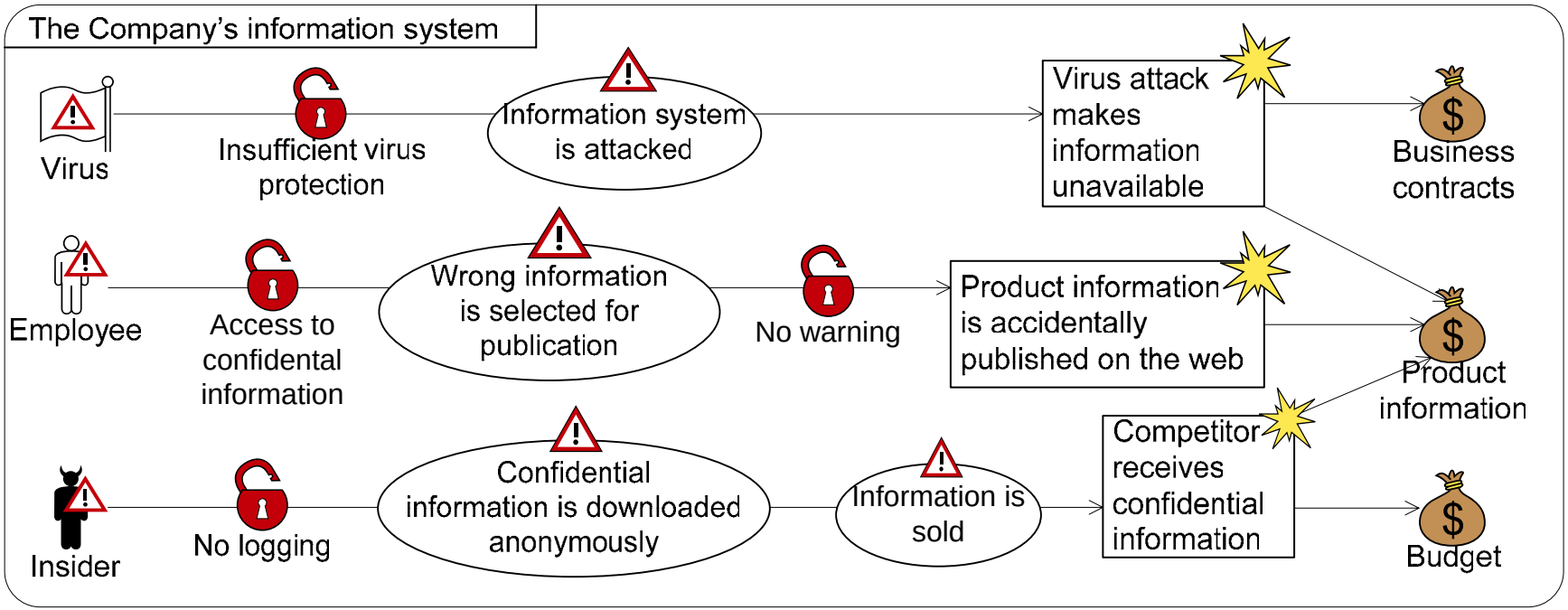
- **Threat**: *something or someone that may cause harm to the assets*
- **Unwanted incident**: *an incident that harms one or more assets*



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

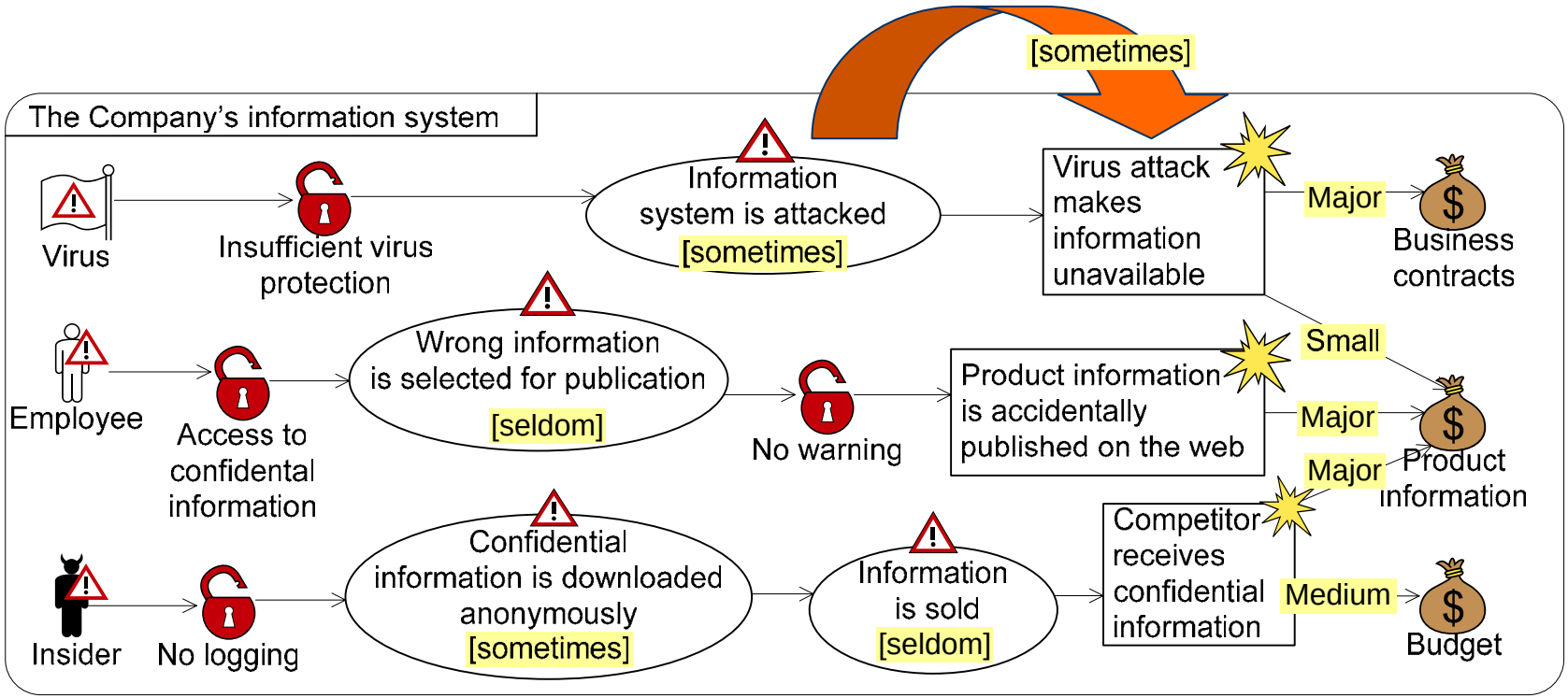
Identifying and documenting vulnerabilities and threat scenarios

- **Vulnerability**: *a weakness or deficiency that may be exploited*
- **Threat scenario**: *a description of how the threat acts*
- Forces the participants to specify “why” incidents can happen (vulnerabilities) and “how” (threat scenarios)
- Impossible or wrong paths are likely to be discovered



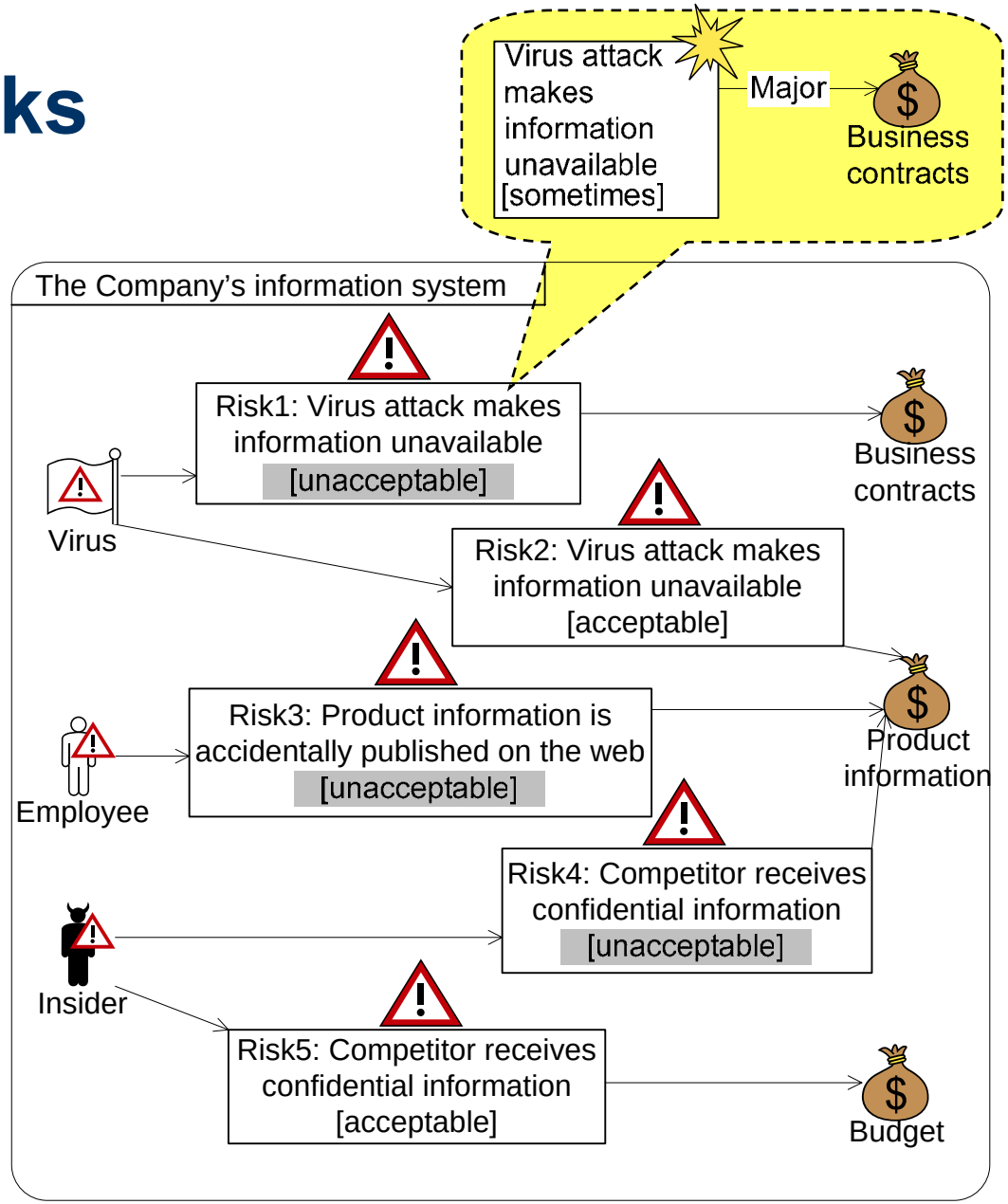
Identifying and documenting likelihood and consequences:

- **Likelihood:** *how often may something occur*
- **Consequence:** *potential damage to an asset*
- Capturing the rationale for the likelihood estimates



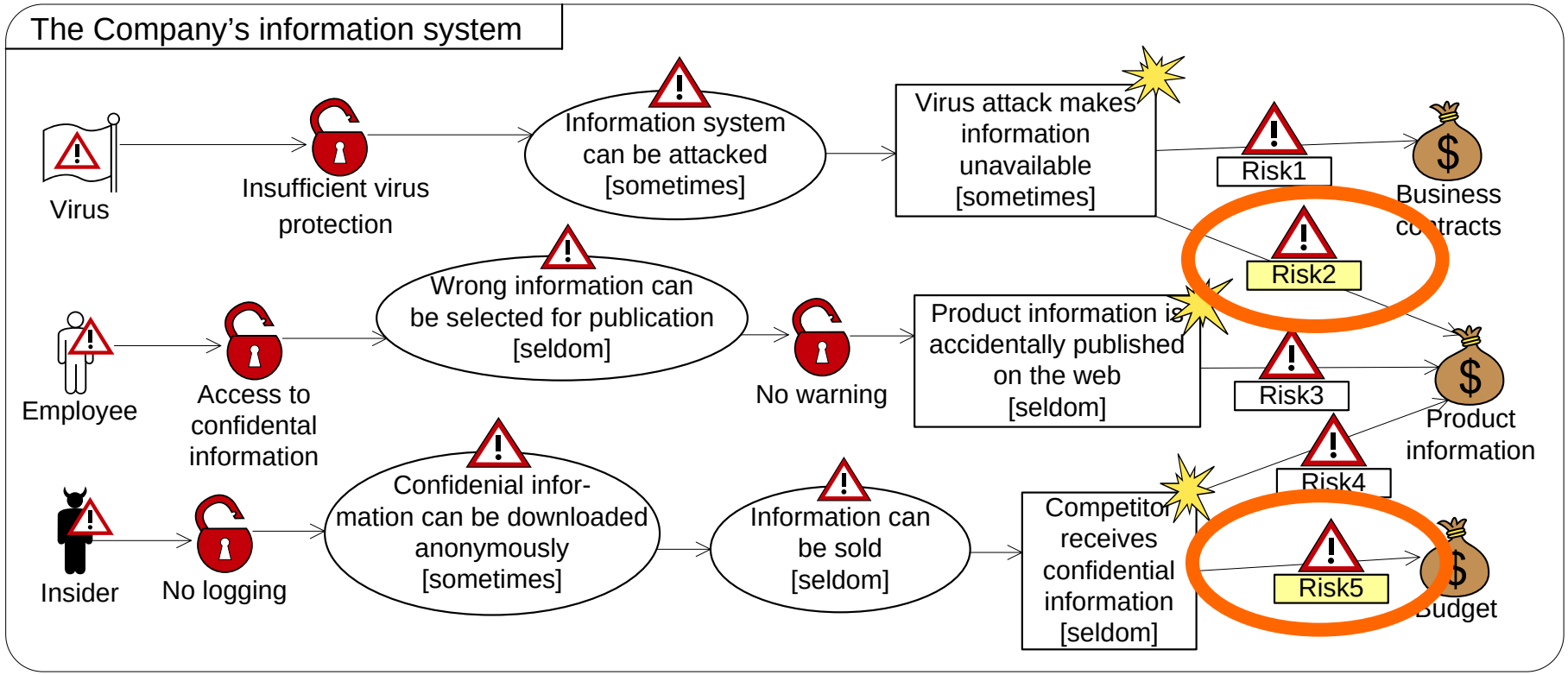
Documenting risks

- **Risk**: *an unwanted incident that has been given a likelihood and consequence estimate*
- Compared to the client's risk acceptance levels
- Acceptable and non-acceptable risks are shown in a risk overview
  - decision makers
  - planning treatments
  - communicating risks



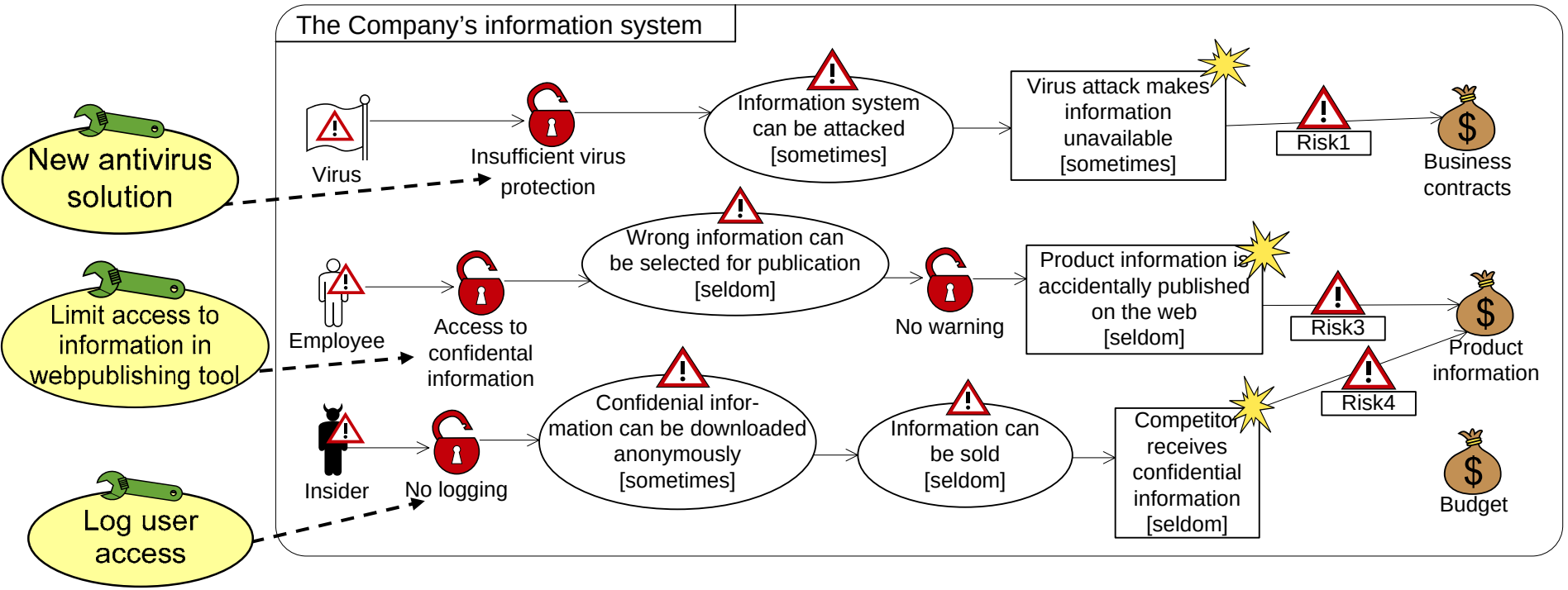
Identifying and documenting risk treatments

- 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 action that should mitigate the risk*
- Treatments are added where they should have effect



Experiences from field trials:

- Increased commitment from the participants
- Contributed to more effective communication between the different participants
- A useful visualization technique, suitable for presentation purposes
- Brings more focus to the message/purpose of the analysis
- A precise specification of risks, especially the chain of events between a threat and an unwanted incident
- Contributed to a more detailed documentation of the risk picture

Empirical investigations

Issue	Some findings
1. Comprehensibility of the terminology model (I)	Revised the model on the basis of the results to make it more comprehensible. (31 students as subjects)
2. Use of special risk icons	Those receiving material with special icons managed to complete more tasks than the others. (25 students as subjects)

Empirical investigations

Issue	Some findings
3. Comprehensibility of the terminology model (II)	Likelihood (and other frequency measures) is the least understood concept. Asset and vulnerability are best understood. (34 professionals, 23 students as subjects)
4. Modeling preferences	Textual information labels are often preferred over graphical means in the models. (33 professionals as subjects)

Various information

- Next lecture on Security Analysis: The seven steps of the CORAS method
- Based on Chapter 2 of
  - The CORAS Model-based Method for Security Risk Analysis
  - A report of 91 pages available on the INF5150 webpage
- INF5150 Group on Tuesday
  - More on STAIRS and refinement
  - Excercises will be made available tomorrow
- The CORAS Tool will be made available on Tuesday next week
- Further detailing of the security analysis part of Drop II will also be made available on Tuesday next week