Security analysis: The CORAS Approach

October 31, 2008

Ketil Stølen, SINTEF & UiO

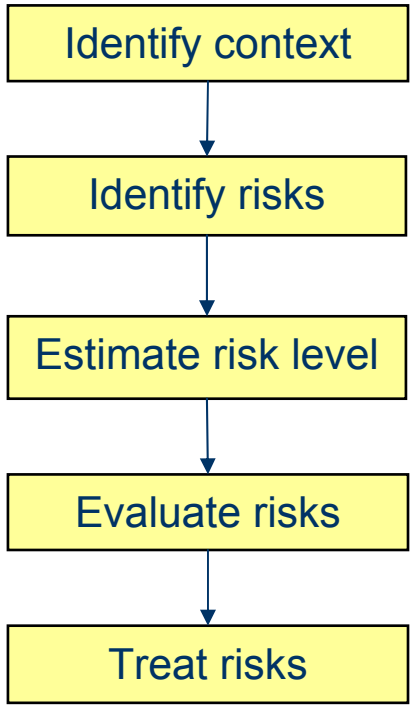
What is CORAS?

- 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 calculus
  - A set of rules for reasoning about diagrams
- The CORAS editor
  - A computerized tool supporting the drawing of diagrams
- The CORAS guideline
  - A guideline for best use of the language within the process

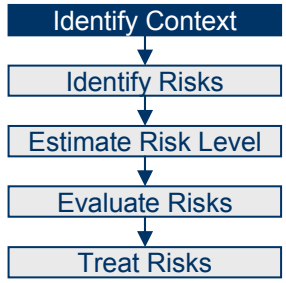
The CORAS process

The CORAS process

- Risk analysis process based on the standard AS/NZS 4360: Risk Management

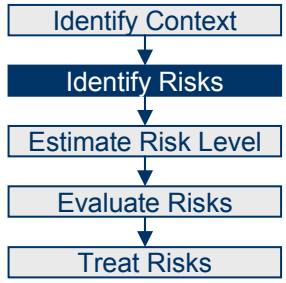


Context identification



- 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
  - What losses can the client tolerate?
  - Similar to requirements in system development

Risk identification

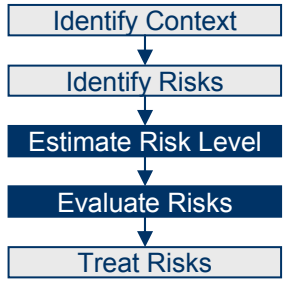


- Identify threats to assets through structured brainstorming
  - Involves decision makers, users, developers, domain experts, risk analysis experts, etc. (typically 5-7 people)
- Identify vulnerabilities of assets
  - Questionnaires and checklists

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?
- …

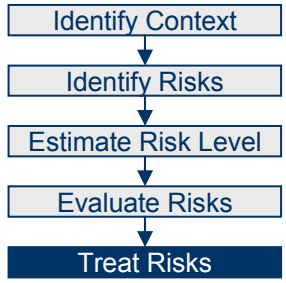
Risk evaluation



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

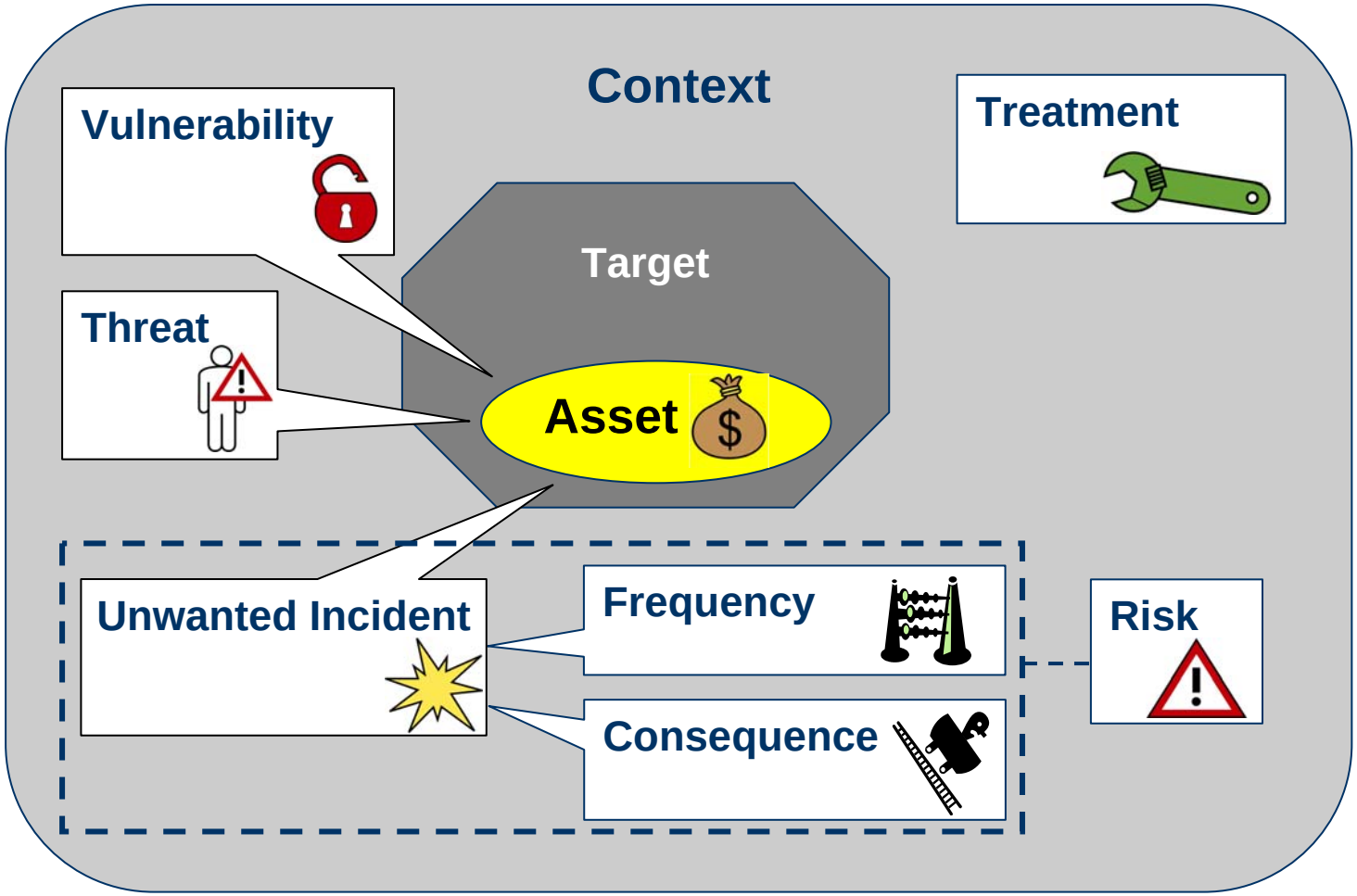
- Risk level is determined based on analysis of the frequency and consequence of the unwanted incident
  - Quantitative values: e.g., loss of 1M€, 25% chance per year
  - Qualitative values: e.g., high, medium, low

Risk treatment



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

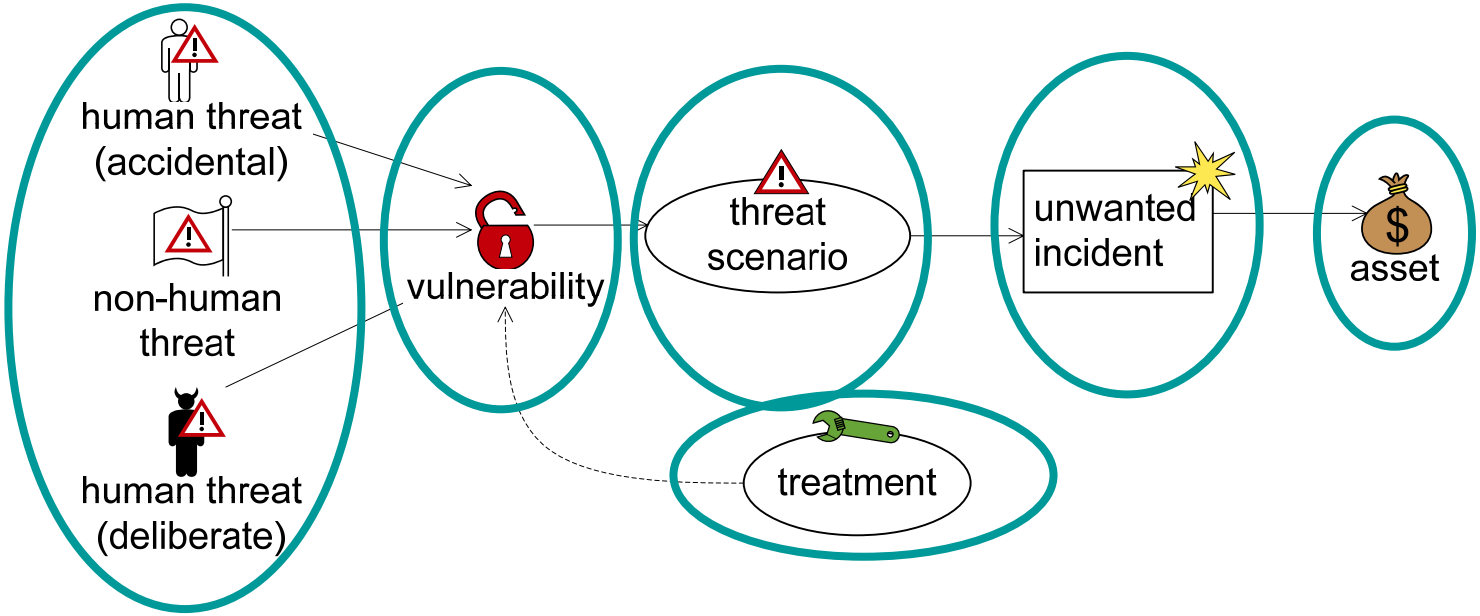
Elements of security risk analysis



The CORAS language (diagrams)

The CORAS security risk modeling language

- Key symbols:

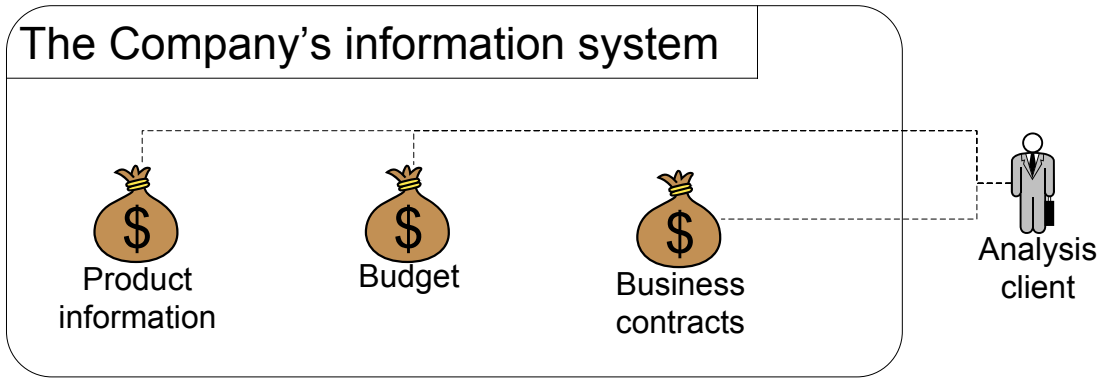


The CORAS diagrams

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

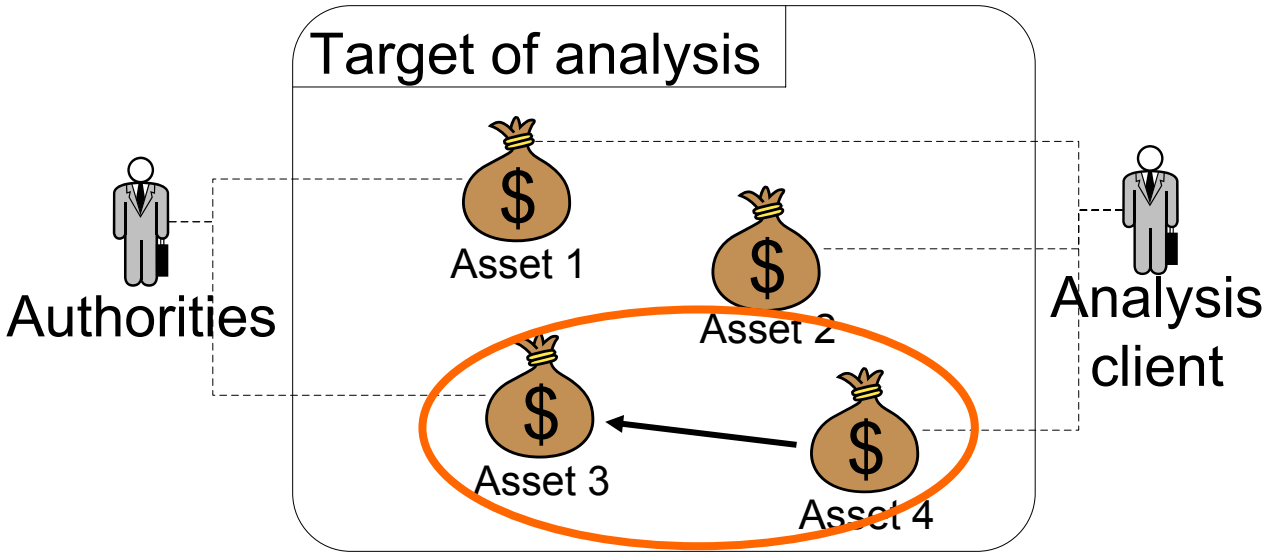
Identifying and documenting assets

- 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



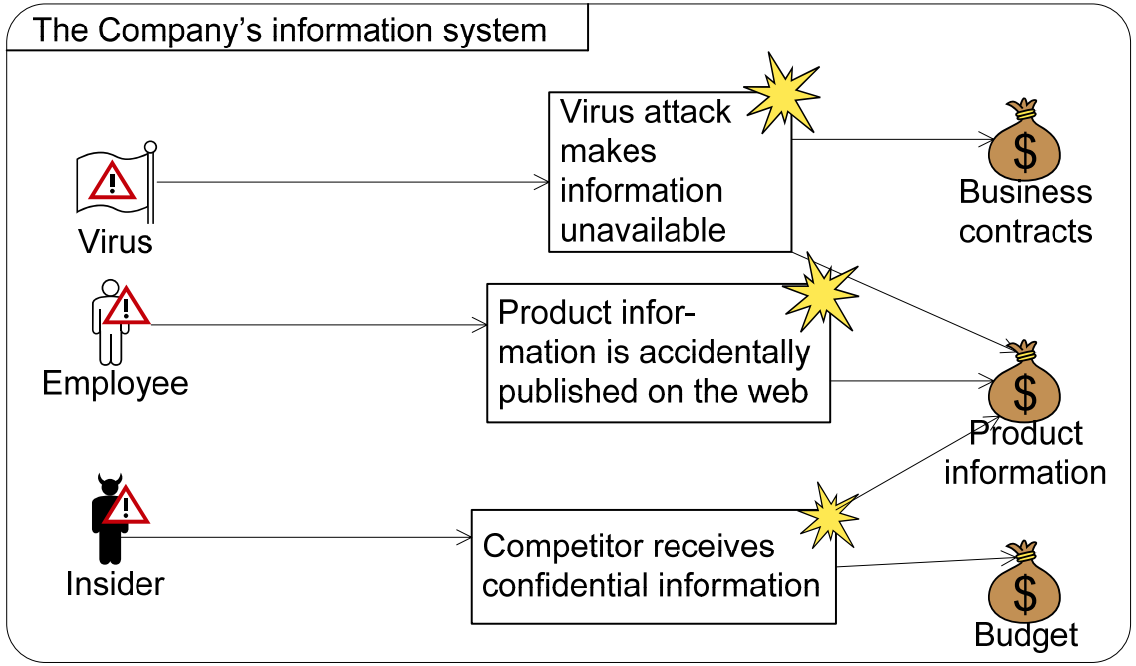
Identifying and documenting assets

- 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

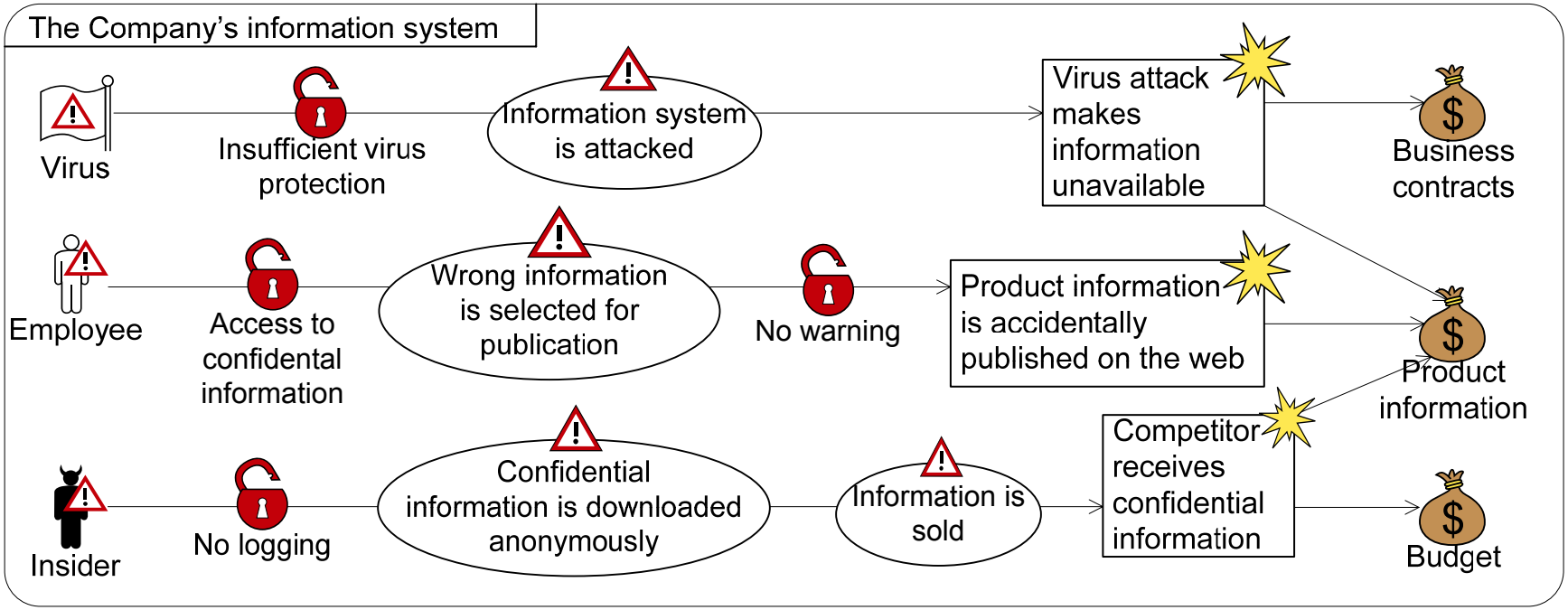
- **Threat**: *something or someone that may cause harm to the assets*
- **Unwanted incident**: *an incident that harms one or more assets*



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

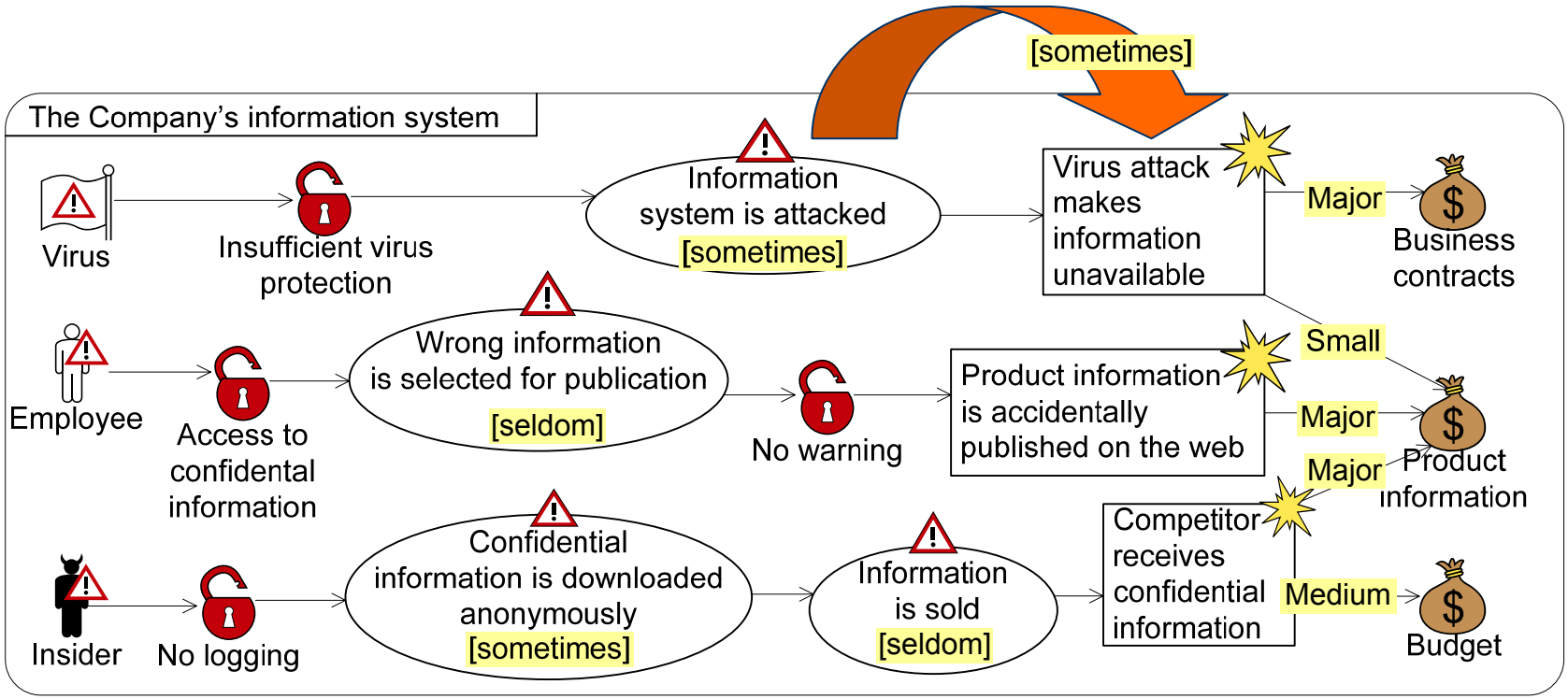
Identifying and documenting vulnerabilities and threat scenarios

- **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



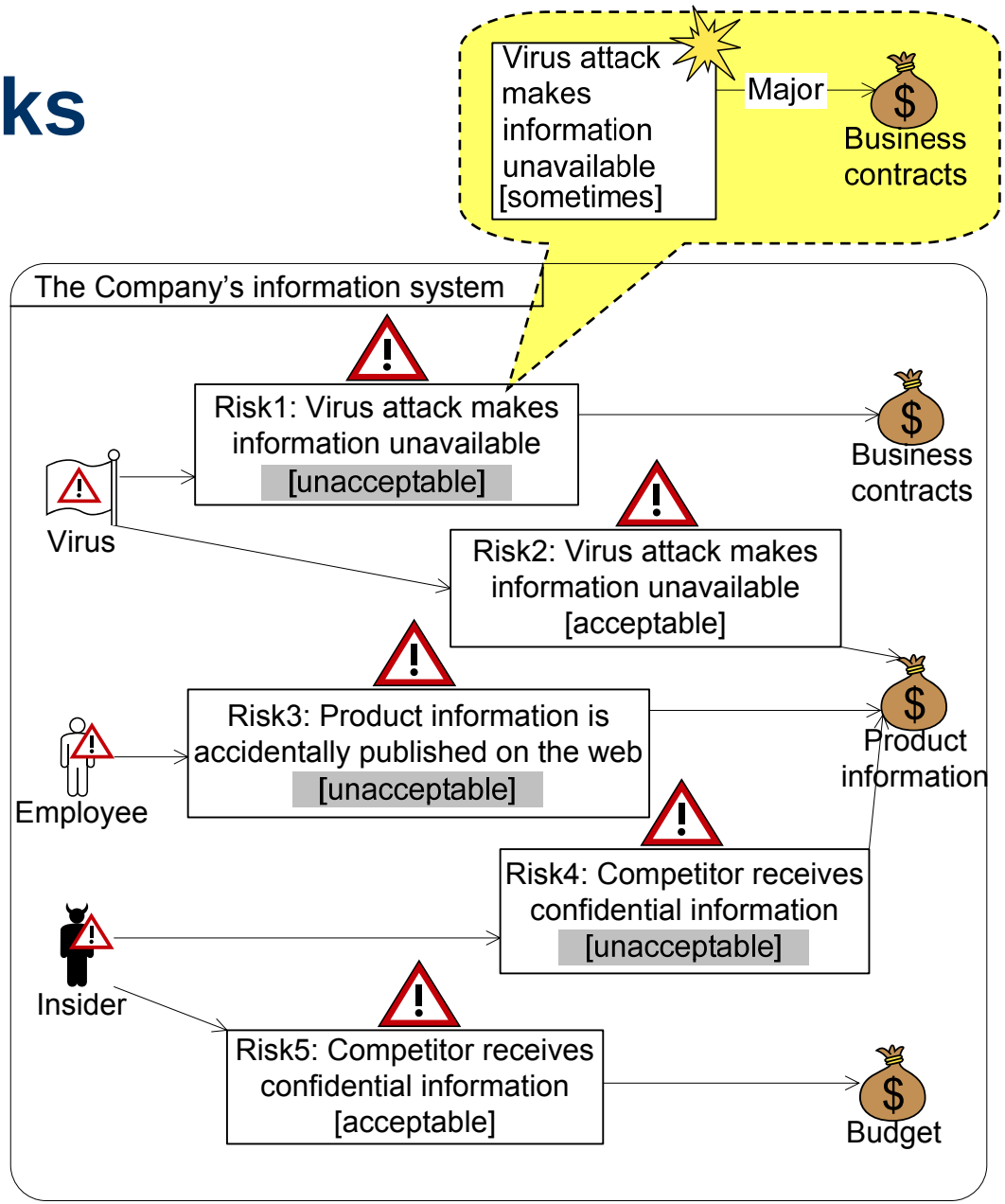
Identifying and documenting likelihoods and consequences

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



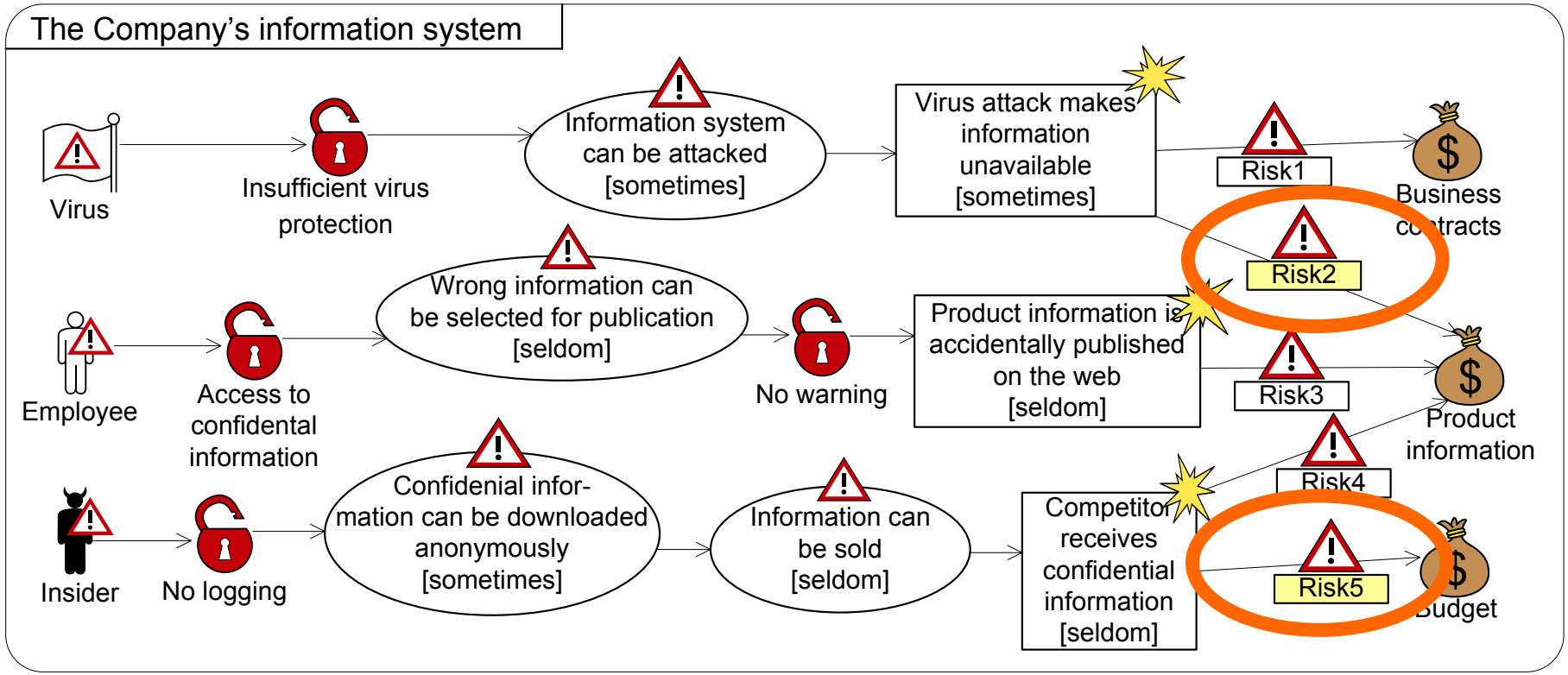
Documenting risks

- **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



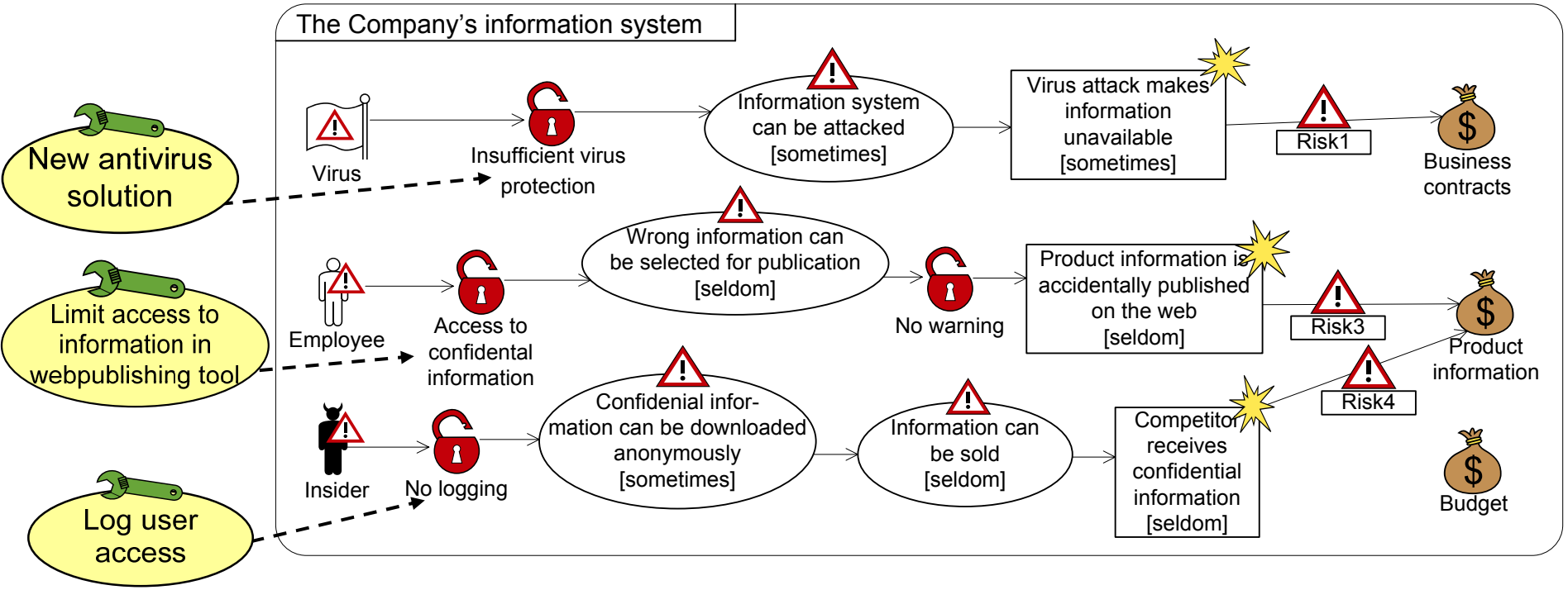
Identifying and documenting risk treatments

- 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

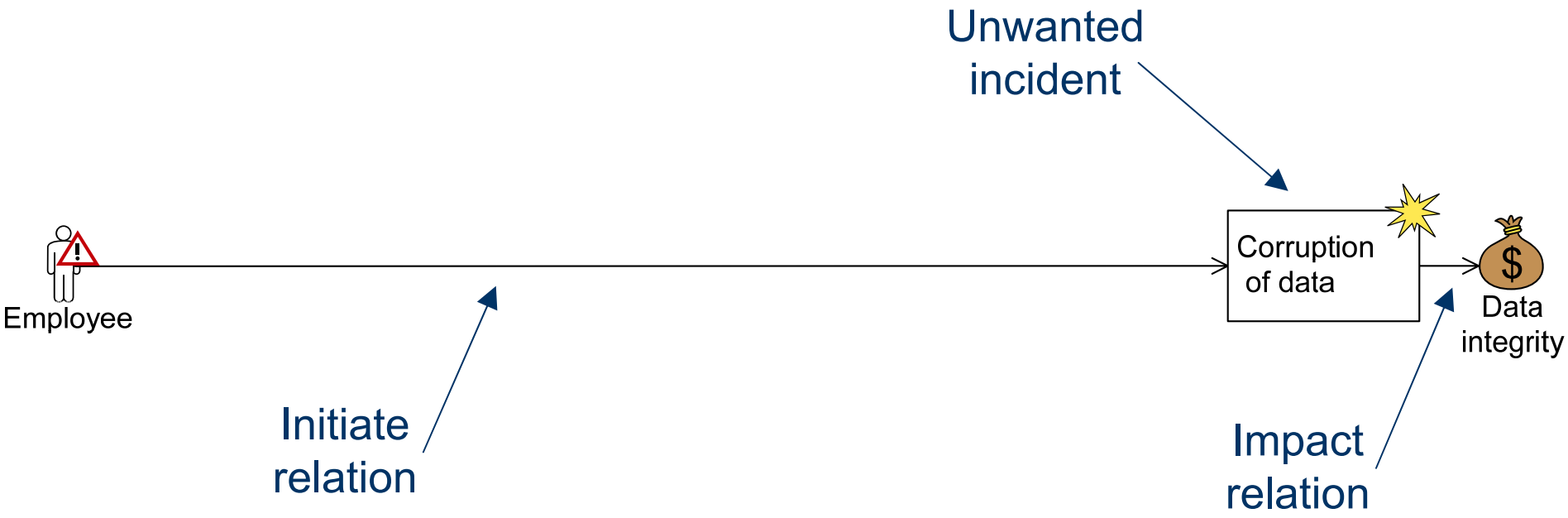
- **Risk treatment**: *an action that should mitigate the risk*
- Treatments are added where they should have effect



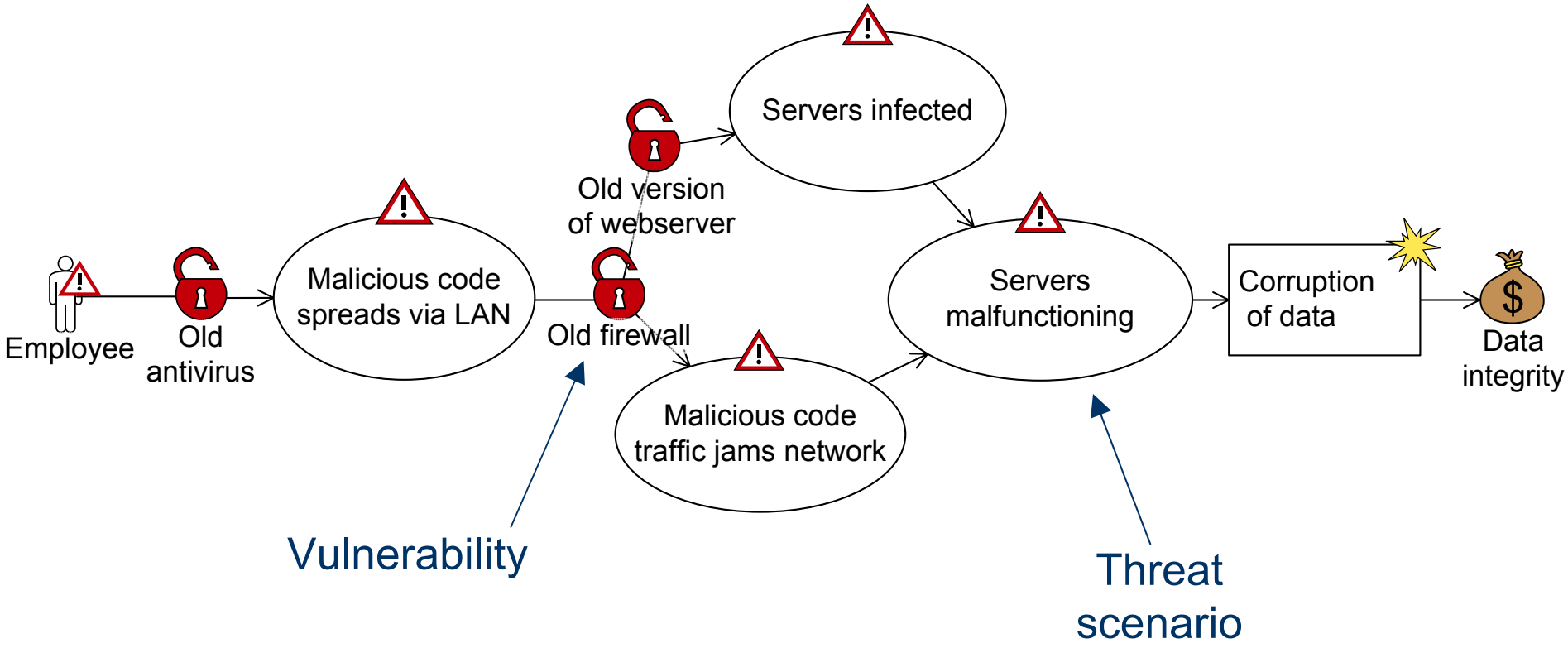
The CORAS semantics

Building a threat diagram (1)

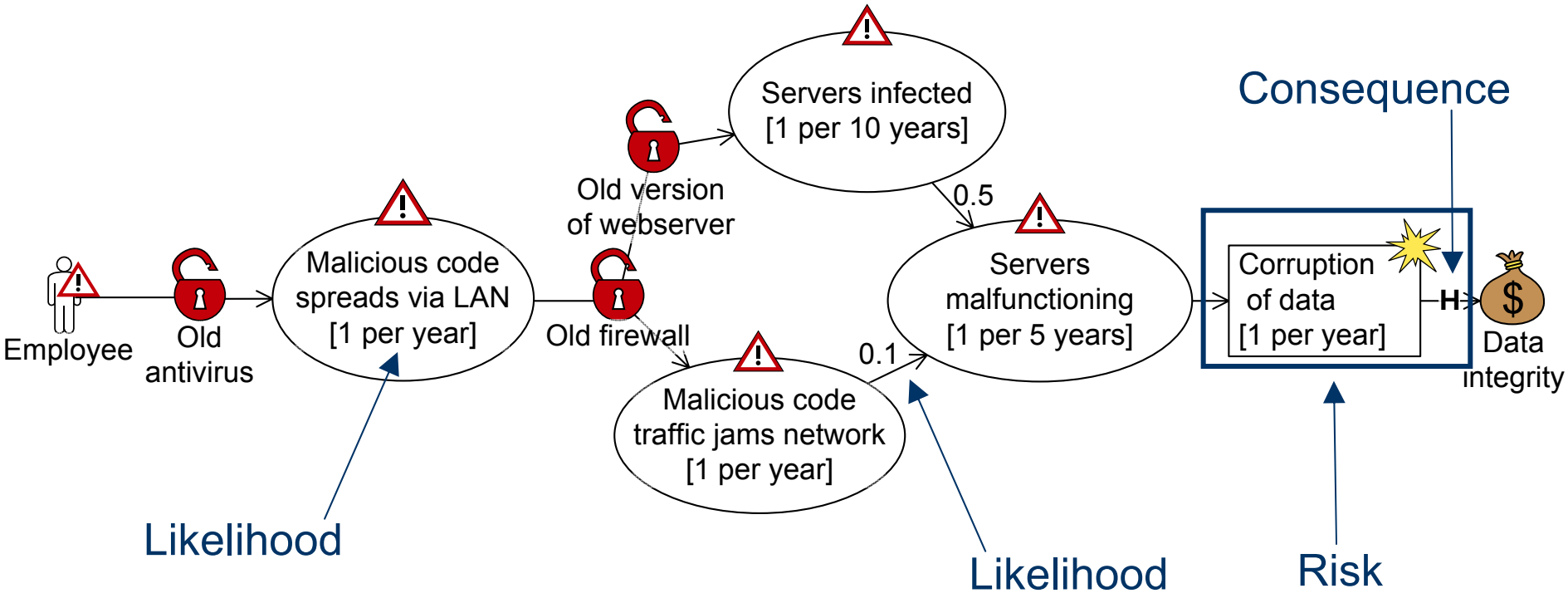
Building a threat diagram (2)



Building a threat diagram (3)



Building a threat diagram (4)



How do we interpret this diagram?

How do we interpret CORAS diagrams?

In order to answer this question, we have

- Formulated a textual syntax
  - Defined by Extended BNF grammars
- Defined a structured semantics
  - STEP 1: Translation of a diagram into its textual representation
  - STEP 2: Translation of the textual representation into its meaning as a paragraph in English

Success criteria we defined for the CORAS semantics

- The semantics should be modular
- The translation should be easy to perform
- The resulting English sentences should be easily understandable
- The translation should be possible to automate
- It should be possible to translate any diagram

Semantics of the impact relation

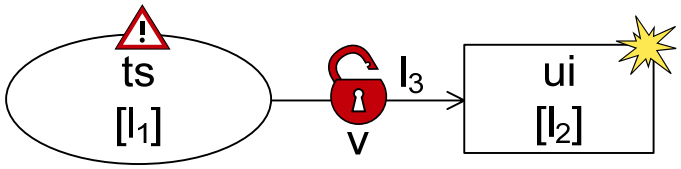
[[ui]] := Unwanted incident ***ui*** occurs with undefined likelihood.

[[a]] := ***a*** is an asset.

[[ui $\xrightarrow{c}$ a]] := ***ui*** impacts ***a*** with [[c]].

[[c]] := consequence ***c***

Semantics of the initiate relation



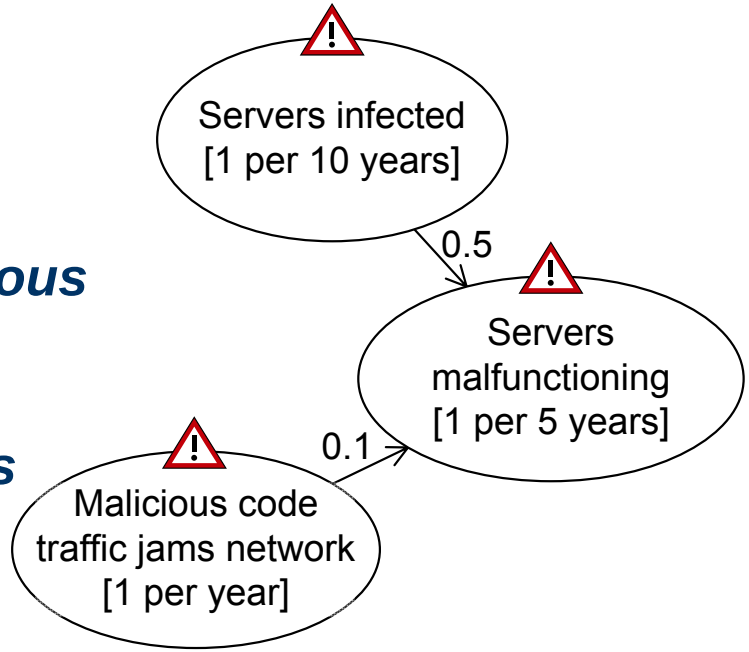
$\Rightarrow$ ts $\xrightarrow{v \; l_3}$ ui

[[ts(l_1)]] := Threat scenario ***ts*** occurs with [[l_1]].
[[ui(l_2)]] := Unwanted incident ***ui*** occurs with [[l_2]].

[[v]] := vulnerability ***v***
[[l]] := likelihood ***l***

[[ts $\xrightarrow{v \; l_3}$ ui]] := ***ts*** leads to ***ui*** with [[l_3]], due to [[v]].

An example



Threat scenario ***Servers infected by malicious code*** occurs with likelihood ***1 per 10 years***.

Threat scenario ***Malicious code traffic jams network*** occurs with likelihood ***1 per year***.

Threat scenario ***Application servers malfunctioning*** occurs with likelihood ***1 per 5 years***.

Servers infected by malicious code leads to ***Application servers malfunctioning*** with likelihood ***0.5***.

Malicious code traffic jams network leads to ***Application servers malfunctioning*** with likelihood ***0.1***.

The CORAS calculus

Initiate rule

If the vertices t and v are related by initiate, we have:

$$\frac{t \xrightarrow{l} v}{(t \sqcap v)(l)}$$

Leads-to rule

If the vertices v_1 and v_2 are related by leads-to, we have:

$$\frac{v_1(f) \quad v_1 \xrightarrow{l} v_2}{(v_1 \sqcap v_2)(f \cdot l)}$$

Mutually exclusive vertices rule

If the vertices v_1 *and* v_2 *are mutually exclusive, we have:*

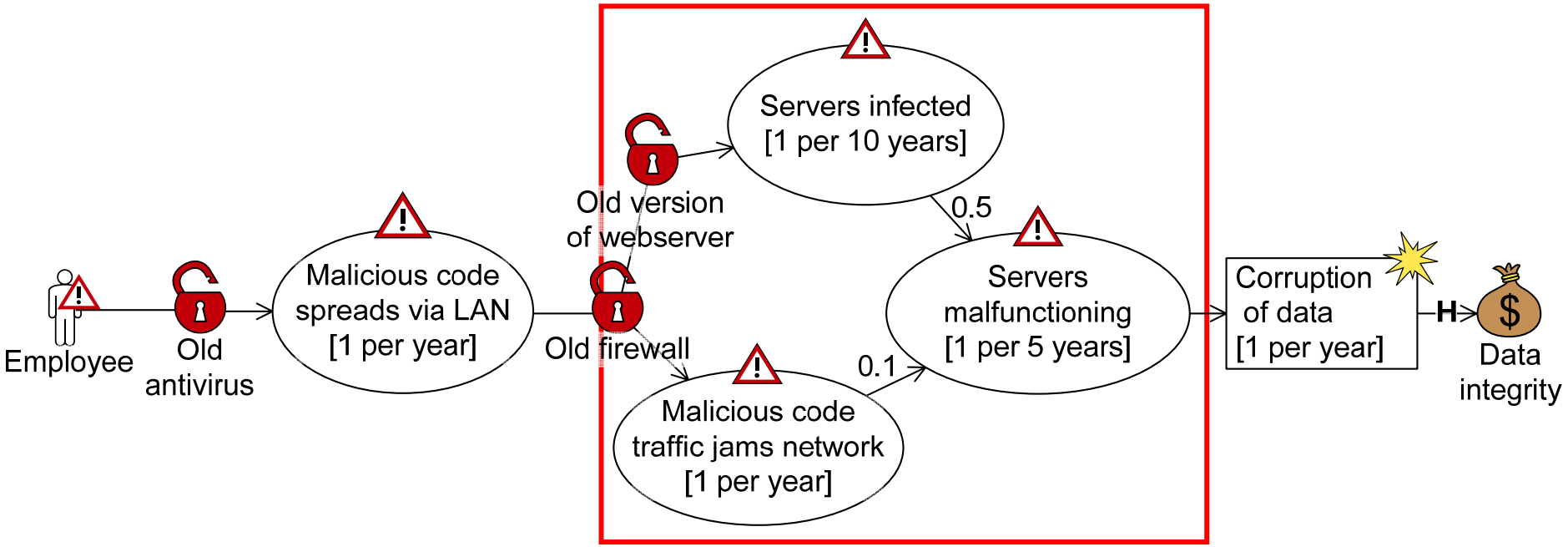
$$\frac{v_1(f_1) \quad v_2(f_2)}{(v_1 \sqcup v_2)(f_1 + f_2)}$$

Independent vertices rule

If the vertices v_1 *and* v_2 *are statistically independent, we have:*

$$\frac{v_1(f_1) \quad v_2(f_2)}{(v_1 \sqcup v_2)(f_1 + f_2 - f_1 \cdot f_2)}$$

Consistency checking of likelihoods



1 per 10 years x 0.5 = 1 per 20 years = 0.05
1 per year x 0.1 = 1 per 10 years = 0.1

Given that the events are statistically independent, we may calculate a minimum for the end node: 1 – (1 – 0.05)(1 – 0.1) = 0.145

1 per 5 years = 0.2 > 0.145

If the events had been mutually exclusive the minimum would have been 0.05 + 0.1 = 0.15

The CORAS editor

CORAS editor v.2.0.b5

Download from:

http://coras.sourceforge.net/downloads.html

Hints for use of the CORAS editor

- The CORAS editor is built on the idea that a diagram is a view of a model
- A CORAS editor file (.dgx) therefore contains a model and zero or more diagrams (views of the model)
- When a file is opened in the editor, each diagram (view of the model) is shown in a tab

- THE FOLLOWING FUNCTIONALITY DOES NOT WORK PROPERLY, SO DO NOT USE IT
  - Never have more then one diagram in a .dgx file
  - Never use the ”New Diagram” function in the editor
  - If you are working on two diagrams at the same time, have the diagrams in separate files and work with two instances of the editor
  - When you delete an element from a diagram, do not use the Delete-button, but right click on the element and chose ”Delete From Model” (and not ”Delete From Diagram”)