The CORAS method for security risk analysis

ESSCaSS 2008

NODES Tutorial

28/8-08

Heidi E. I. Dahl

SINTEF

SINTEF

- Norwegian research group with 2000 employees from 55 different countries
- More than 90 percent of our earnings come from contracts for industry and the public sector, and from project grants from the Research Council of Norway
- Research divisions
  - Health Research
  - Technology and Society
  - ICT
  - Materials and Chemistry
  - Building and Infrastructure

  } SINTEF Foundation

  - Marine
  - Petroleum and Energy

  } Limited companies

SINTEF ICT
> Cooperative and Trusted Systems
> Quality and Security Technology

- Model based security analysis
- Model driven security architecture
- Trust management
- Tools for analysis and documentation
- Empirical research on methods and tools to build secure systems

- Security risk analysis – CORAS
  - Method
  - Language (textual syntax, semantics, calculus)
  - Usability and Security

Outline

- Security risk analysis
- An example driven introduction to the CORAS method
- CORAS resources

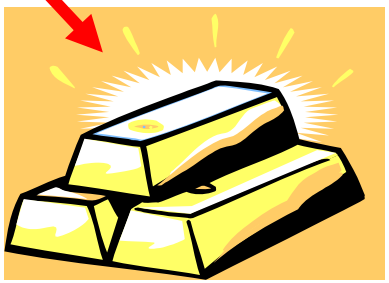
The example

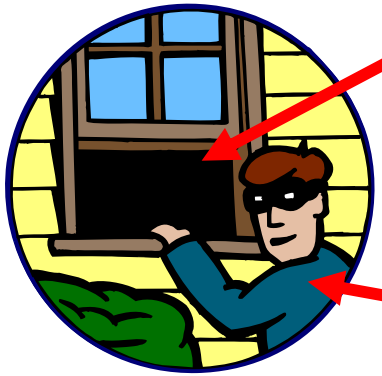
- A PhD student is worried about losing the work she has done on her thesis
- The Big Corporation funding her work is worried that sensitive business information will reach its competitors

- They decide to do a security risk analysis to determine whether the risk level is acceptable

Why do we analyse security risks?

asset, something of value





vulnerability

threat

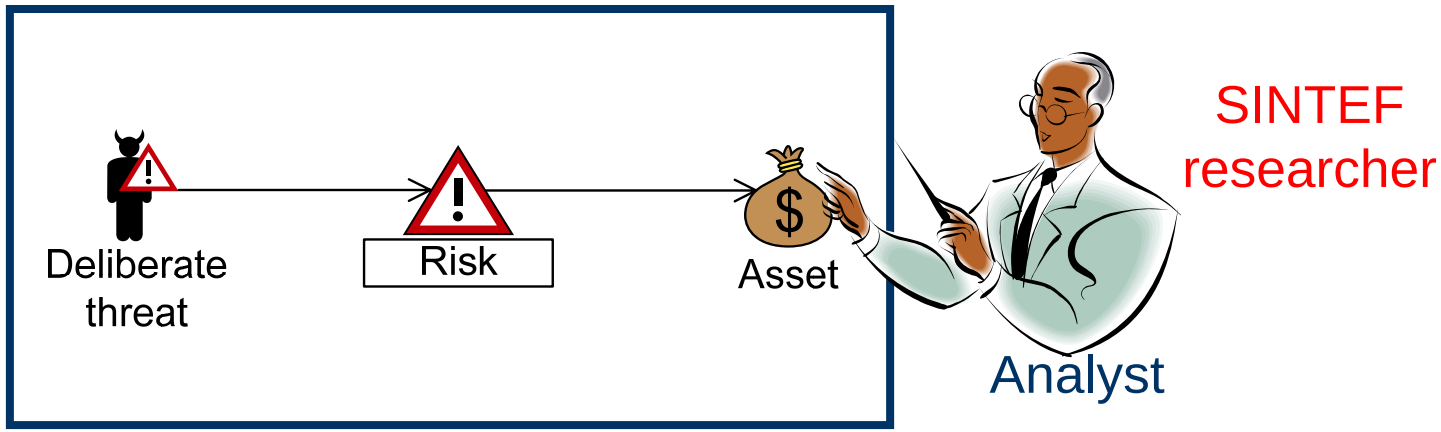
reduced risk level

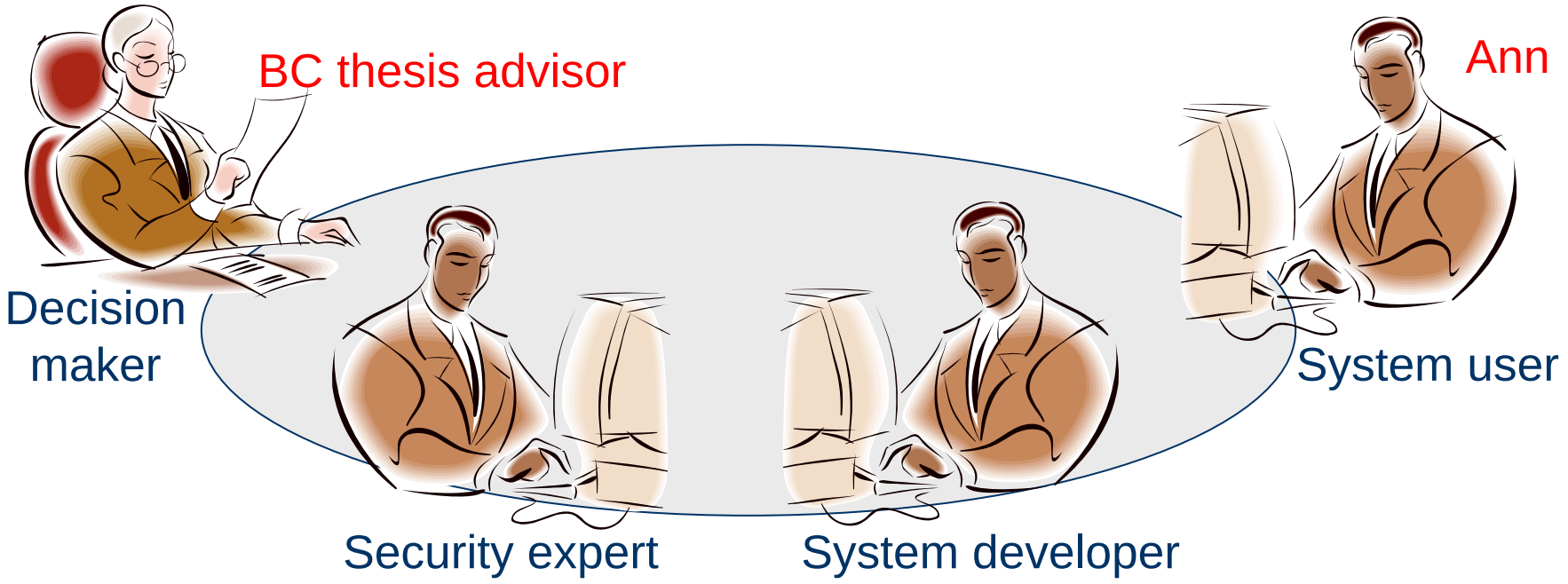
constitutes a security risk

we need to introduce security mechanisms

75 % of all sensitive data losses are caused by human error

Taking Action to Protect Sensitive Data,
IT Policy Compliance Group, 2007


Deliberate threat
Risk
Asset
SINTEF researcher
Analyst


BC thesis advisor
Ann
Decision maker
System user
Security expert
System developer
BC security expert

The CORAS method

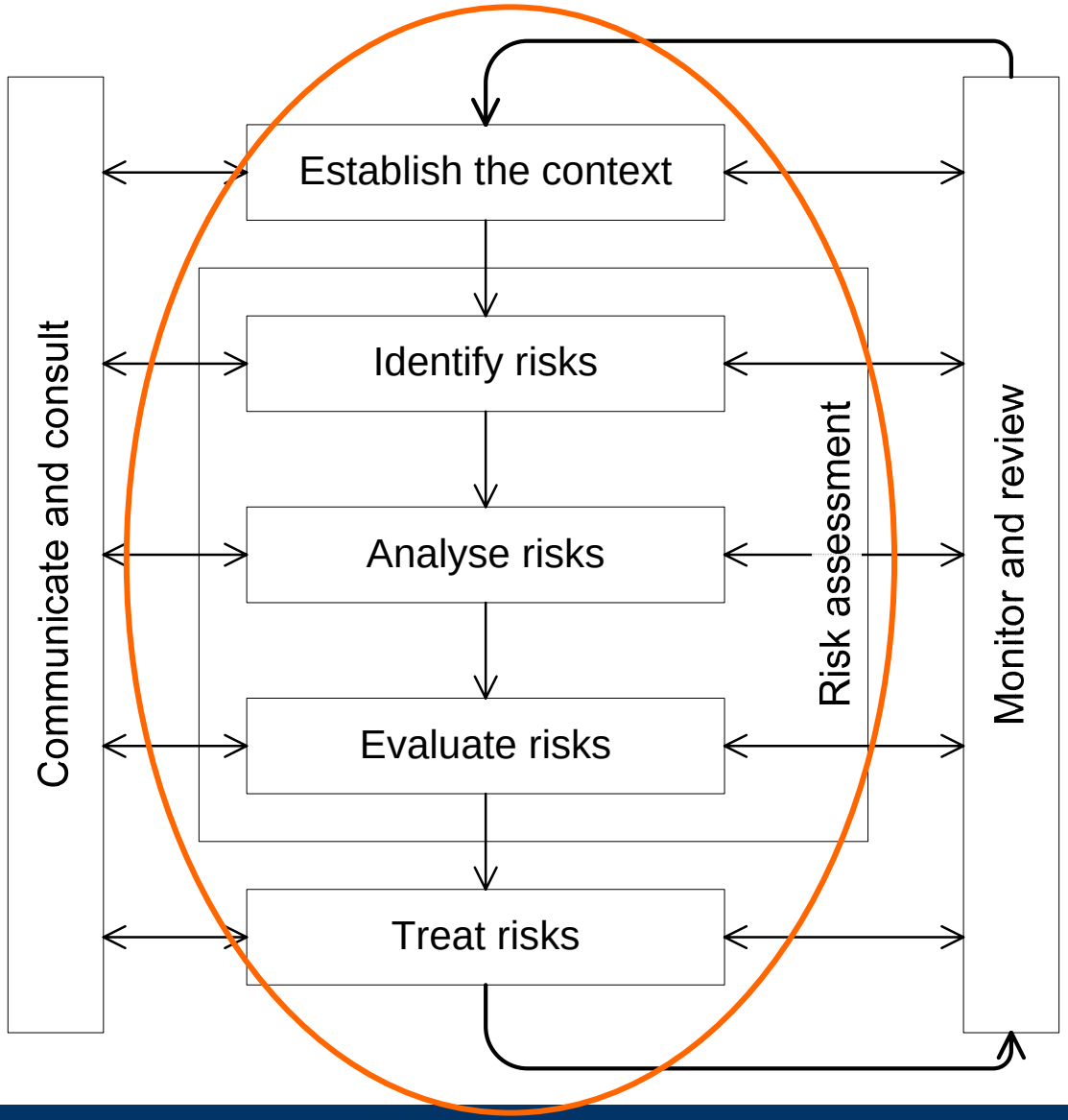
Model based method for security risk analysis that provides

- a customized graphical language for threat and risk modelling
- a diagram editor
- detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis

CORAS

- has been developed through both empirical investigations and a series of industrial field studies (projects financed by the Norwegian Research Council and the EU)
- is based on international standards for risk management (e.g. AS/NZS 4360:2004)

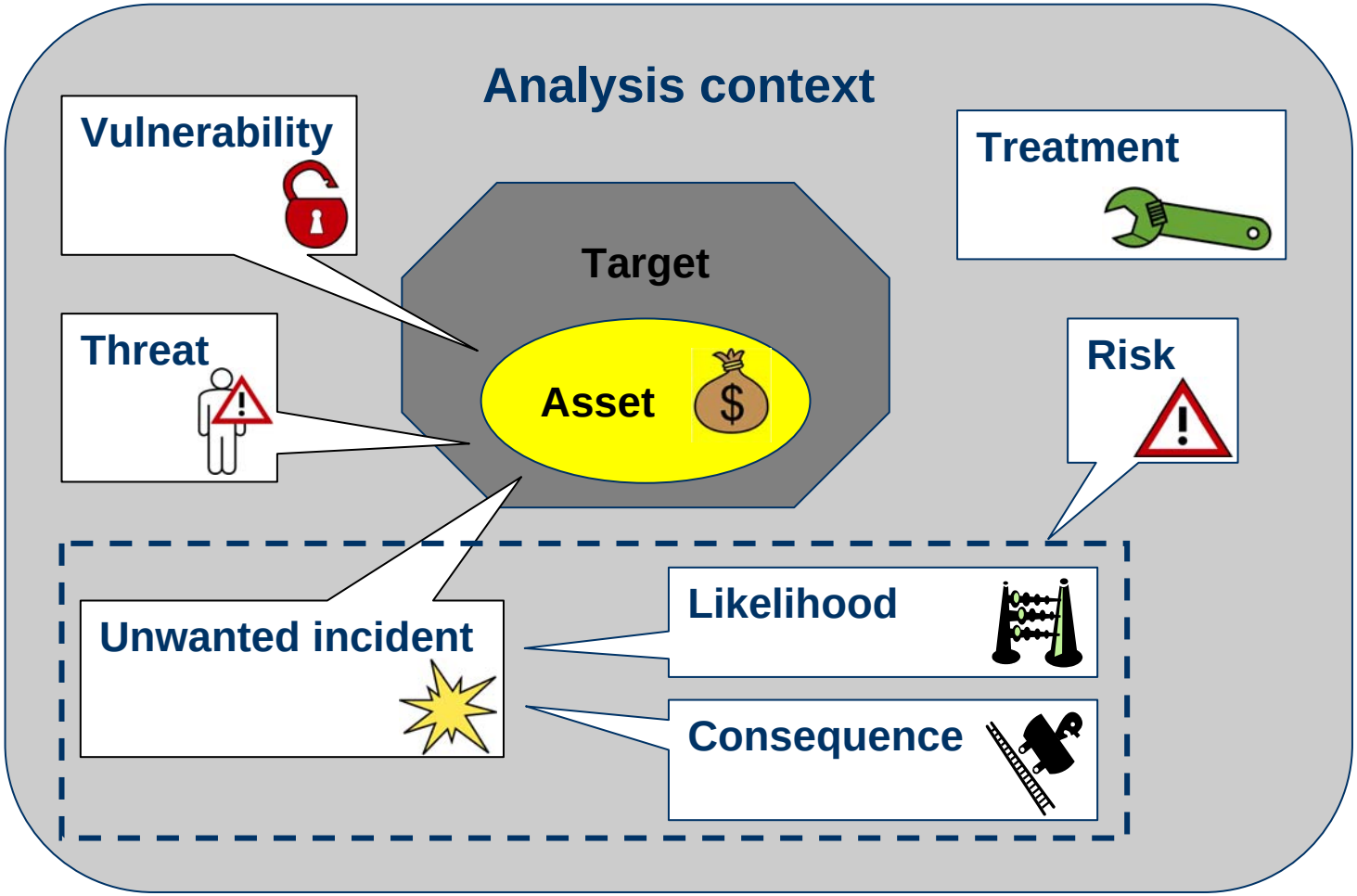
The standard analysis process



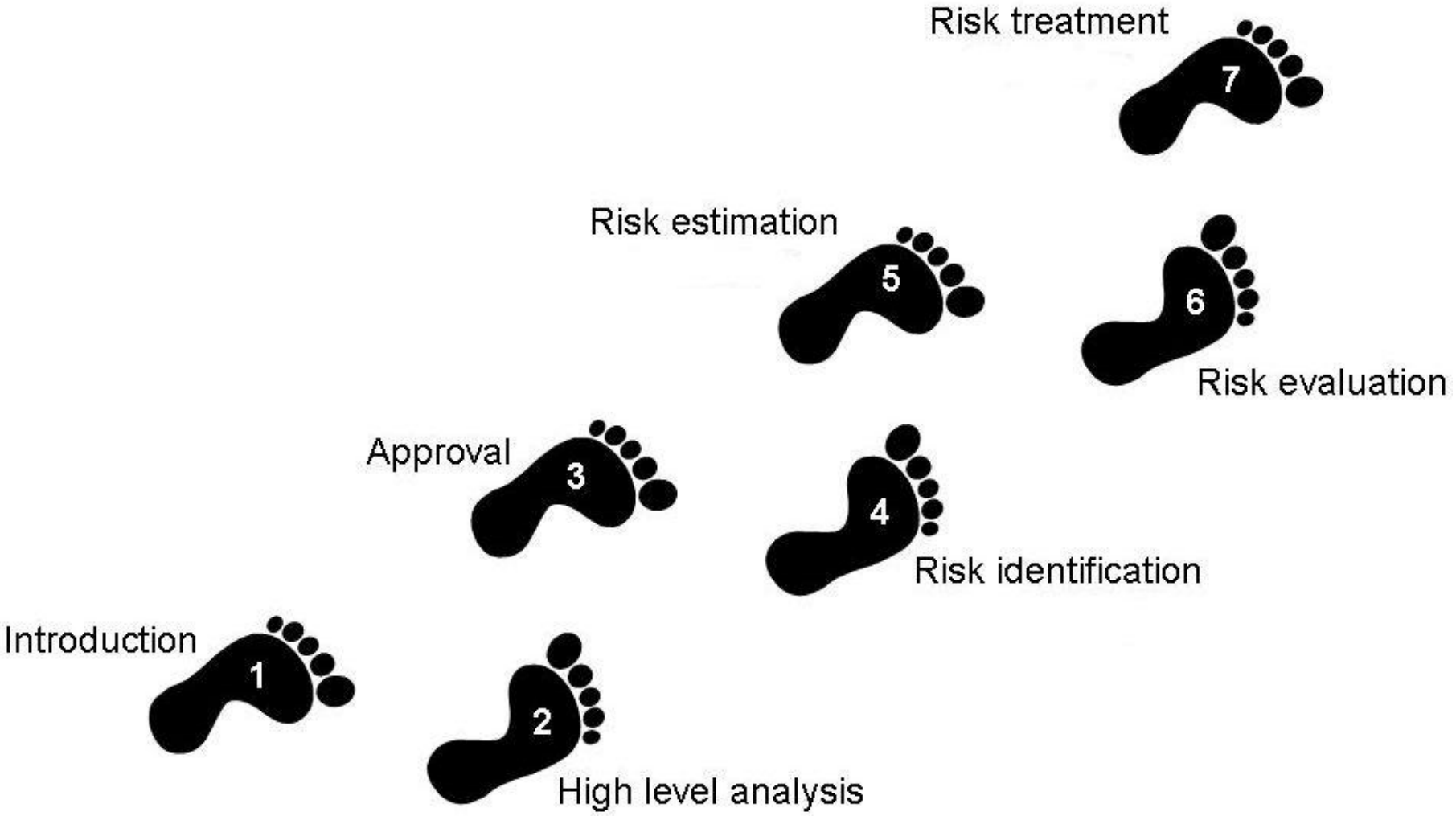
from the *Australian Risk Management Standard*

AS/NZS 4360:2004

Elements of the analysis



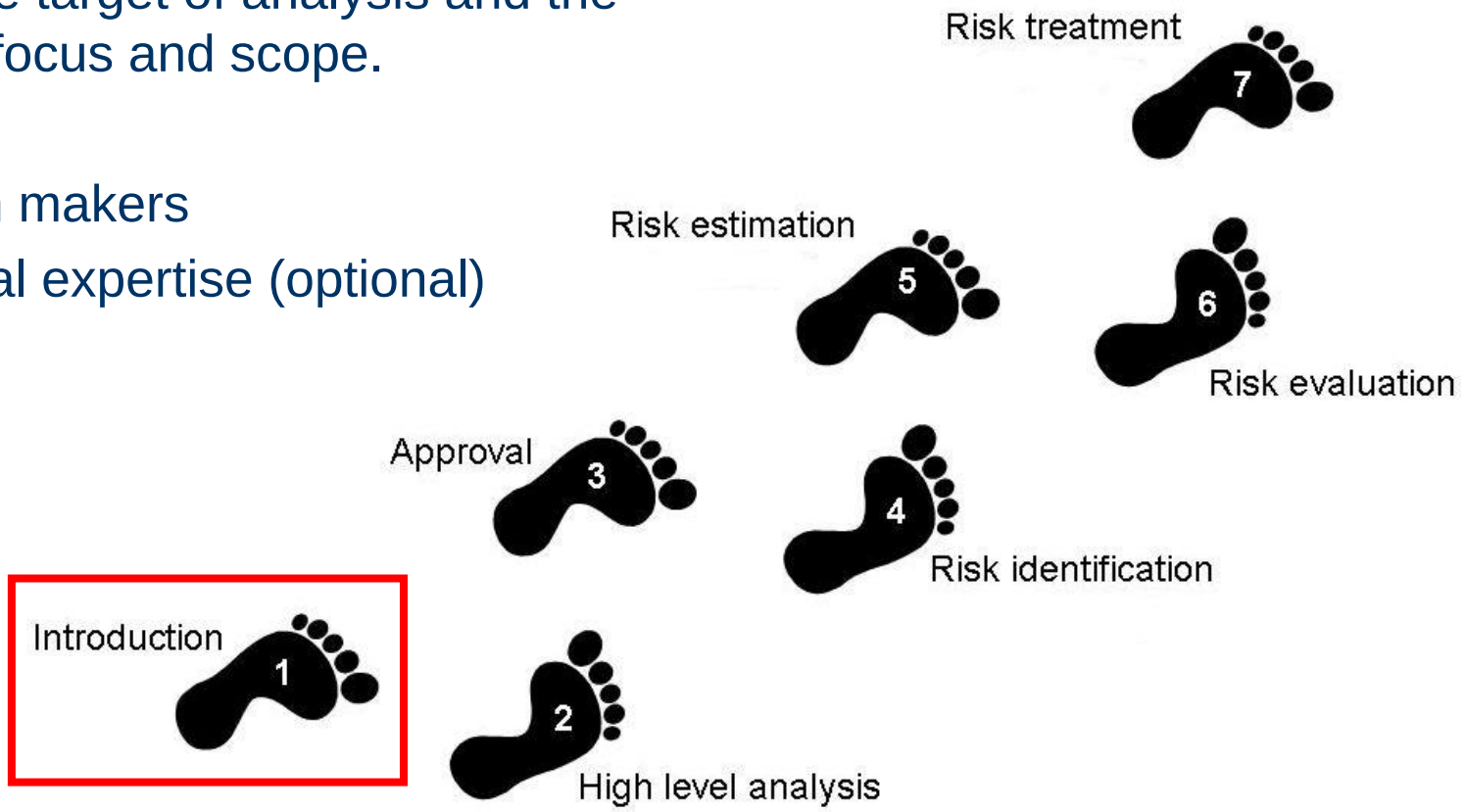
The CORAS method



Introductory meeting

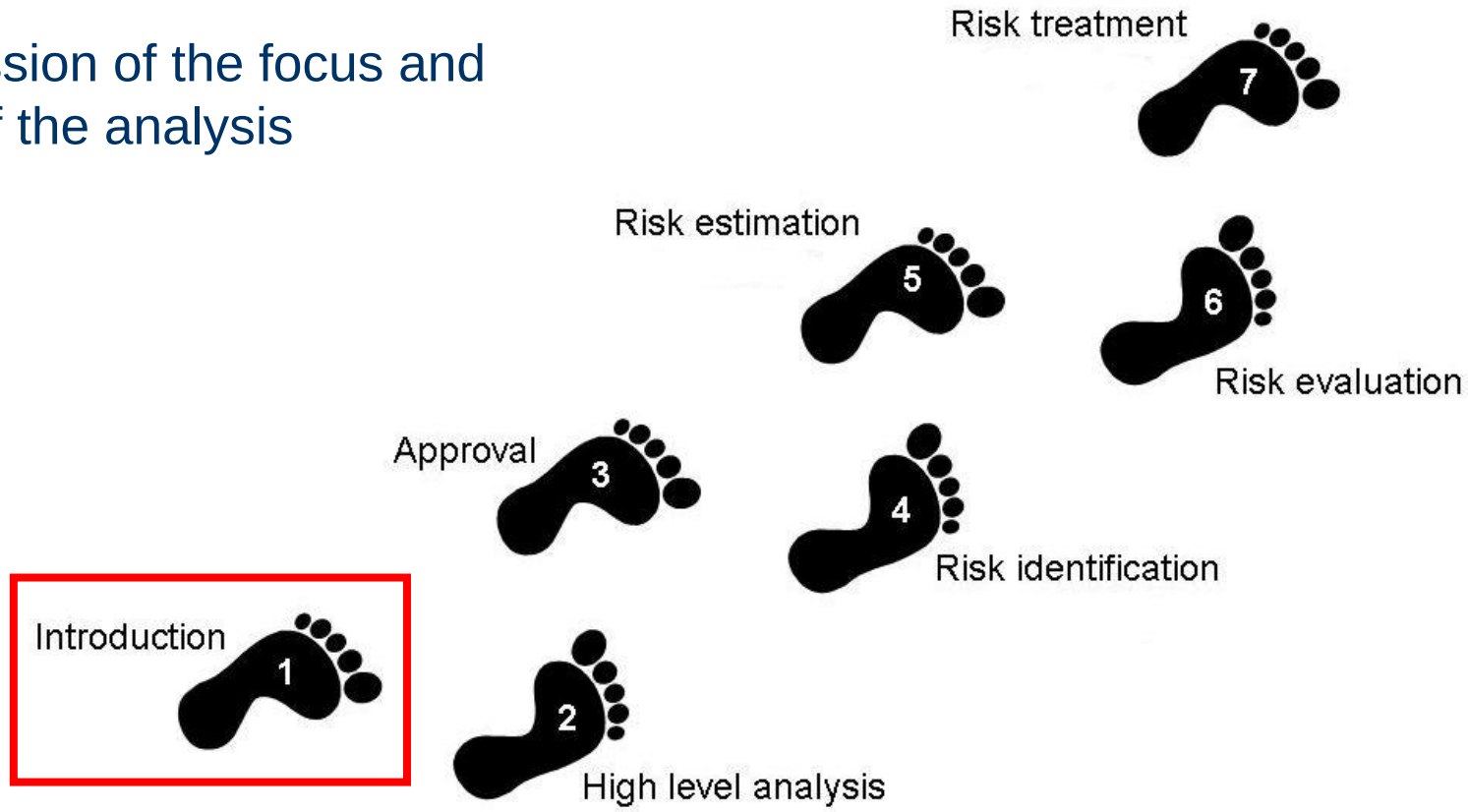
- Introduce the analysis method
- Gather information from the client about the target of analysis and the desired focus and scope.

- Decision makers
- Technical expertise (optional)



Introductory meeting – Agenda

- A short introduction to CORAS
- The client presents the target of analysis
- A discussion of the focus and scope of the analysis



Client's presentation of target

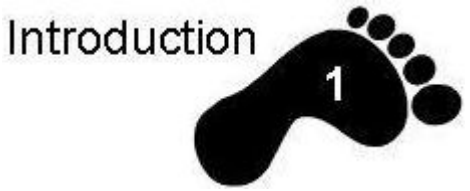
- Ann Onymous
- PhD student in Computer Science
- Uses data from Big Corporation (BC)
- Works in her office at the university and at home

At the university

- Shares an office with another PhD student
- Works on laptop in docking station
- Wired internet

At home

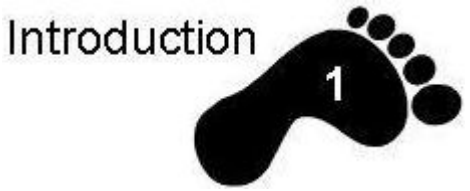
- Lives with her boyfriend
- Brings her laptop home with her or uses shared computer
- Wireless internet



Focus and scope

The focus of the analysis is data security, in terms of business sensitive data from BC and the PhD thesis itself.

The scope is data security at home and at work. We do not consider risks involved in transporting the data.



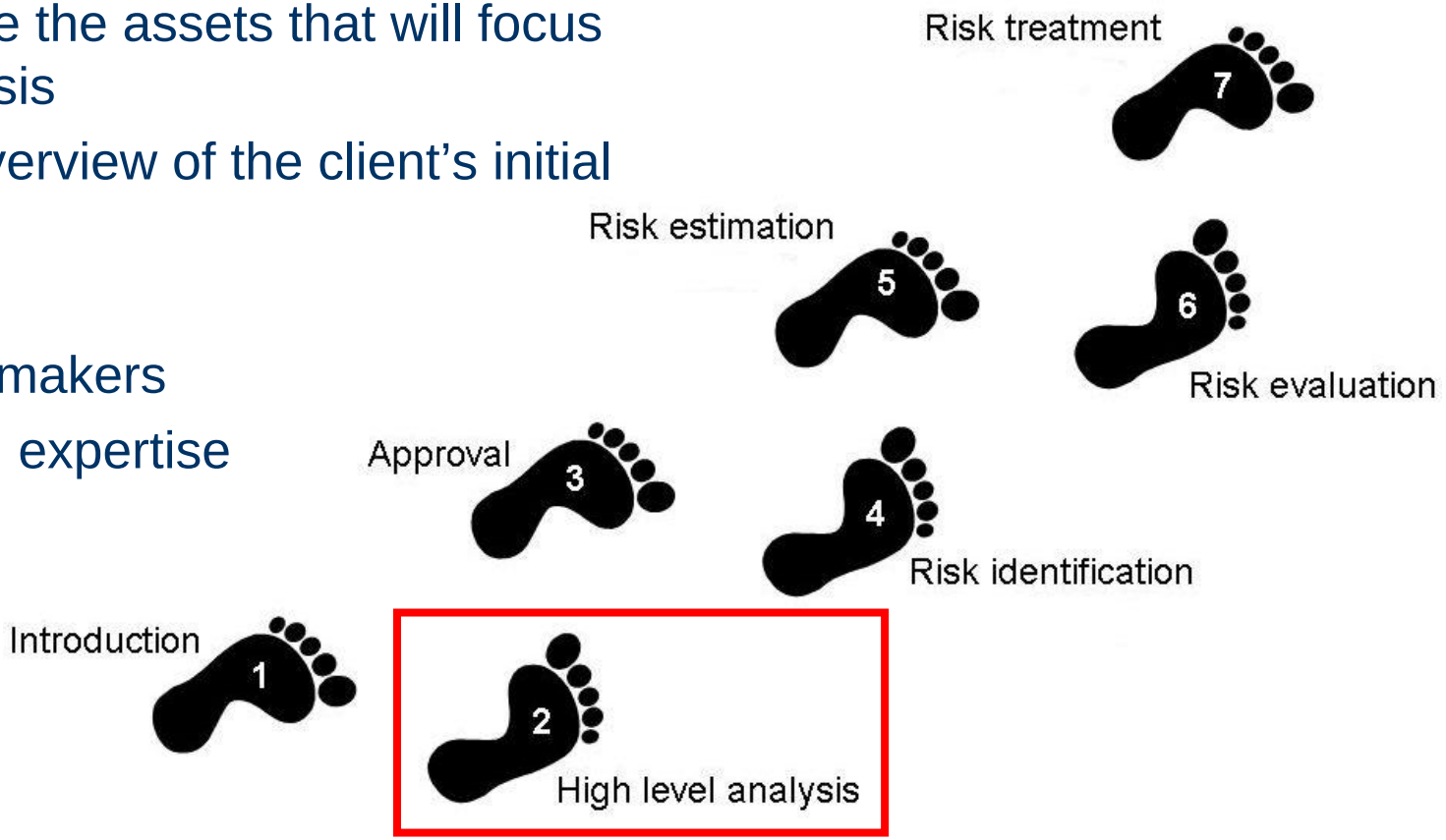
Output from the introductory meeting

- Informal description of the target
- Necessary system documentation
  - Contract between Ann and BC
  - IT security guidelines at the university
  - Security measures in place at home and at the university
  - A sketch of Ann’s work habits
- A short statement of the focus and scope of the analysis

High-level analysis

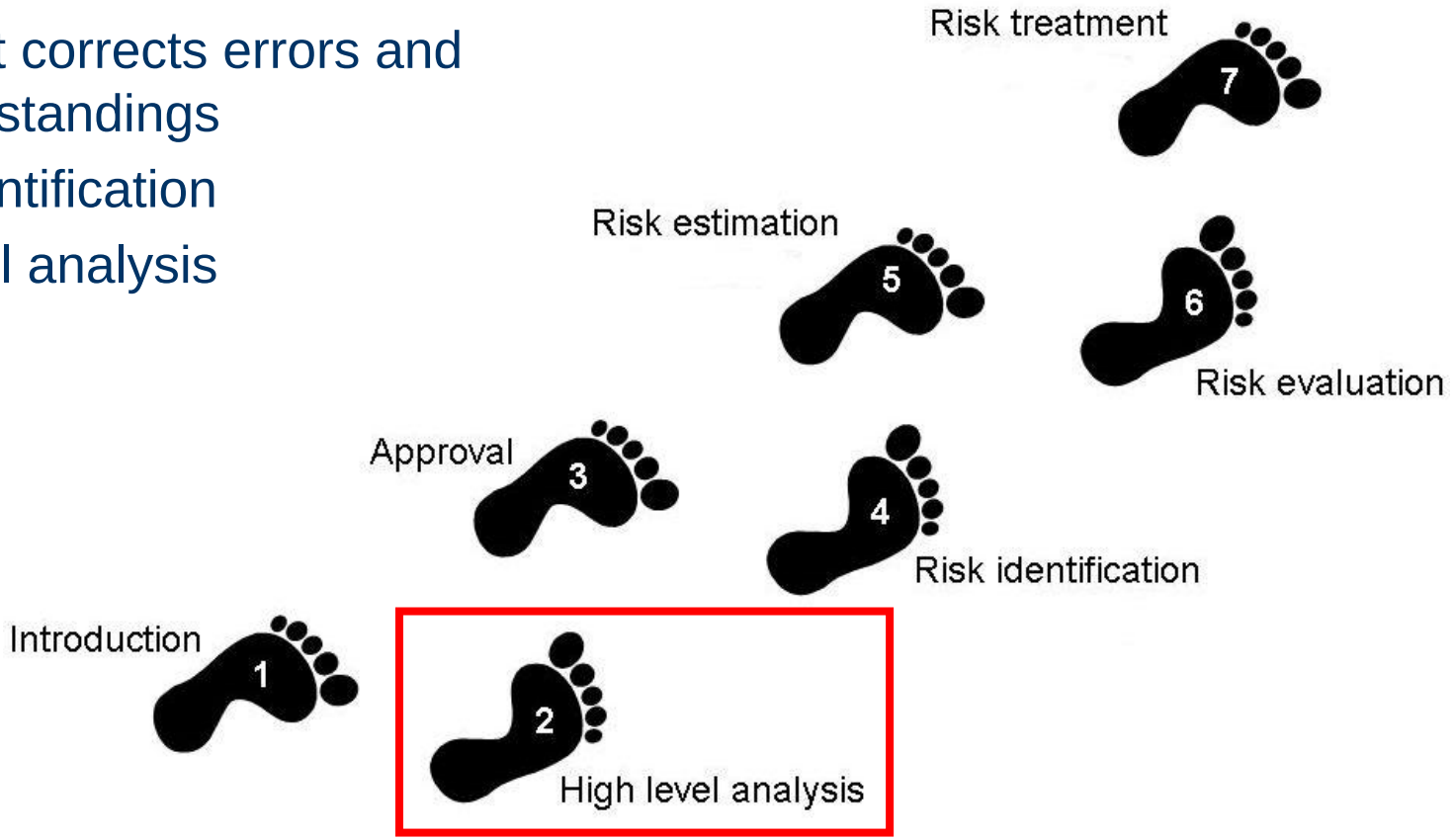
- Ensure that the analysts and the client have a common understanding of the target of analysis
- Determine the assets that will focus the analysis
- Get an overview of the client's initial concerns

- Decision makers
- Technical expertise



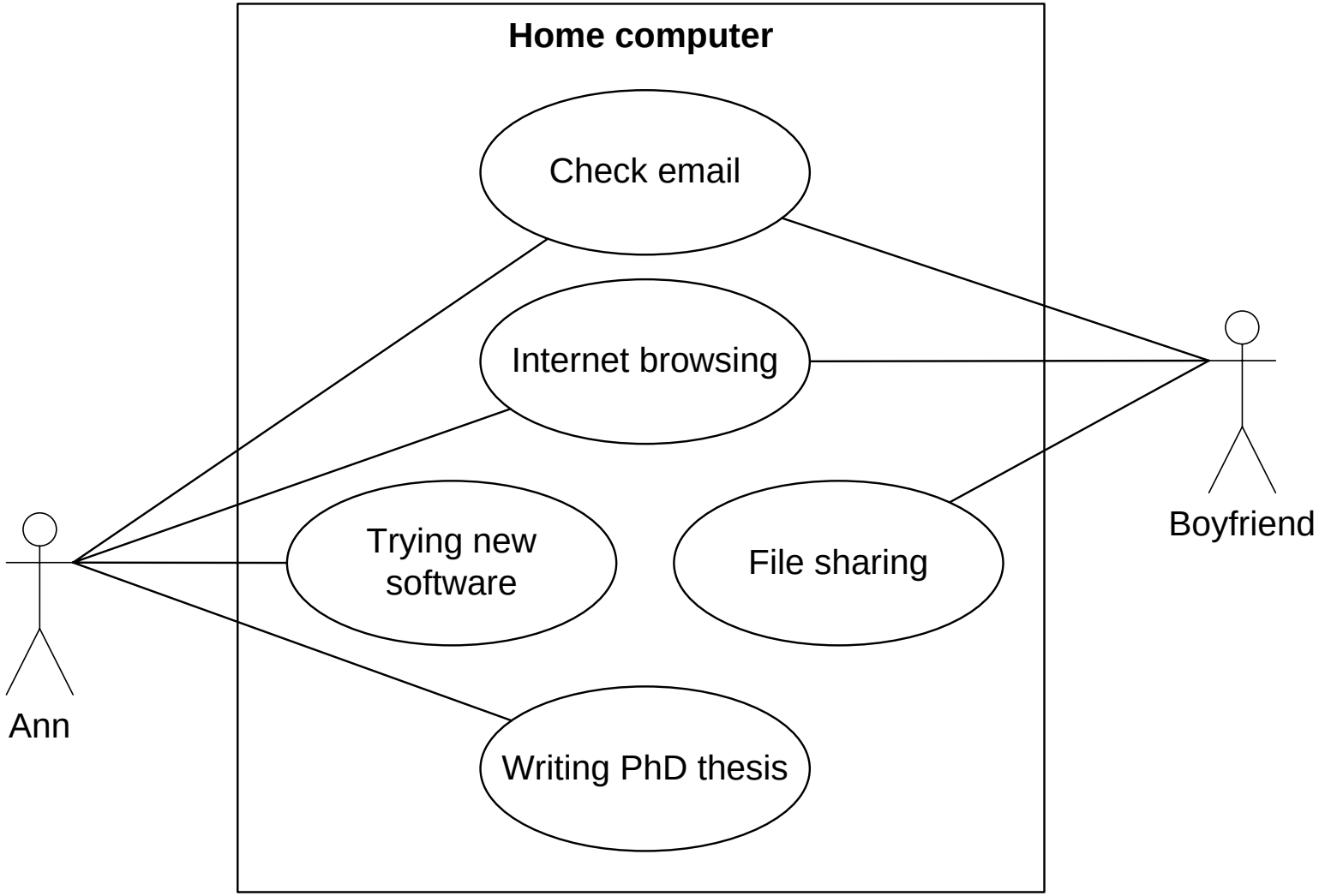
High-level analysis – Agenda

- The analysts presents a description of the target of analysis
- The client corrects errors and misunderstandings
- Asset identification
- High-level analysis



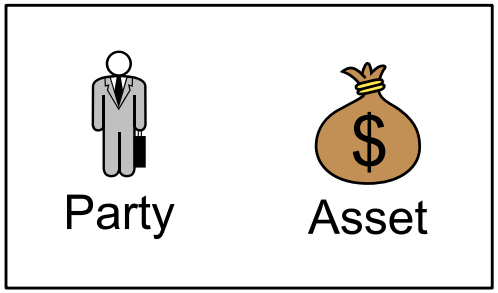
System description

High level analysis



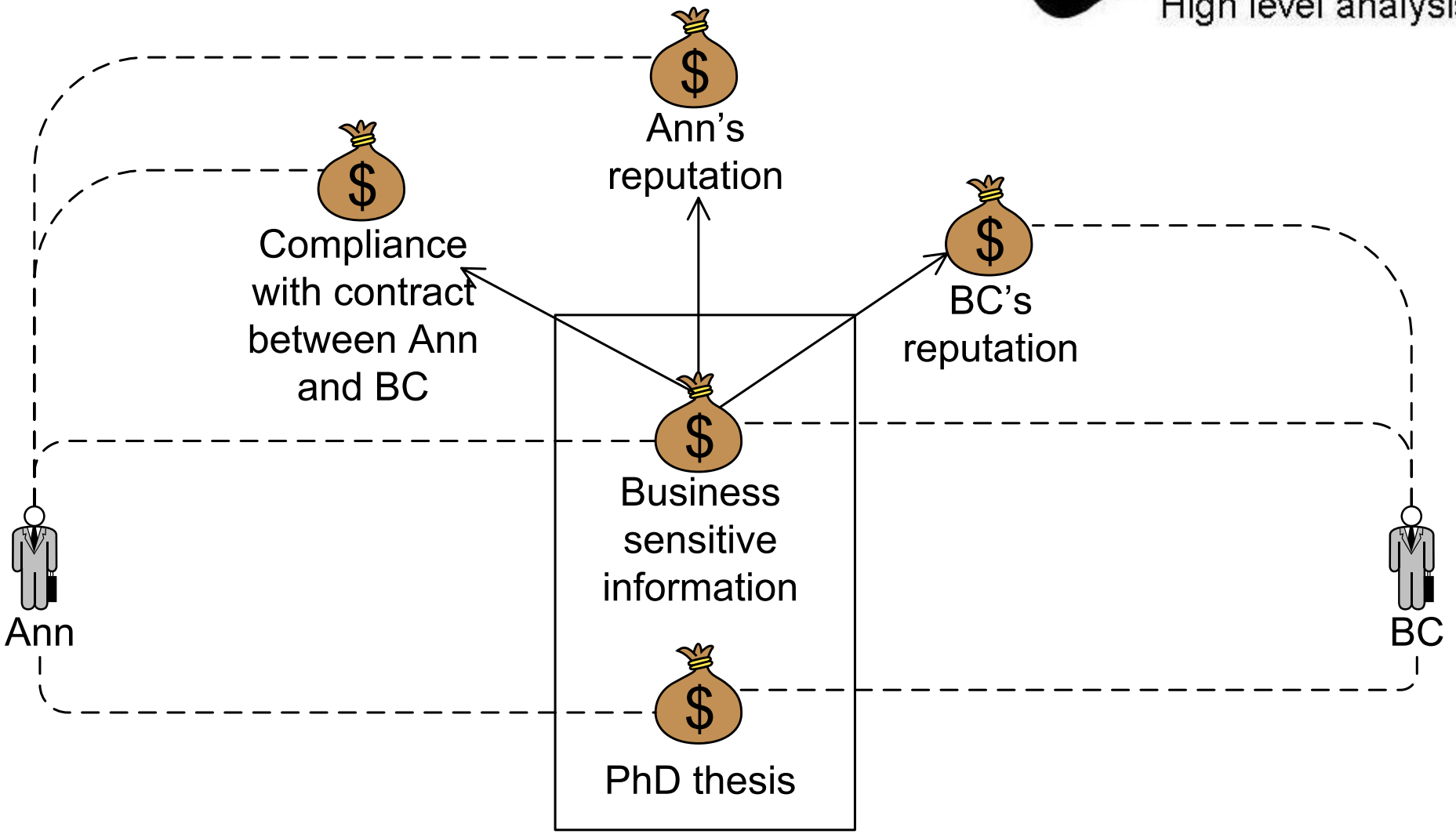
Asset identification

- We use an asset diagram to model the parties involved in the analysis, which assets they want to protect, and whether harm to one asset may cause harm to any of the others.

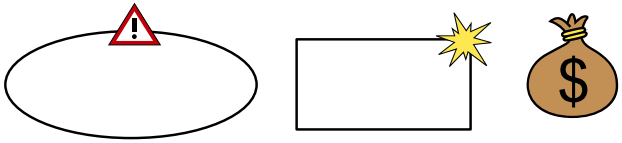


Asset diagram

High level analysis



High-level analysis

		
Who/what is the cause?	**How? What may happen? What does it harm?**	**What makes this possible?**
Ann	Deletes the thesis by mistake	No backup
Laptop	Crashes and the last hours' work is lost	Old laptop
Hacker	Gains access to business sensitive information and sells it to competitor	Lack of security at home

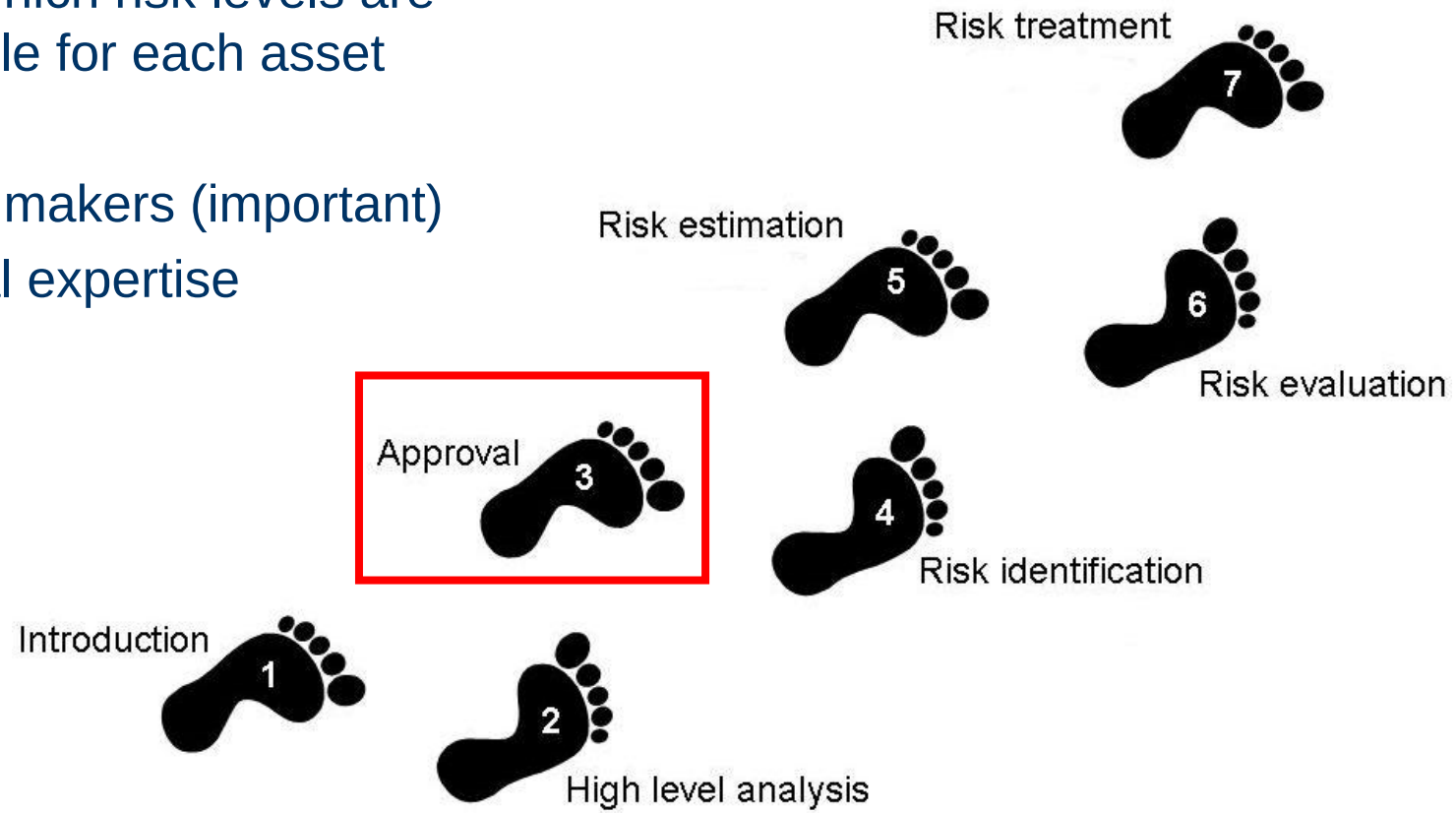
Output from the high-level analysis meeting

- Asset diagram
- Preliminary list of unwanted incidents

Approval

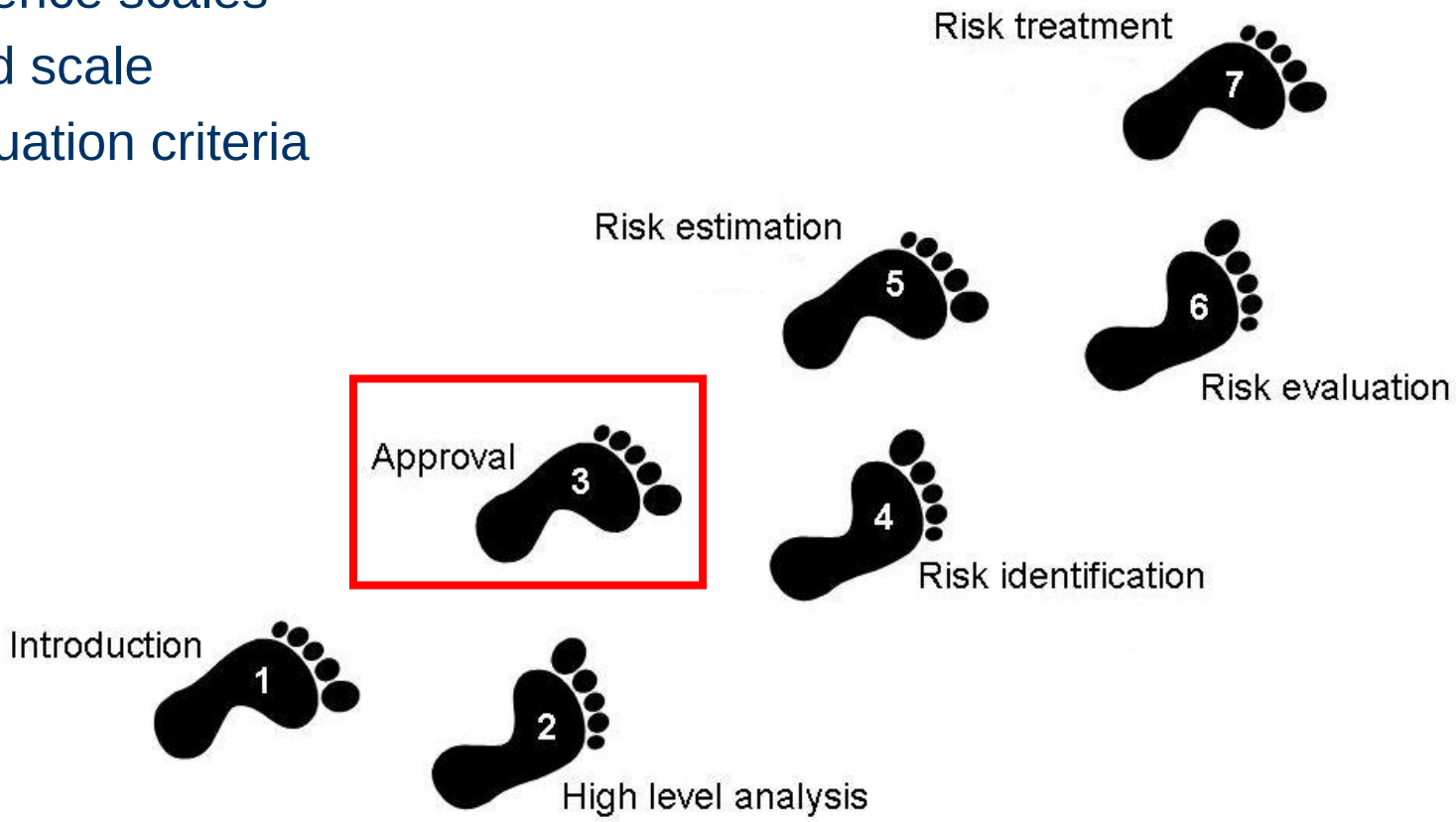
- Arrive at an approved target description
- Decide which risk levels are acceptable for each asset

- Decision makers (important)
- Technical expertise



Approval – Agenda

- The target description and assets are approved by the client
- Consequence scales
- Likelihood scale
- Risk evaluation criteria



Likelihood scale

Likelihood	
1	rarely
2	sometimes
3	regularly
4	often

Consequence scale

Consequence (PhD thesis and Business sensitive information)	
1	harmless
2	moderate
3	serious
4	catastrophic

Risk matrix

Risk matrix

(PhD thesis and Business sensitive information**)**

c \ l	rarely	sometimes	regularly	often
harmless				
moderate				
serious				
catastrophic				

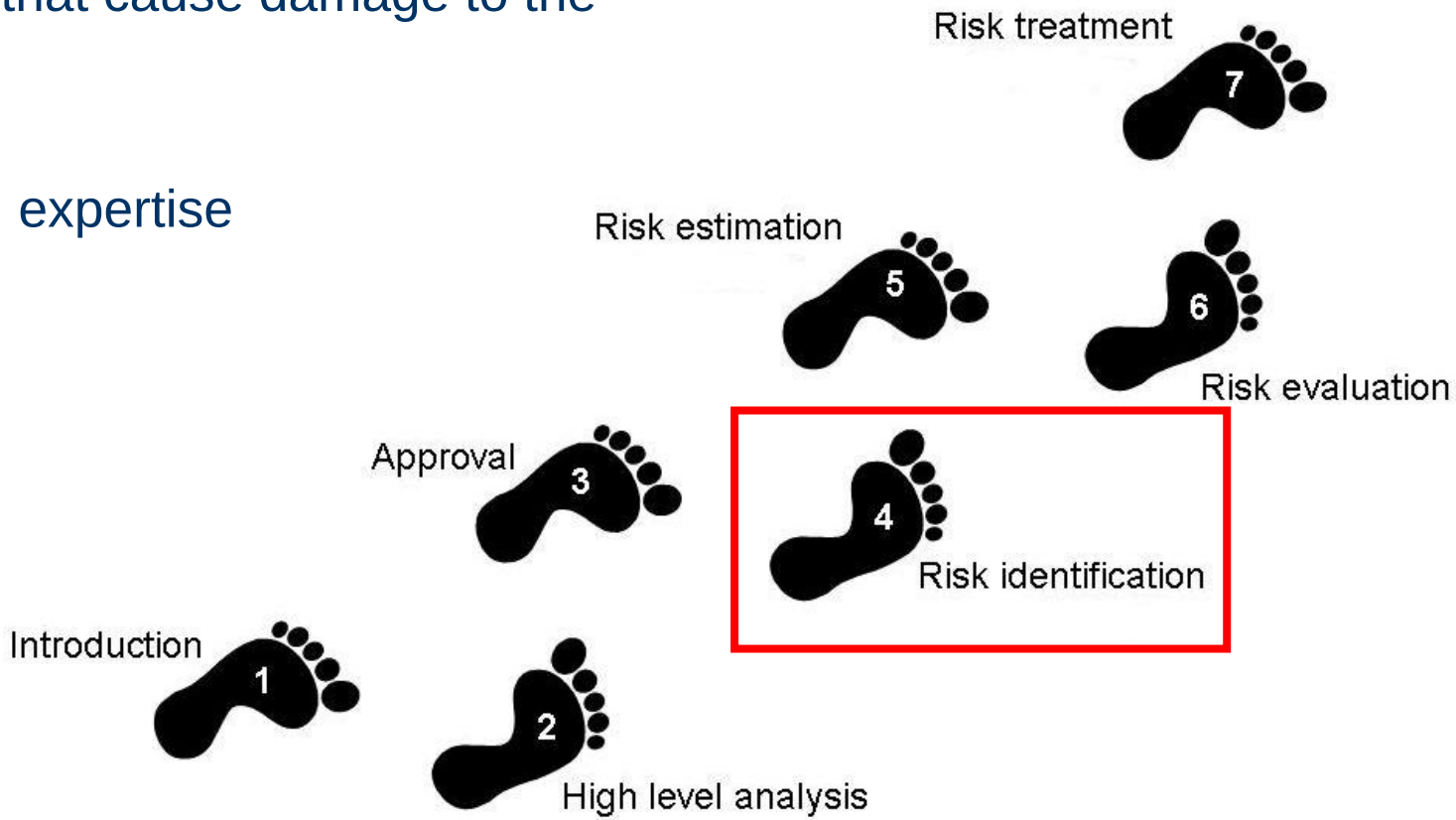
Output from the approval meeting

- Approved target description
- Likelihood and consequence scales
- Risk matrices

Risk identification

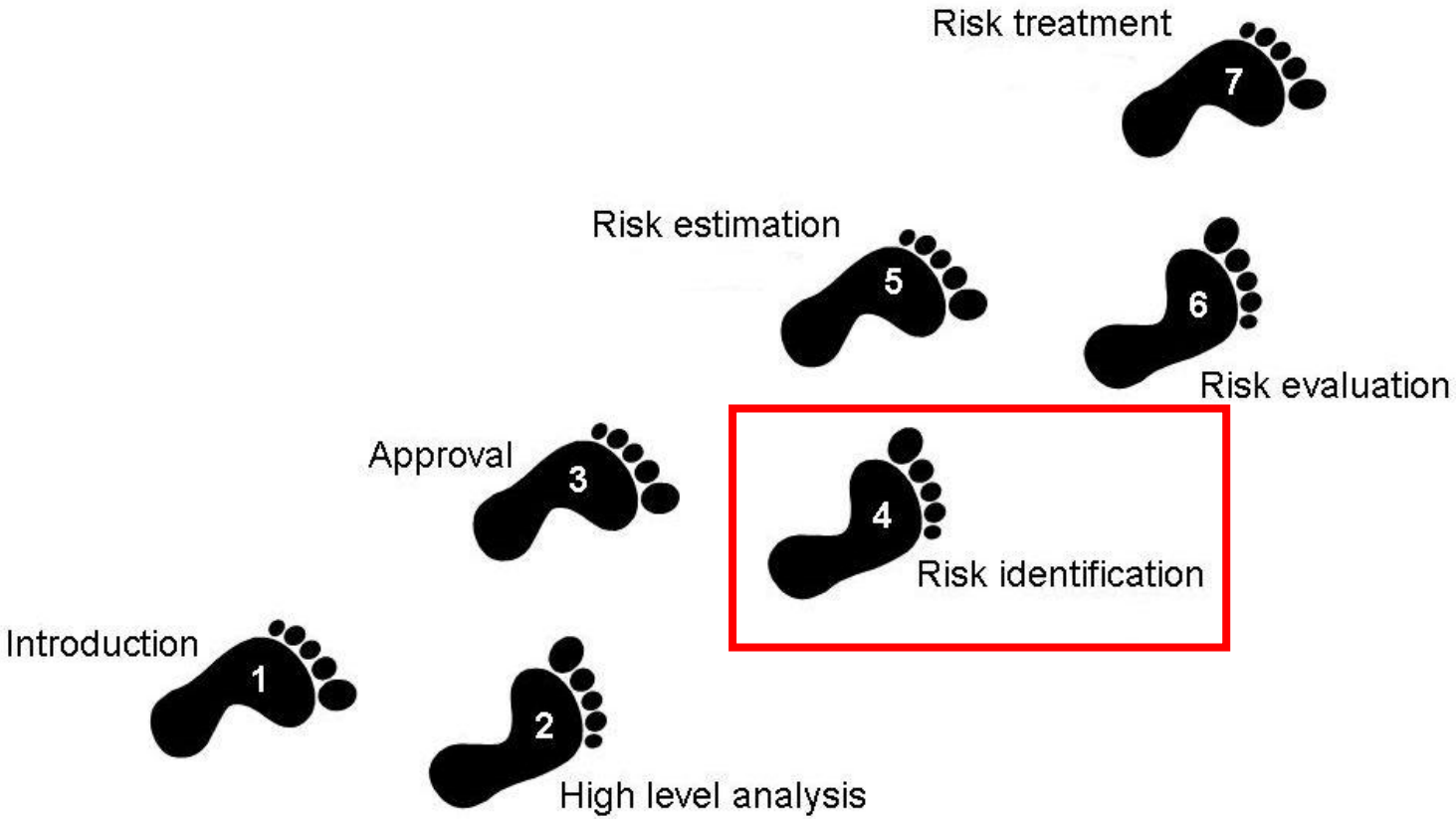
- Create an overview of the risk picture, i.e. how threats may exploit vulnerabilities to cause unwanted incidents that cause damage to the assets.

- Technical expertise
- Users



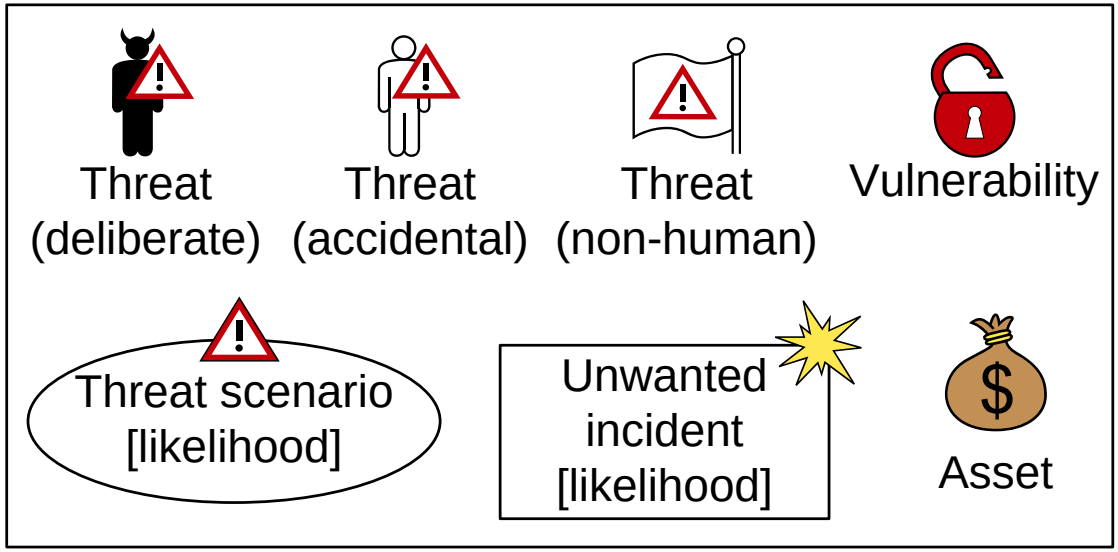
Risk identification – Agenda

→ Model risks in threat diagrams



Modelling risks in threat diagrams

- We use threat diagrams to model threats, what we fear they may do to our assets, how it happens and which vulnerabilities makes this possible.



What are the threats?


Hacker


Ann


Home computer


Business sensitive information

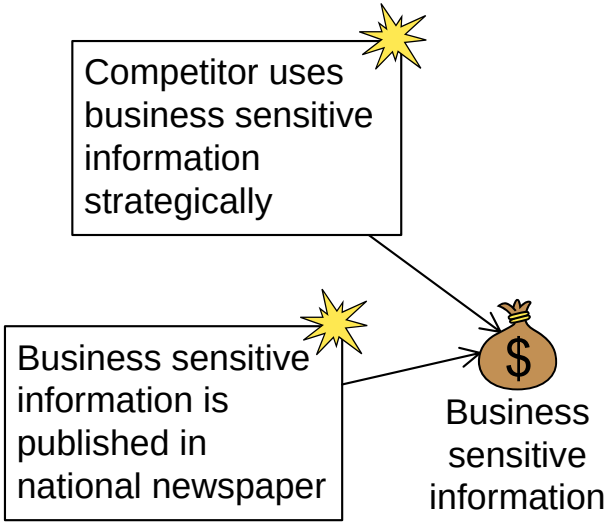

PhD thesis

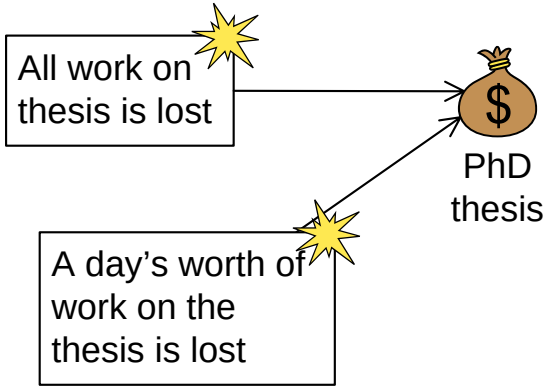
What do we fear will happen?


Hacker

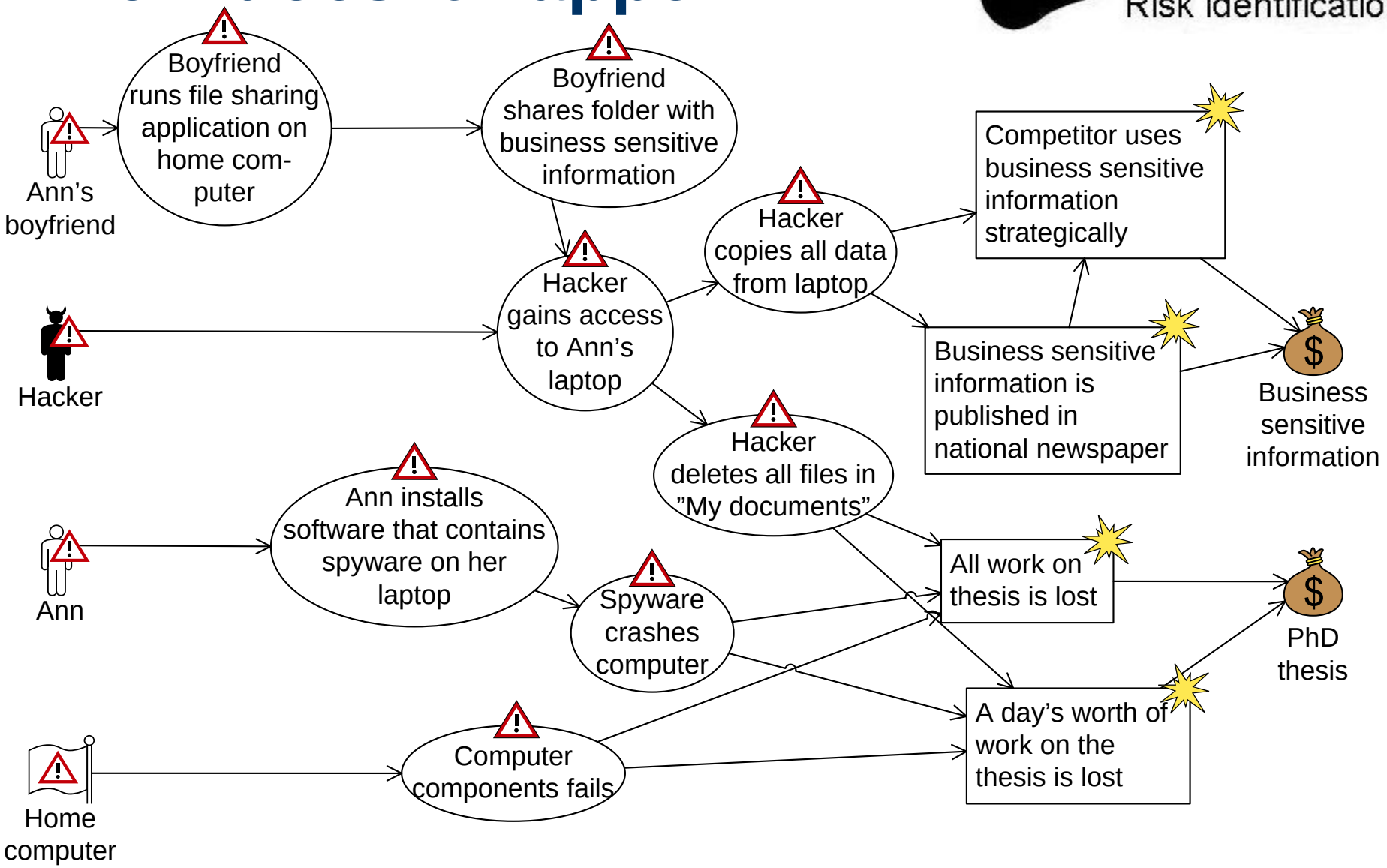

Ann


Home computer

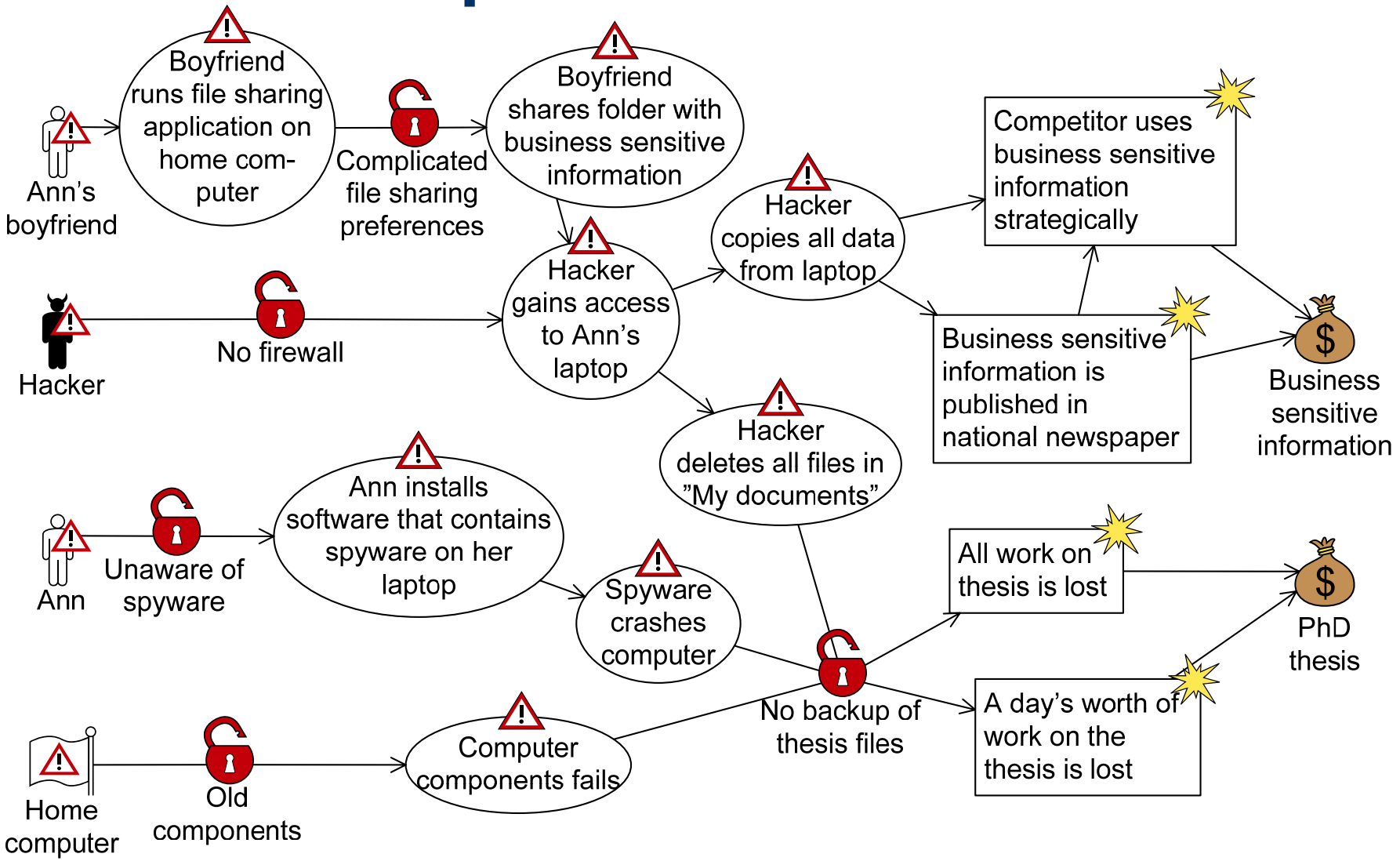




How does it happen?



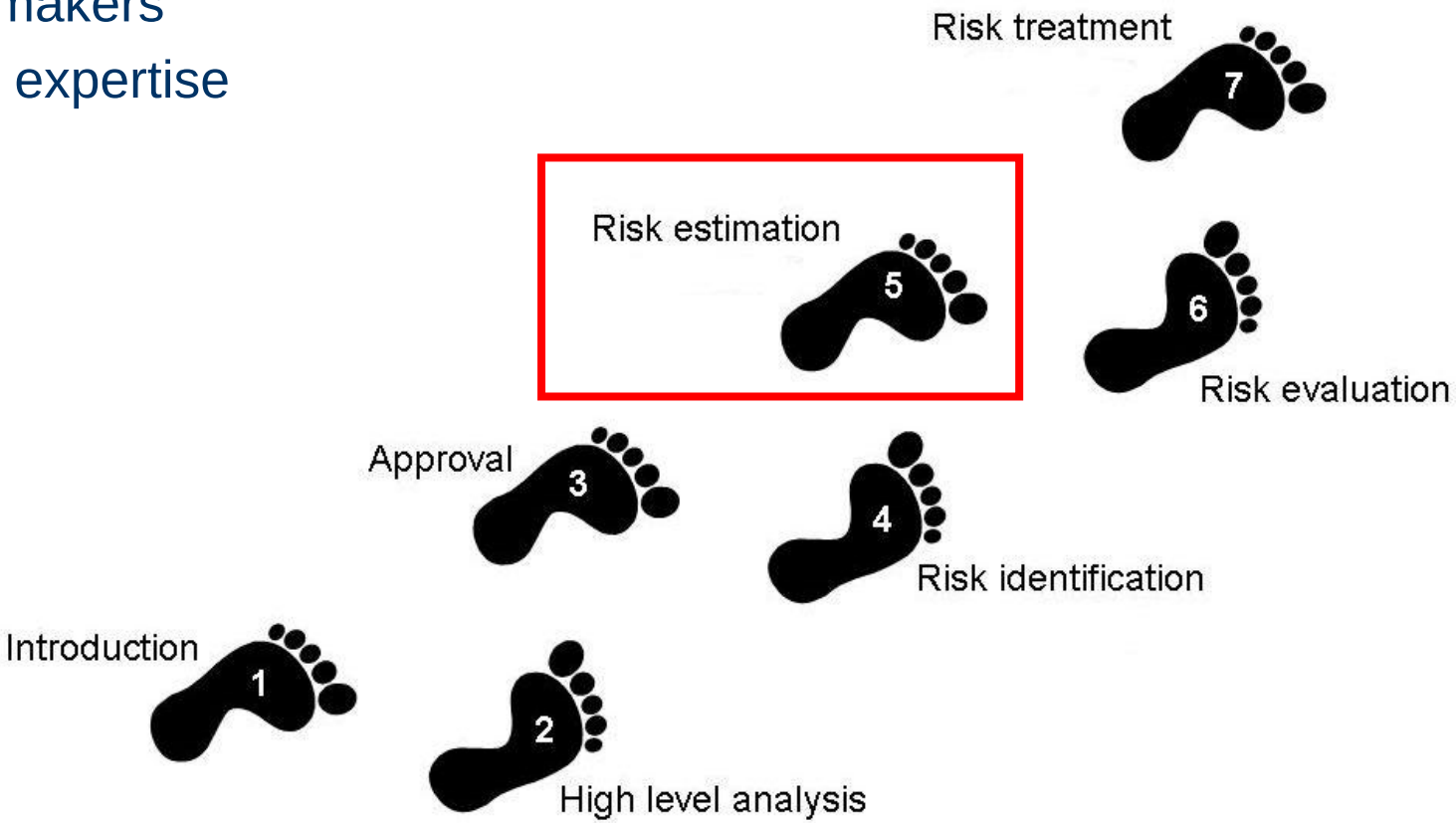
Which vulnerabilities makes this possible?



Risk estimation

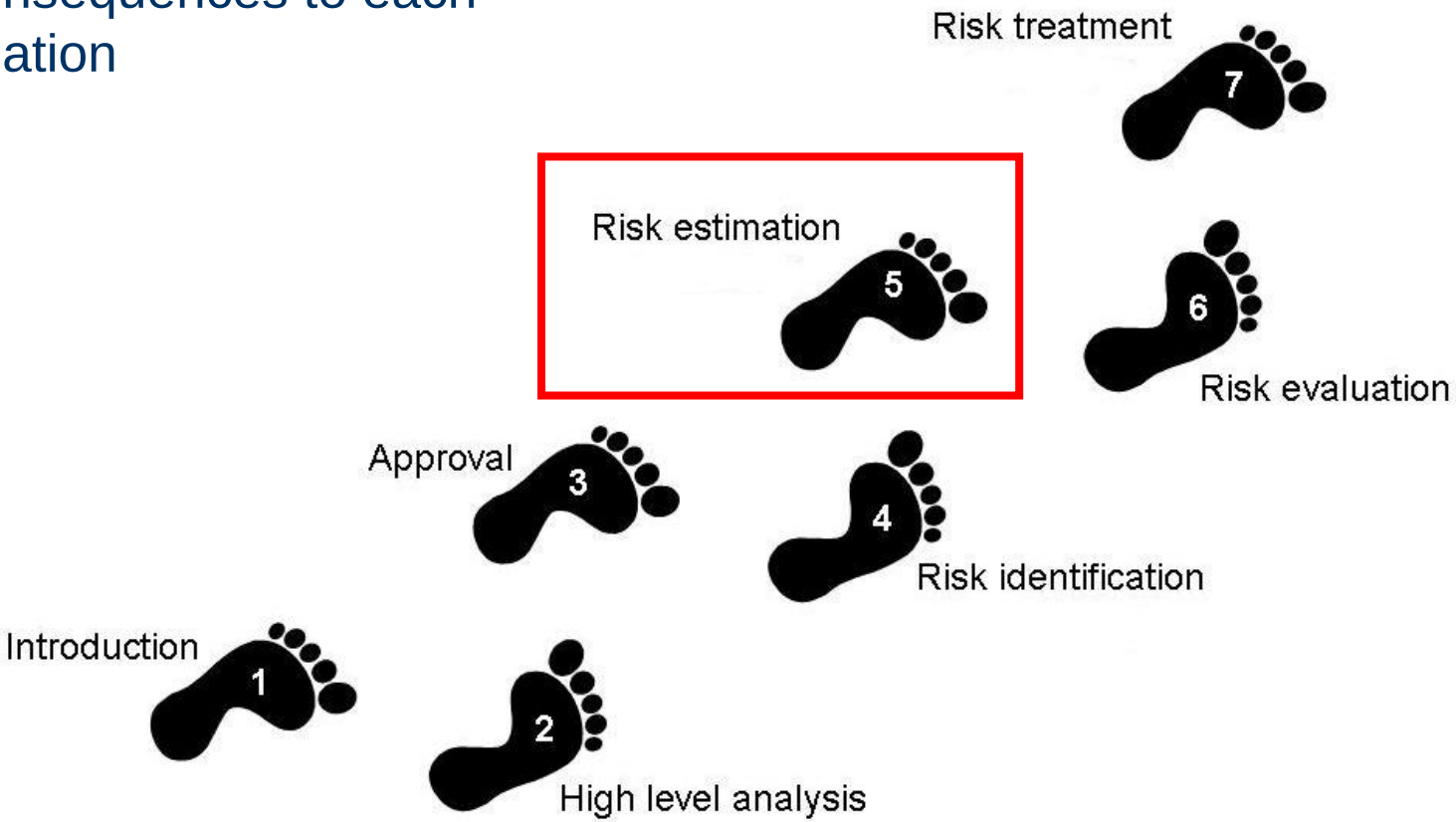
- Estimate the current risk level

- Decision makers
- Technical expertise
- Users

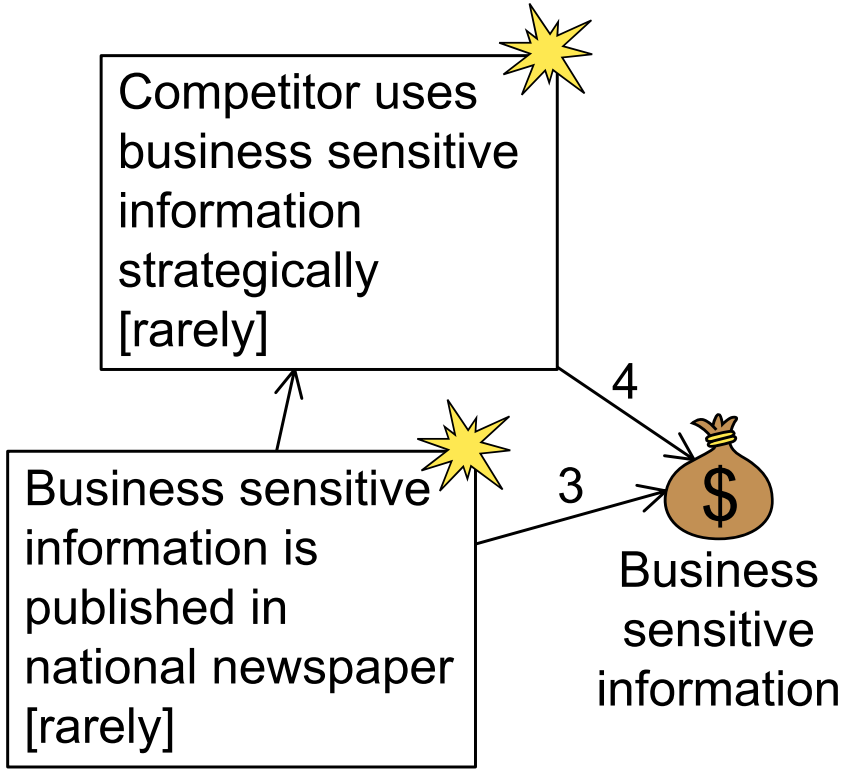


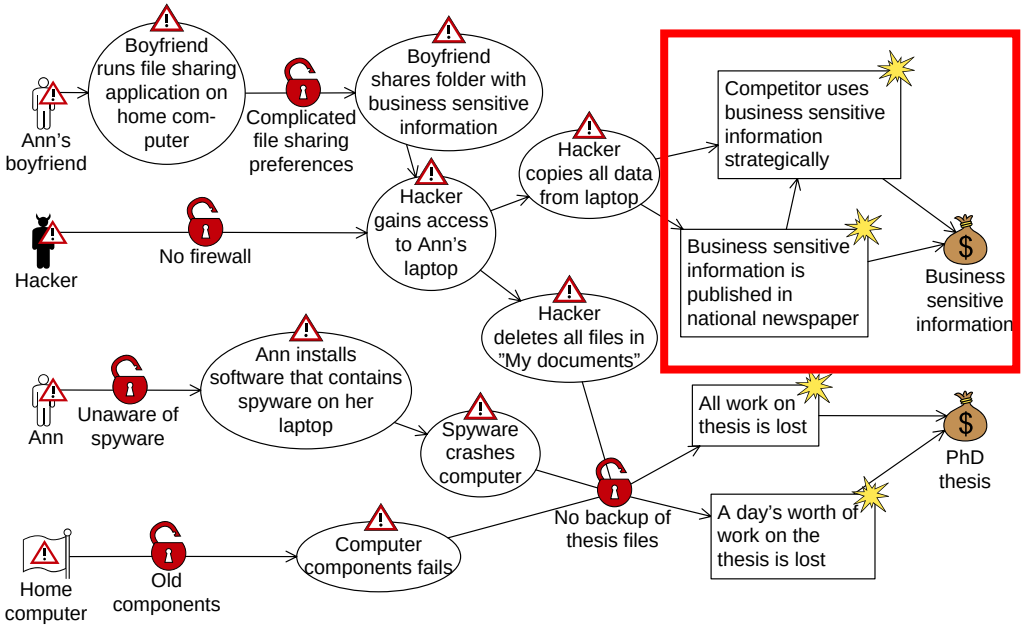
Risk estimation – Agenda

- Assign likelihoods to each unwanted incident
- Assign consequences to each impact relation

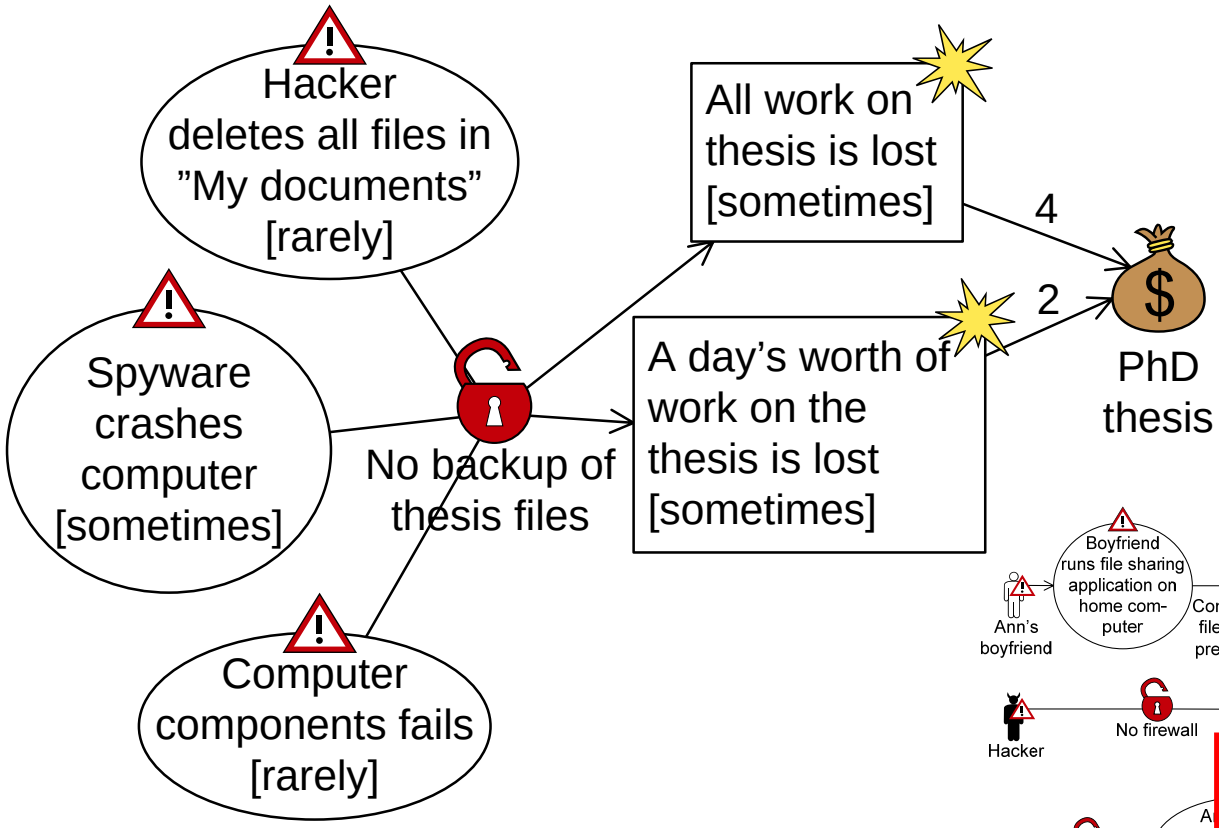


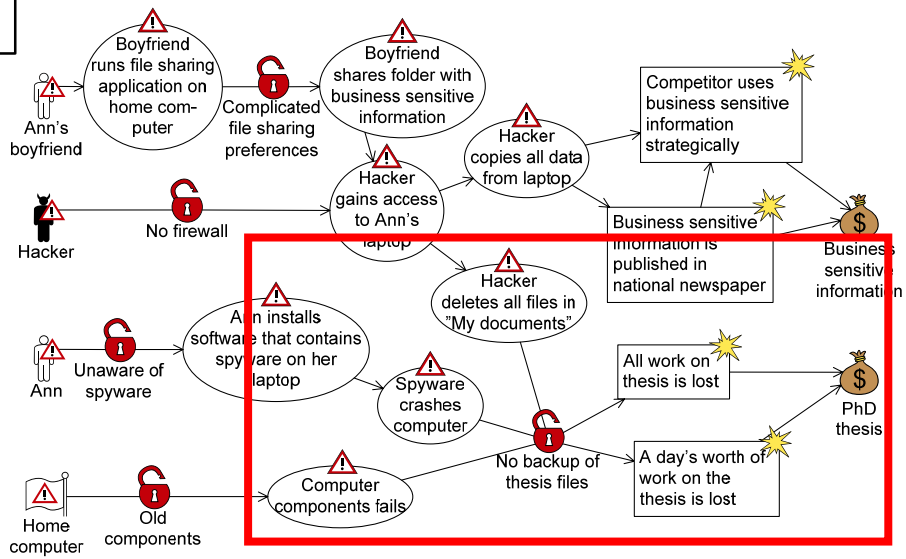
Assigning likelihoods and consequences



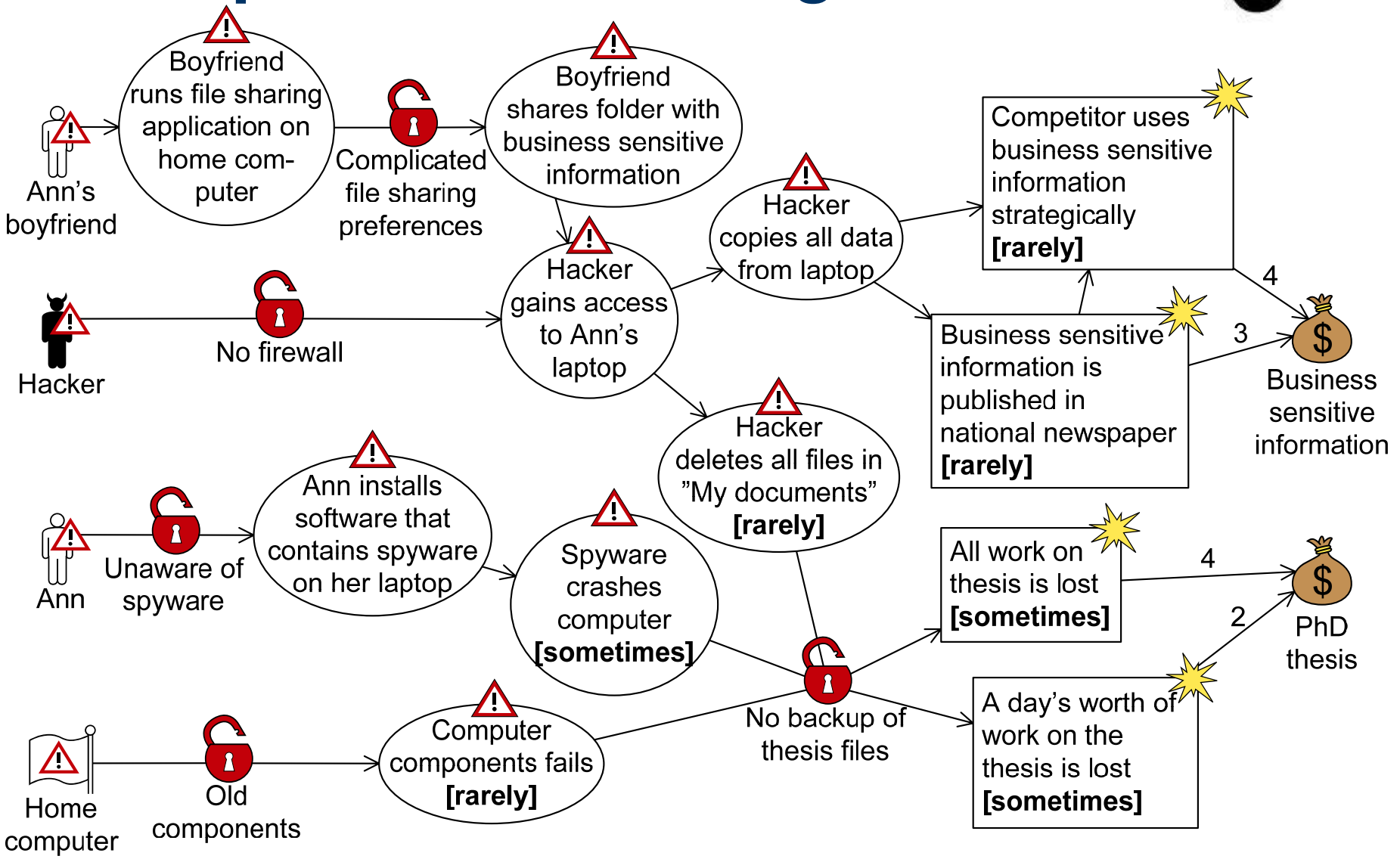


Assigning likelihoods and consequences





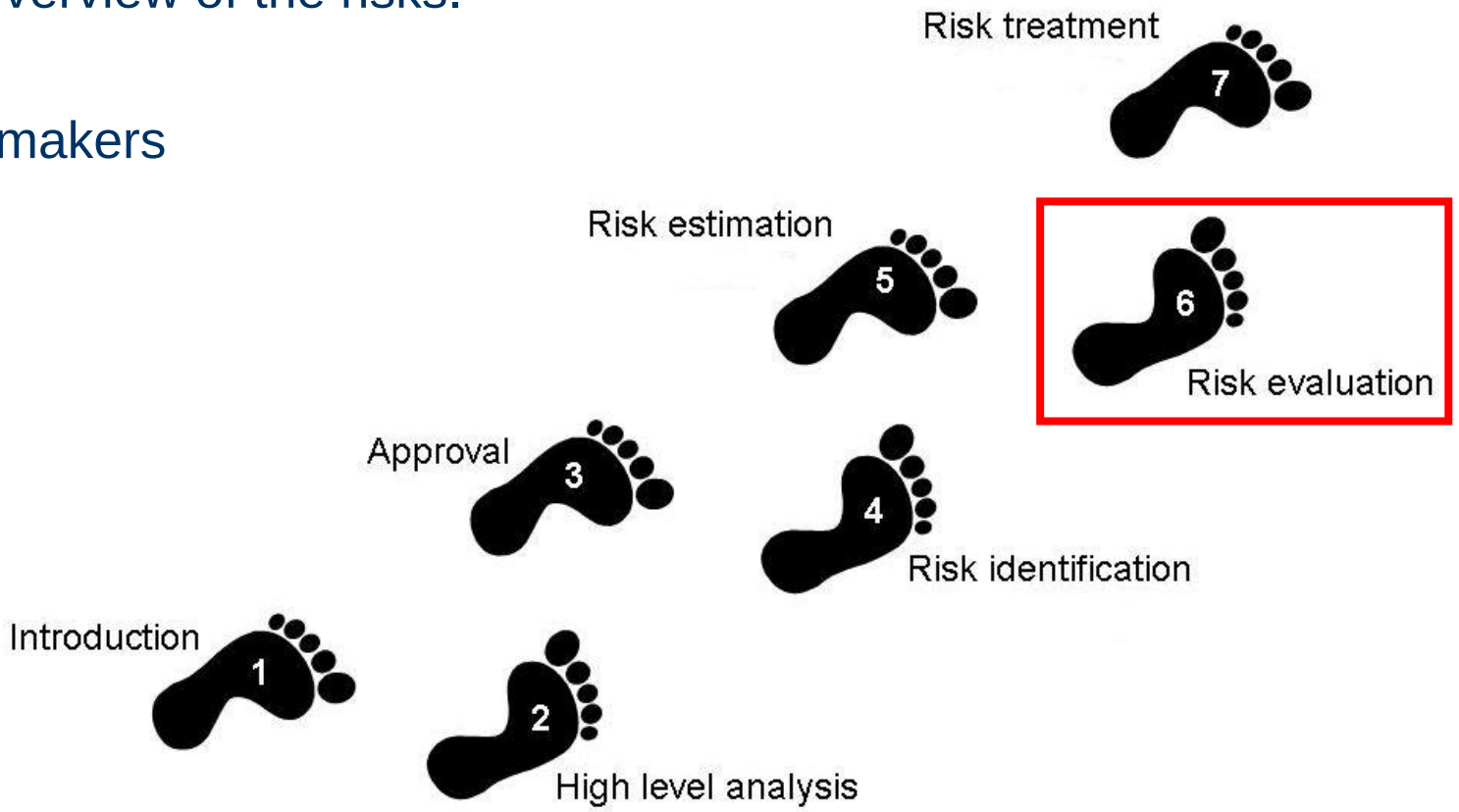
Completed threat diagram



Risk evaluation

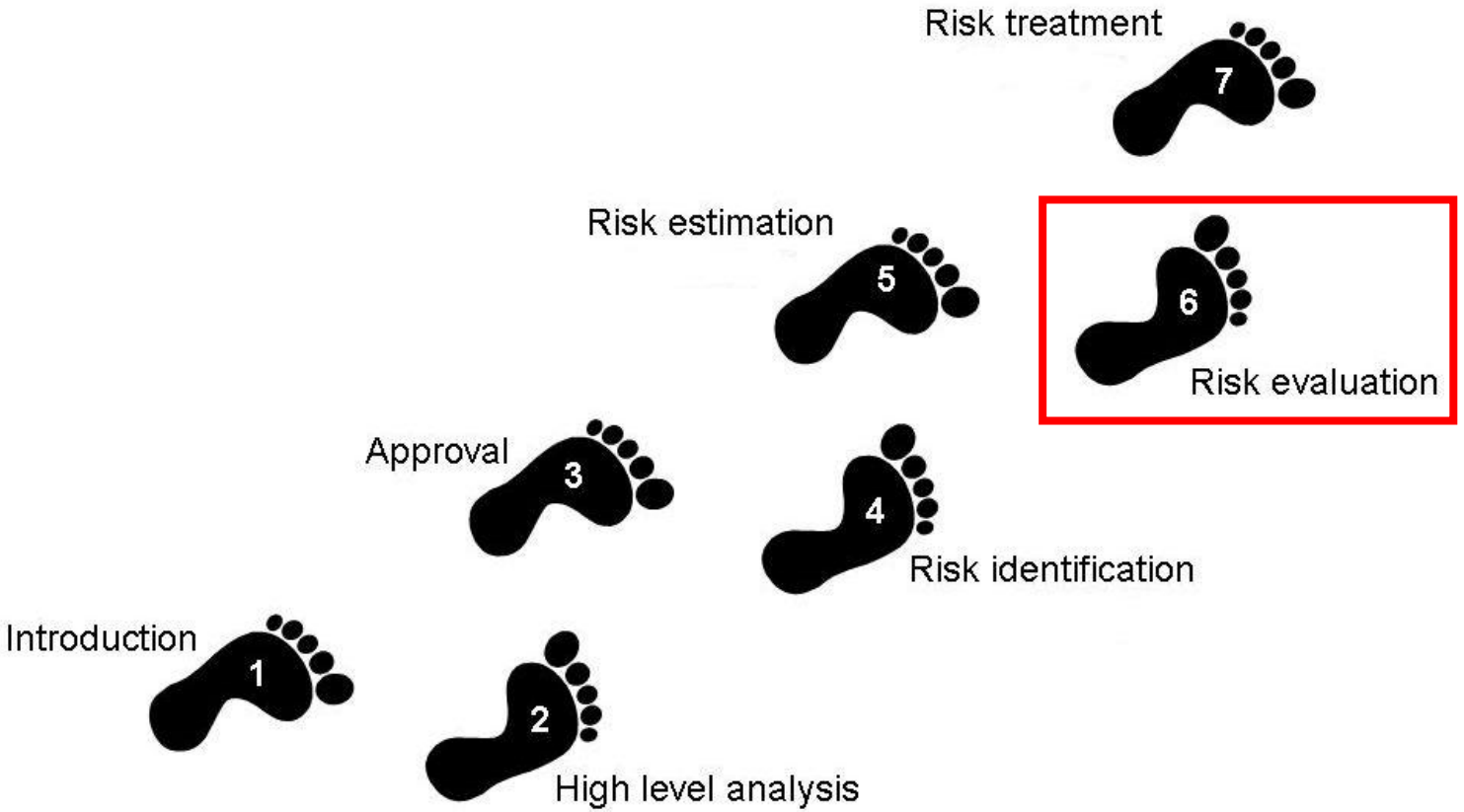
- Evaluating which risks are acceptable and which are not.
- Give an overview of the risks.

- Decision makers



Risk evaluation – Agenda

- Enter the risks in the risk matrix
- Summarize the risk picture in risk diagrams



Are the risks acceptable?

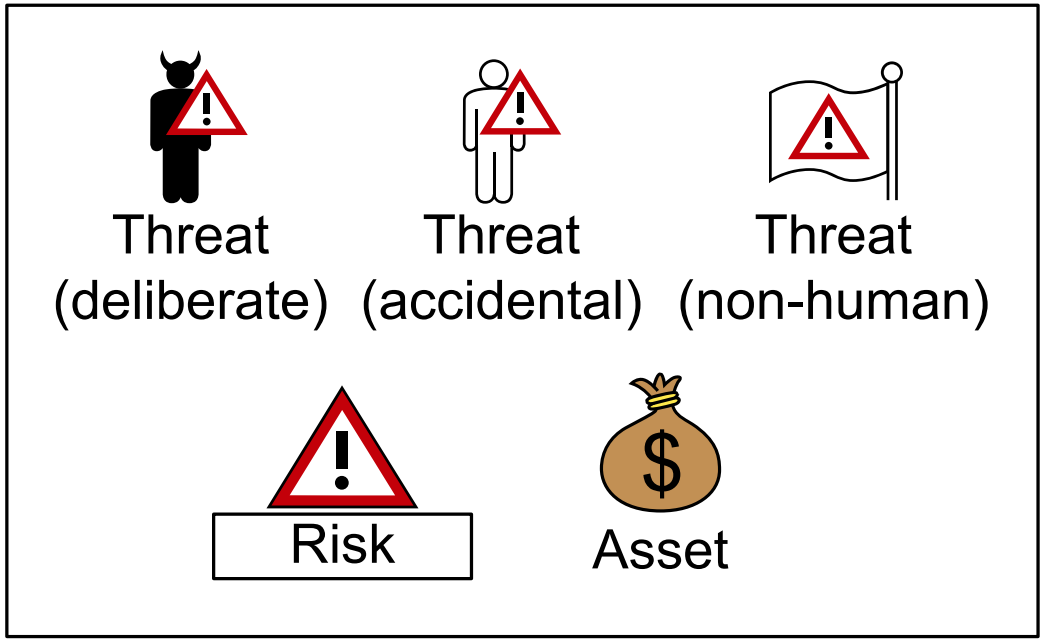
Risk evaluation

Risk matrix (PhD thesis and Business sensitive information**)**

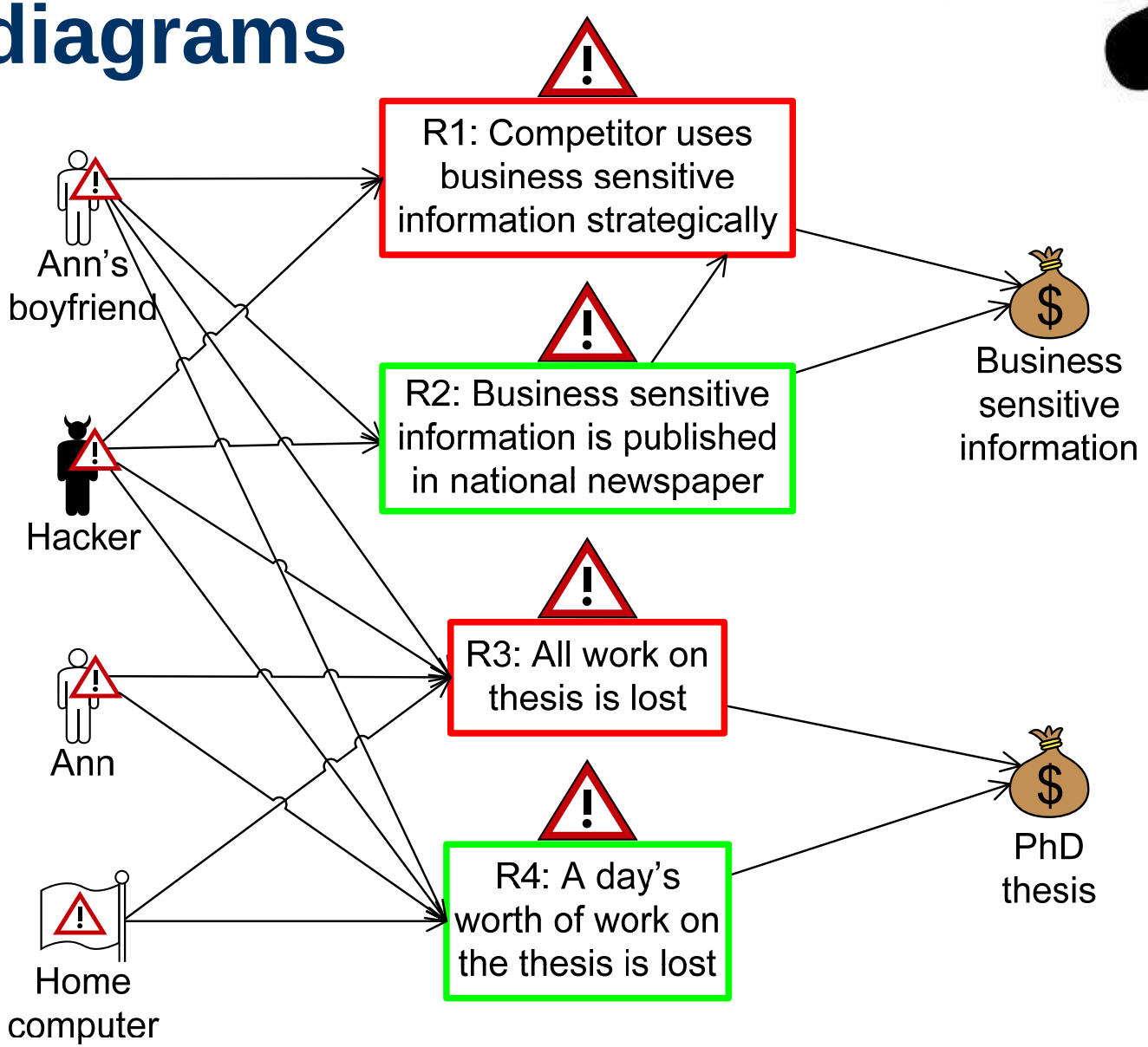
c \ l	rarely	sometimes	regularly	often
harmless				
moderate		A day's worth of work on the thesis is lost		
serious	BS info is published in national newspaper			
catastrophic	Competitor uses BS info strategically	All work on thesis is lost		

Summarizing the risk picture

- We use risk diagrams to show how threats pose risks to the assets.



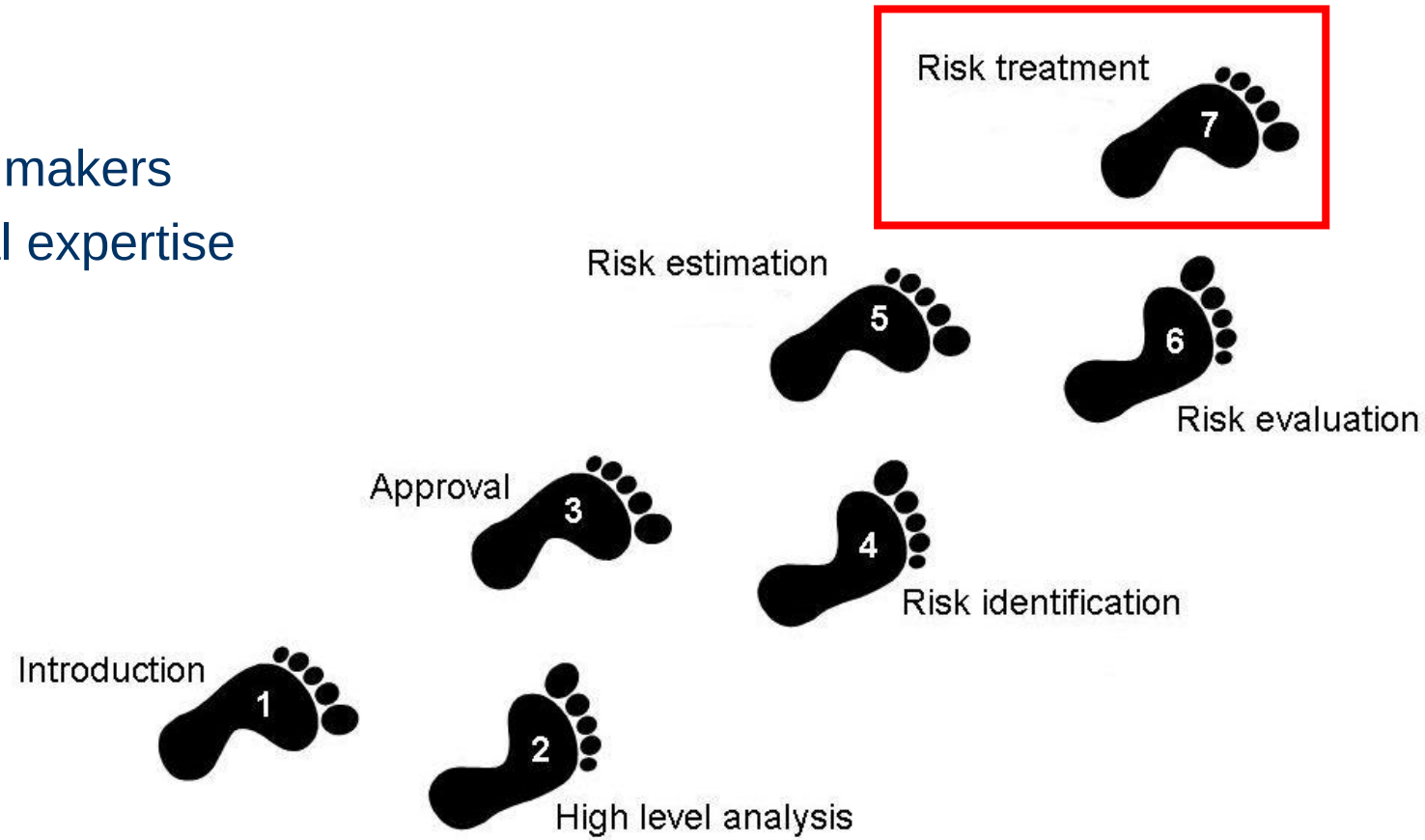
Risk diagrams



Risk treatment

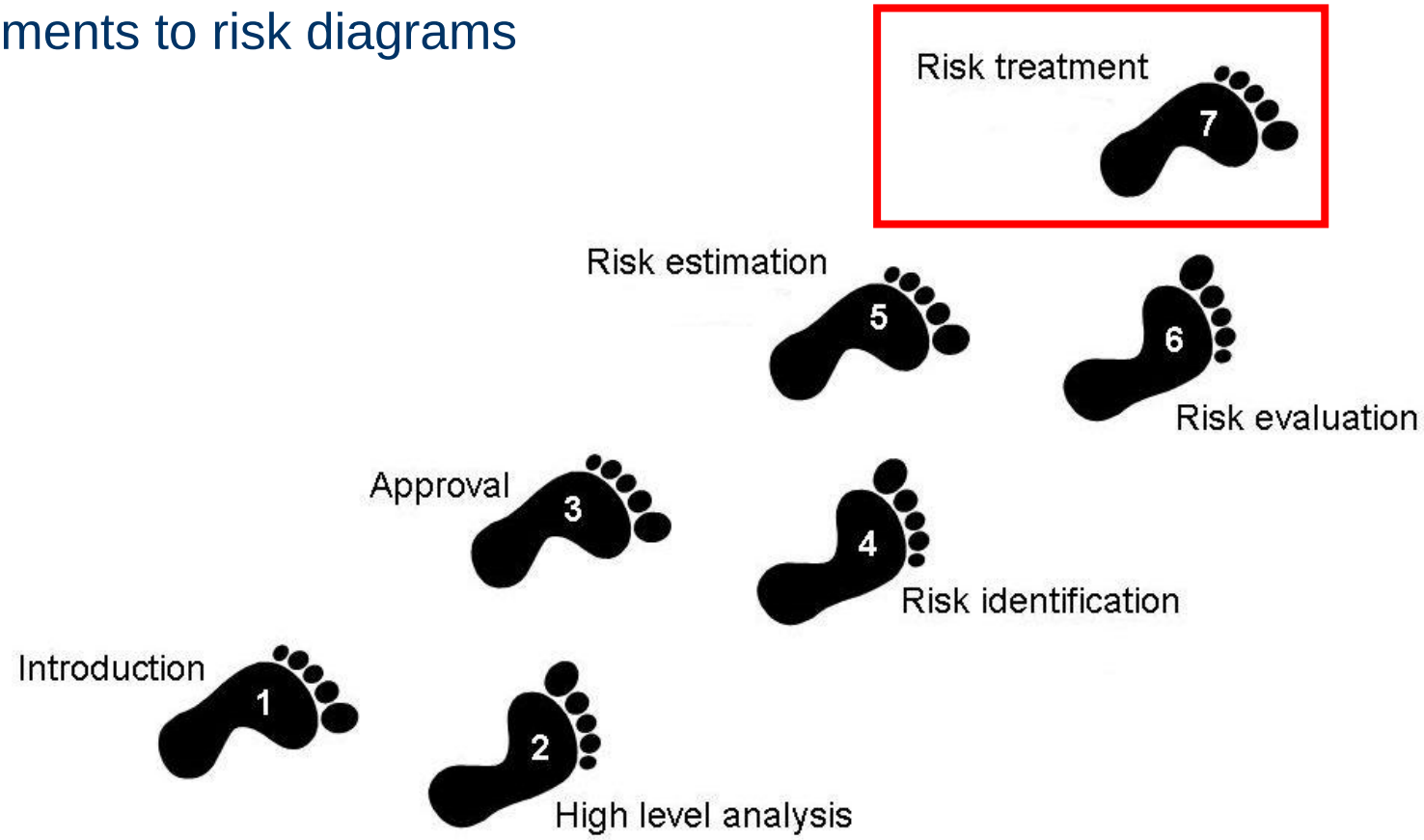
- Getting an overview of potential treatments of the unacceptable risks.

- Decision makers
- Technical expertise
- Users

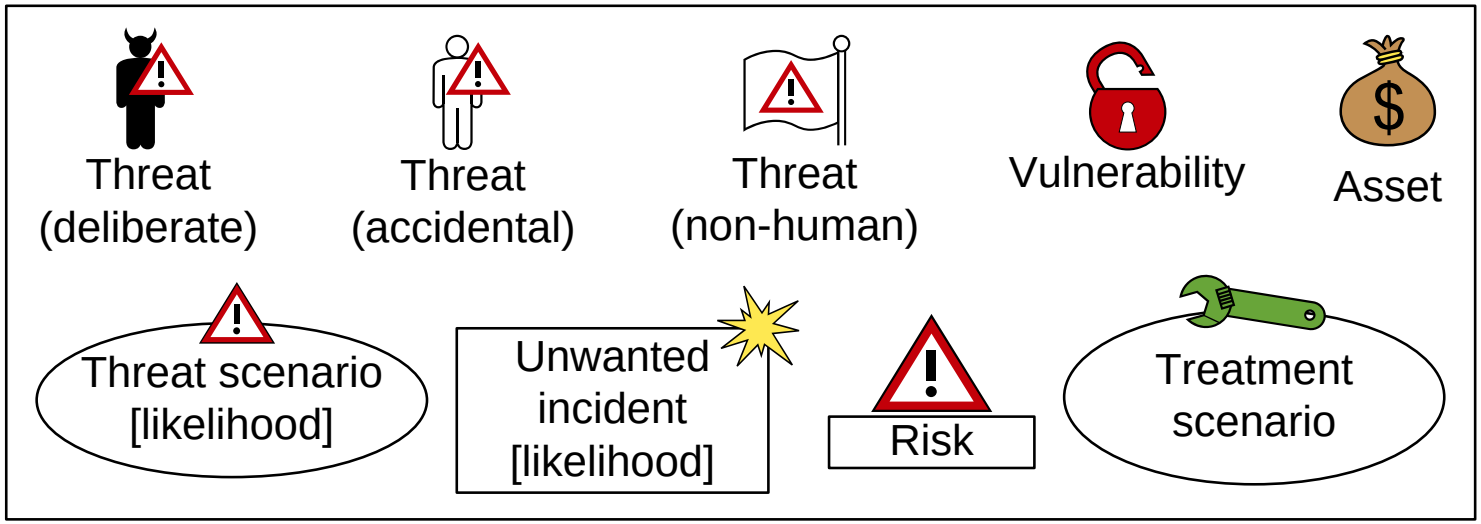


Risk treatment – Agenda

- Add treatments to the threat diagrams
- Add treatments to risk diagrams

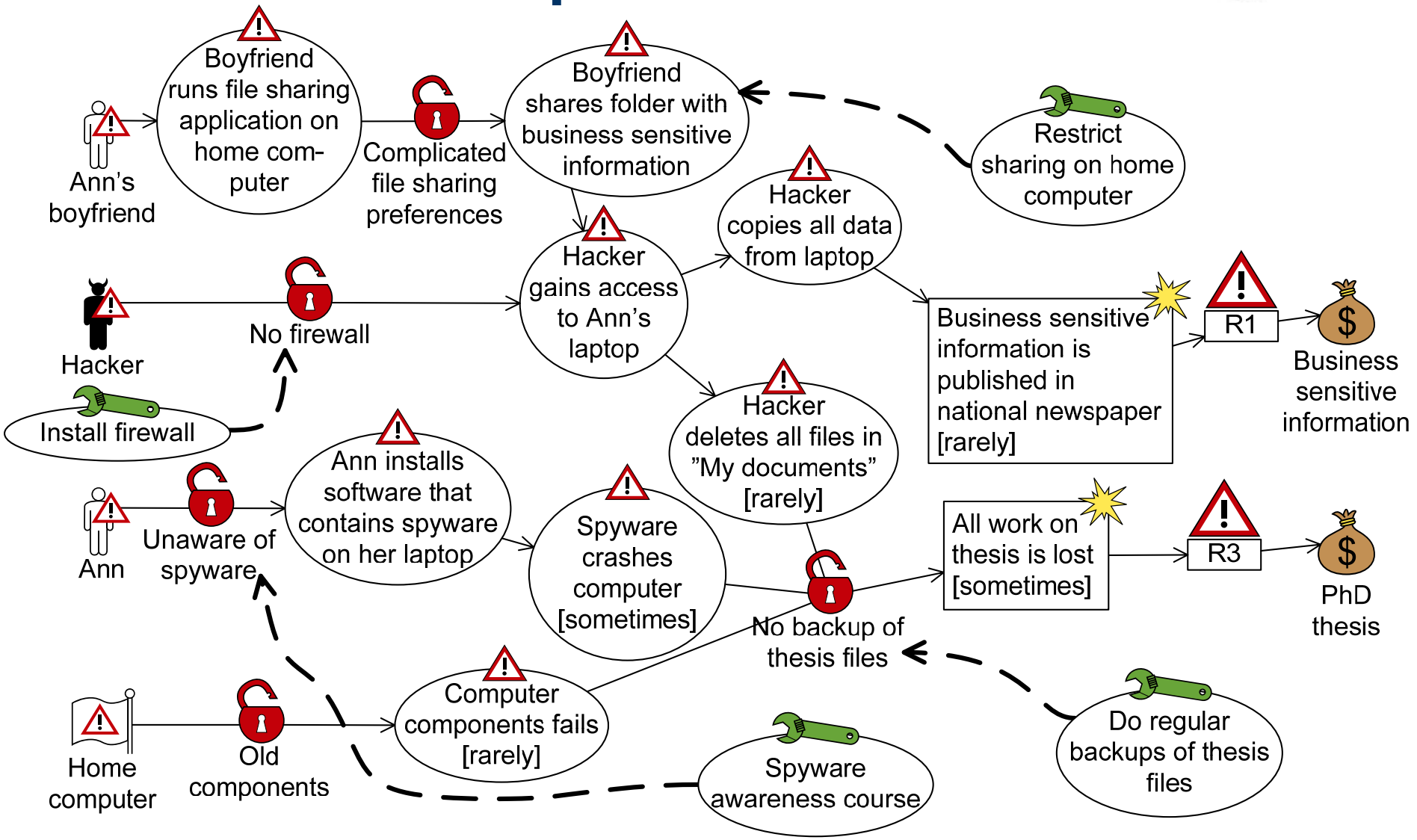


Adding treatments to the threat diagrams

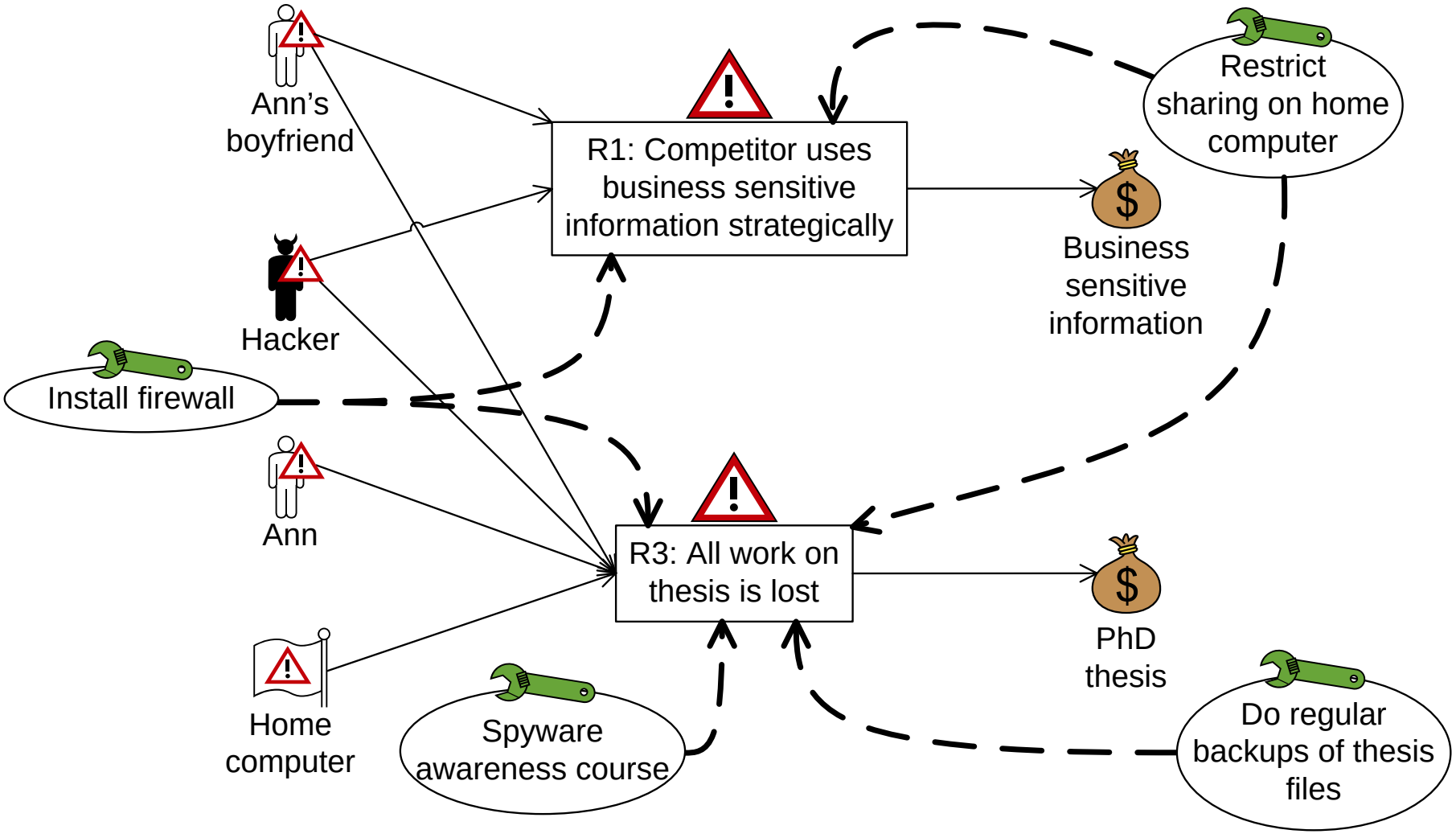


What can we do to reduce the risks to an acceptable level?

Risk treatment



Treatment overview diagram



Executive summary

- The focus of the security risk analysis is data security, in terms of business sensitive data from BC and the PhD thesis itself.
- The scope is data security at home and at work. We do not consider risks involved in transporting the data.
- The unacceptable risks that were uncovered were
  - R1: Competitor uses business sensitive information strategically
  - R3: All work on thesis is lost
- In order to reduce the risks to an acceptable level, the following treatments were suggested:
  - Restrict sharing on home computer
  - Install firewall
  - Spyware awareness course
  - Do regular backups of thesis files

Resources: http://coras.sourceforge.net/

- Downloads
  - The CORAS diagram editor
  - The CORAS icons (Visio stencil, PNG, SVG)
- Publications:
  - Folker den Braber, Ida Hogganvik, Mass Soldal Lund, Ketil Stølen, and Fredrik Vraalsen. **Model-based security analysis in seven steps – a guided tour to the CORAS method.** BT Technology Journal, 25(1): 101 – 117, 2007.
  - Ida Hogganvik. **A graphical approach to security risk analysis.** PhD thesis, Faculty of Mathematics and Natural Sciences, University of Oslo, 2007.
  - Heidi E. I. Dahl and Ida Hogganvik and Ketil Stølen. **Structured semantics for the CORAS security risk modelling language.** Technical report STF07 A970, SINTEF Information and Communication Technology, 2007.

Questions?

Heidi E. I. Dahl
heidi.dahl@sintef.no