Model-Driven Risk Analysis: The CORAS Approach

Le Minh Sang Tran

tran@disi.unitn.it

SINTEF

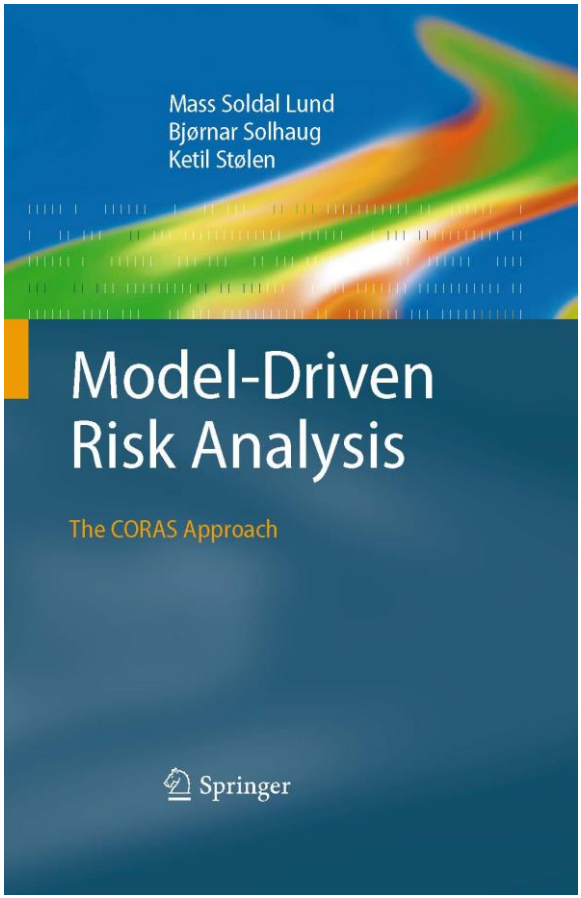
Università degli Studi di Trento

Outline

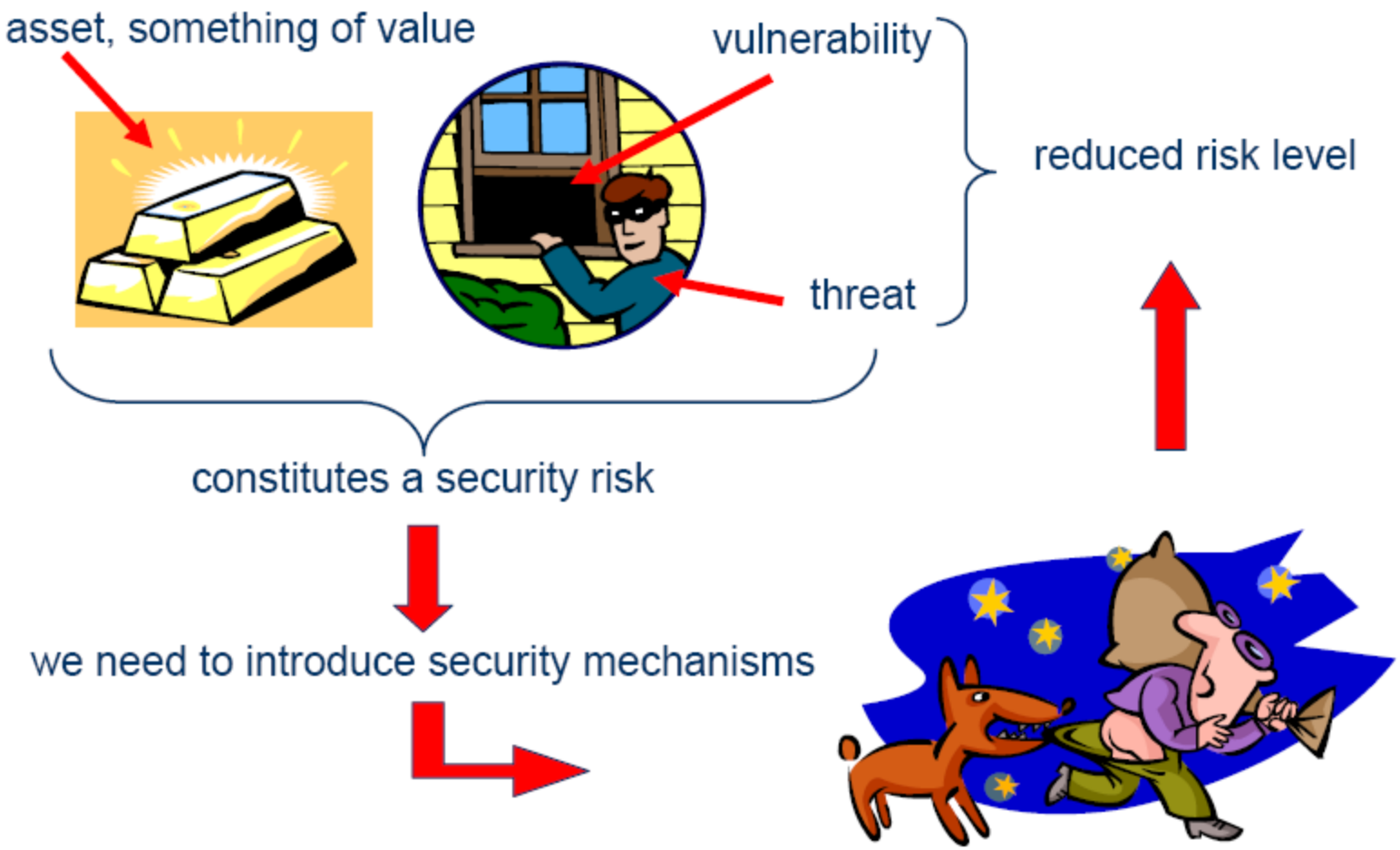
- **What is CORAS?**
  - The CORAS approach
  - Central concepts
- **Steps of risk analysis in CORAS**
- **Tool support and Demo**
- **Summary**

What is CORAS?

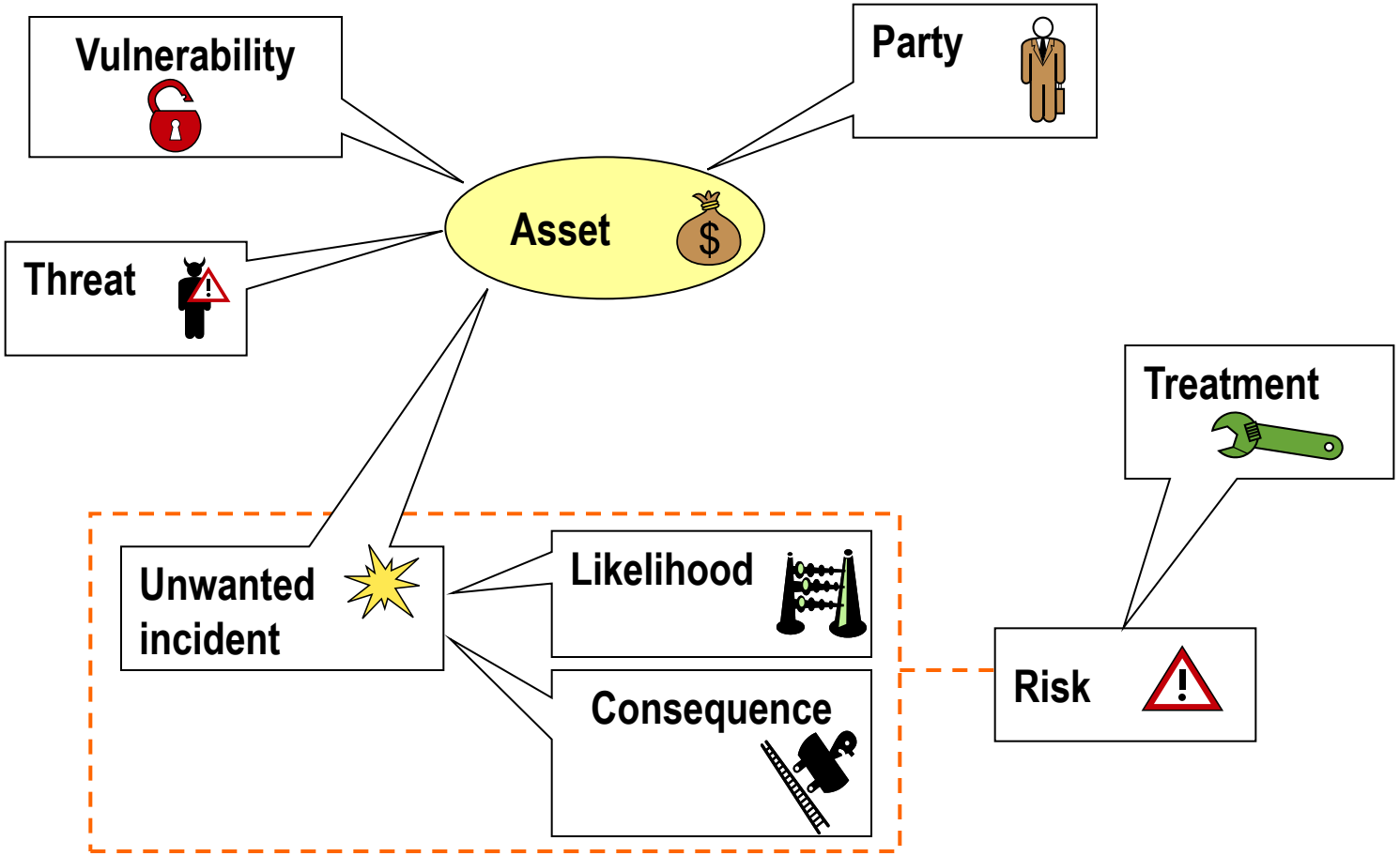
- **The CORAS approach:**
  - A language for risk modeling
  - A tool to support the risk analysis process
  - A method for risk analysis
    - A stepwise, structured and systematic process
    - Asset-driven
    - Concrete tasks with practical guidelines
    - Model-driven
      - Models as basis for and input to analysis tasks
      - Models for documentation of results
- **Based on internationally established standards (*ISO 31000*)**
- **Book:** http://www.springer.com/computer/swe/book/978-3-642-12322-1



Terms

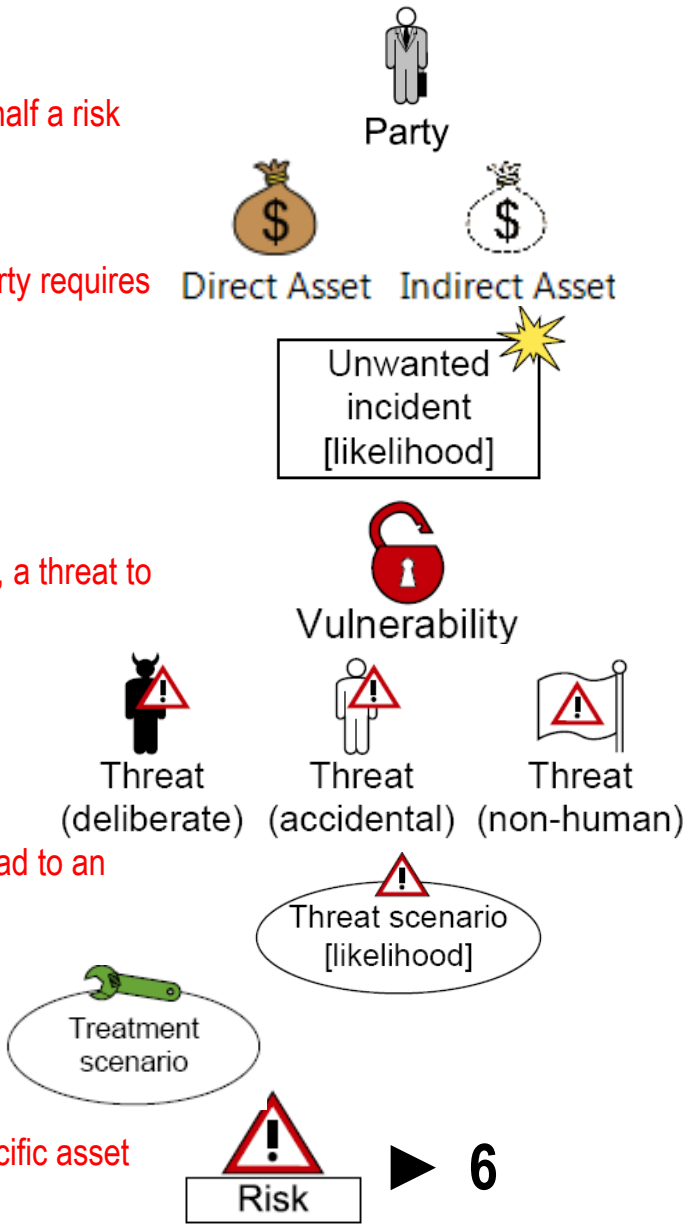

asset, something of value
vulnerability
threat
reduced risk level
constitutes a security risk
we need to introduce security mechanisms

Central Concepts



CORAS Modeling Concepts

- **Party:**
  - An organization, company, person, group or other body on whose behalf a risk analysis is conducted
- **Asset:**
  - Something to which a party assigns value and hence for which the party requires protection
- **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
- **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 (Treatment Scenario):**
  - An appropriate measure to reduce risk level
- **Risk:**
  - The likelihood of an unwanted incident and its consequence for a specific asset

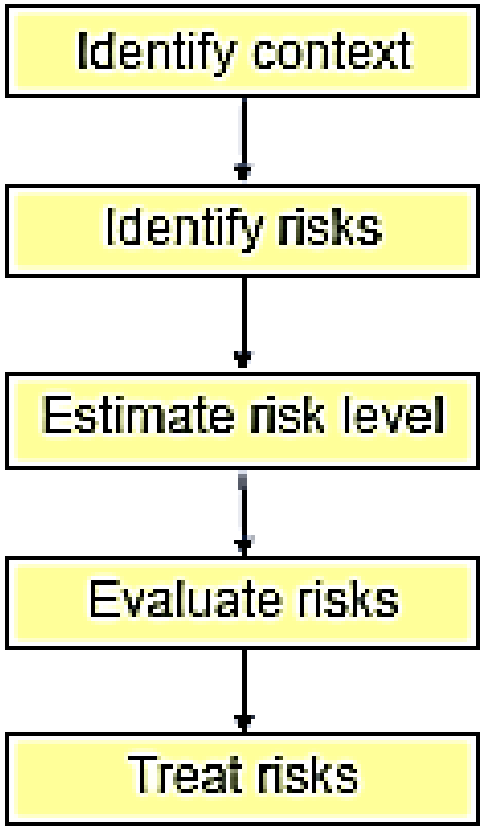


Risk modeling

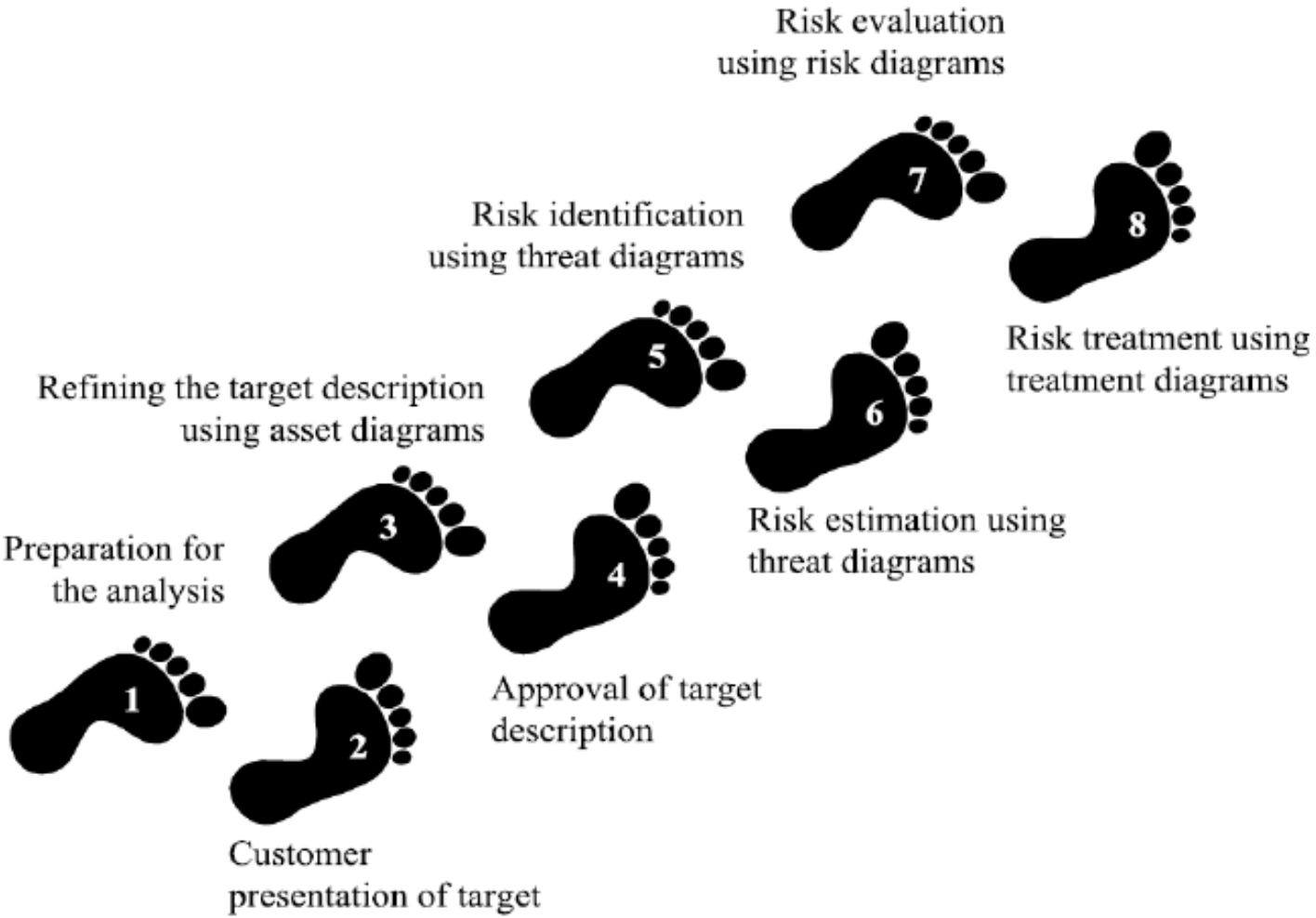
- **The CORAS language consists of five kinds of diagrams**
  - Asset diagrams
  - Threat diagrams
  - Risk diagrams
  - Treatment diagrams
  - Treatment Overview diagrams
- **Each kind of diagram supports specific steps of the risk analysis process**

The CORAS process

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

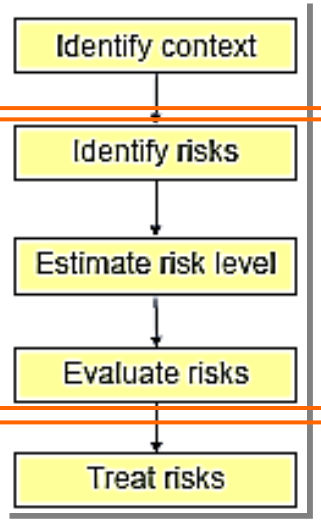


The eight steps of a CORAS risk analysis



The eight steps of a CORAS risk analysis

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



Step 1: Preparation for the analysis

- **Objective: do the necessary initial preparations prior to the actual startup of the analysis**
- **Tasks:**
  - Contact the customer for the case study
  - Roughly setting the scope and focus

Example: AutoParts

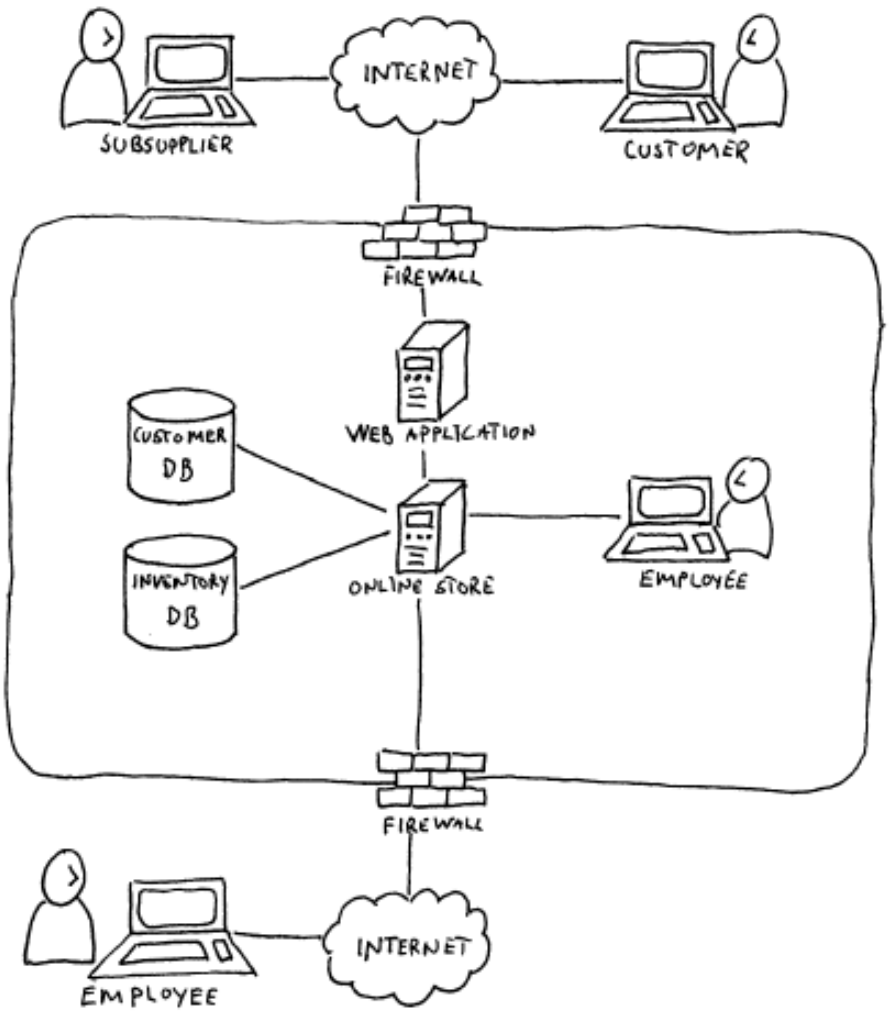
- AutoParts is a company. Its business is to sell spare parts and accessories for a wide range of car makes and vehicle models.
- AutoParts has an automated online store.
- AutoParts is distributing catalogues by mail that present its products and is usually shipping the goods to the customers by cash on delivery mail.
- AutoParts has decided it wants to do a risk analysis of the system.
- Of particular concern for the management is:
  - the web application that connects to both their customer database, their inventory database and their online store.

Step 2: Customer presentation of the target

- **Objective: achieve an initial understanding of the "target" of risk analysis**
- **Tasks:**
  - Customer presentation on the target
  - Target to be understood by risk analysts
  - Set the focus of the analysis
- **Artifact to be produced:**
  - Description of the target:
    - The overall goals of the analysis
    - The target that wishes to have analyzed

Example: Customer presentation on the target

- **Understand customer's goals and target:**
  - Of particular concern for the management is:
    - the web application that connects to both their customer database, their inventory database and their online store.



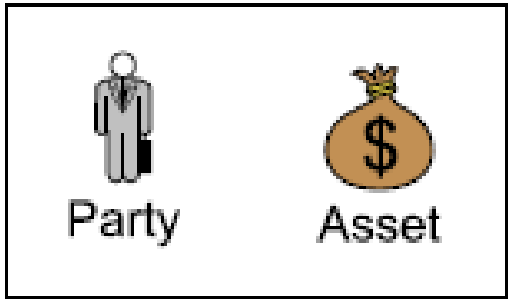
Step 3: Refining the target description using asset diagrams

- **Objective: ensure a common and more precise understanding of the target analysis, including its scope, focus, and main assets**
- **Task:**
  - The target is understood by the risk analysts
  - Identify the parties and assets
  - Conduct a high-level analysis:
    - The first threats, vulnerabilities, threat scenarios and unwanted incidents are identified.
- **Artifacts to be produced:**
  - 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

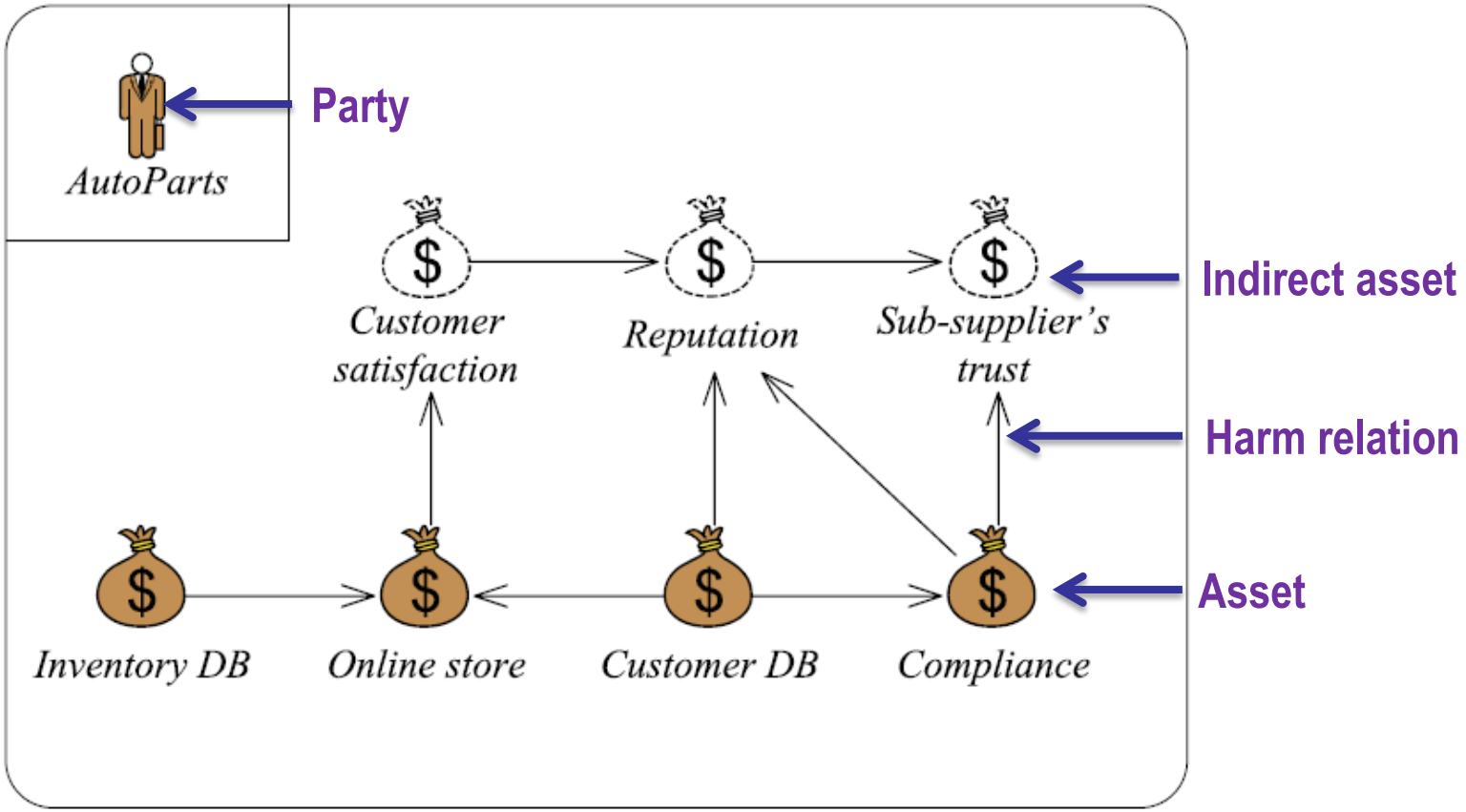
- Notions to be used in Asset Diagram



Example: Identify Party and Asset

- **Party:**
  - AutoParts company
- **Asset:**
  - Inventory DB
  - Customer DB
  - Online store
  - Compliance
  - Company reputation
  - Customer satisfaction
  - Supplier's trust

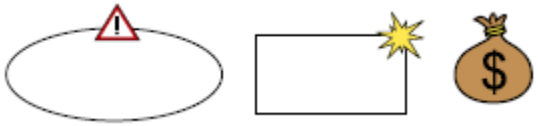
Example: Asset diagram



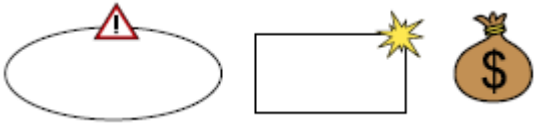
- **Relations between assets**
  - Harm in one asset might harm also other assets.

High level Risk analysis

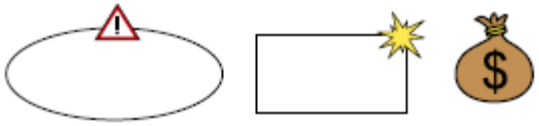
- **Preliminary list of Unwanted Incidents**

 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	Breaks into system and compromises integrity or confidentiality of databases	Use of web application and remote access; insufficient access control
Hacker	Attack compromises integrity or confidentiality of personal data causing loss of compliance with data protection laws	Use of web application and remote access; insufficient access control
Hacker	Introduces virus to the system that compromises integrity or confidentiality of databases	Insufficient virus protection
Hacker	DoS attack causes online store to go down	Use of web application; insufficient DoS attack prevention

Example: High level Risk analysis

 Who/ What is the cause?	 How? What may happen? What does it harm?	 What makes this possible?
System failure	Online store goes down because of failure of web application or loss of network connection	Immature technology; loss of network connection
Employee of AutoParts	Collection and processing of personal data diverge from data protection laws	Lack of competence on data protection laws; insufficient routines for processing personal data
Employee of AutoParts	Sloppiness compromises integrity or confidentiality of databases	Lack of competence; work processes not aligned with policy

Step 4: Approval of the target description

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

Define Likelihood scale

- **Likelihood: the frequency or probability of something to occur**
- **Example of Likelihood scale**

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 Likelihood scale

- **Example of Likelihood scale**

Likelihood	Description
Rarely	A very high number of similar occurrences already on record; has occurred a very high number
Sometimes	A significant number of similar occurrences already on record; has occurred a significant
Regularly	Several similar occurrences on record; has occurred more than once
Often	….
…	….

Define Consequence scale

- **Consequence:**
- **Example of Consequence scale (for direct asset: Inventory DB)**

Consequence	Description
Catastrophic	Range of [50%,100%] of records are affected
Serious	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

- **Example of Consequence scale (for direct asset: Online Store)**

Consequence	Description
Catastrophic	Downtime in range [1 week,∞>
Serious	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

- **Example of Consequence scale (for direct asset: Customer DB)**

Consequence	Description
Catastrophic	Range of [50%,100%] of records are affected
Serious	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

- **Example of Consequence scale (for direct asset: Compliance)**

Consequence	Description
Catastrophic	Chief executive officer is sentenced to jail for more than 1 year
Serious	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 Function and evaluation criteria

- **Determine level of risk as a function of likelihood and consequence**

Risk Function (Inventory DB)					
Consequence/ Likelihood	**Insignificant**	**Minor**	**Moderate**	**Serious**	**Catastrophic**
Rare					
Unlikely					
Possible					
Likely					
Certain					

Acceptable

Monitor

Need to be treated

Example: Risk Function and evaluation criteria

- Determine level of risk as a function of likelihood and consequence

Risk Function (Online Store)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Serious	Catastrophic
Rare					
Unlikely					
Possible					
Likely					
Certain					

Acceptable

Monitor

Need to be treated

Example: Risk Function and evaluation criteria

- Determine level of risk as a function of likelihood and consequence

Risk Function (Customer DB)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Serious	Catastrophic
Rare					
Unlikely					
Possible					
Likely					
Certain					

Acceptable

Monitor

Need to be treated

Example: Risk Function and evaluation criteria

- Determine level of risk as a function of likelihood and consequence

Risk Function (Compliance)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Serious	Catastrophic
Rare					
Unlikely					
Possible					
Likely					
Certain					

Acceptable

Monitor

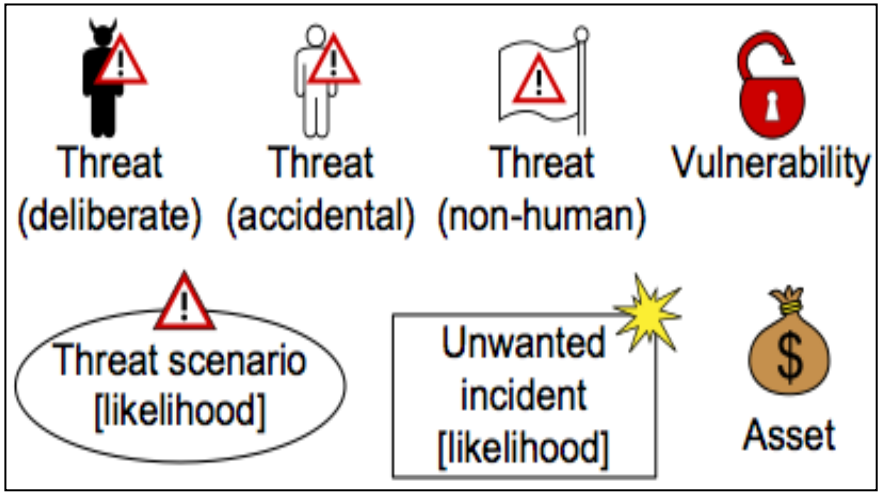
Need to be treated

Step 5: Risk Identification using Threat diagrams

- **Objective: Identify and document risks through the identification and documentation of unwanted incidents, threats, threat scenarios and vulnerabilities**
- **Tasks:**
  - Identify risk that might harm clients' assets
    - How a **threat** exploits a **vulnerability** to cause an **unwanted incident** that harms the client's **asset**
    - *(proposed)* Sub steps:
      - Identify Assets and Threats
      - Identify Unwanted Incidents
      - Identify Threat Scenarios
      - Identify Vulnerabilities
- **Artifact to be produced:**
  - Threat diagram

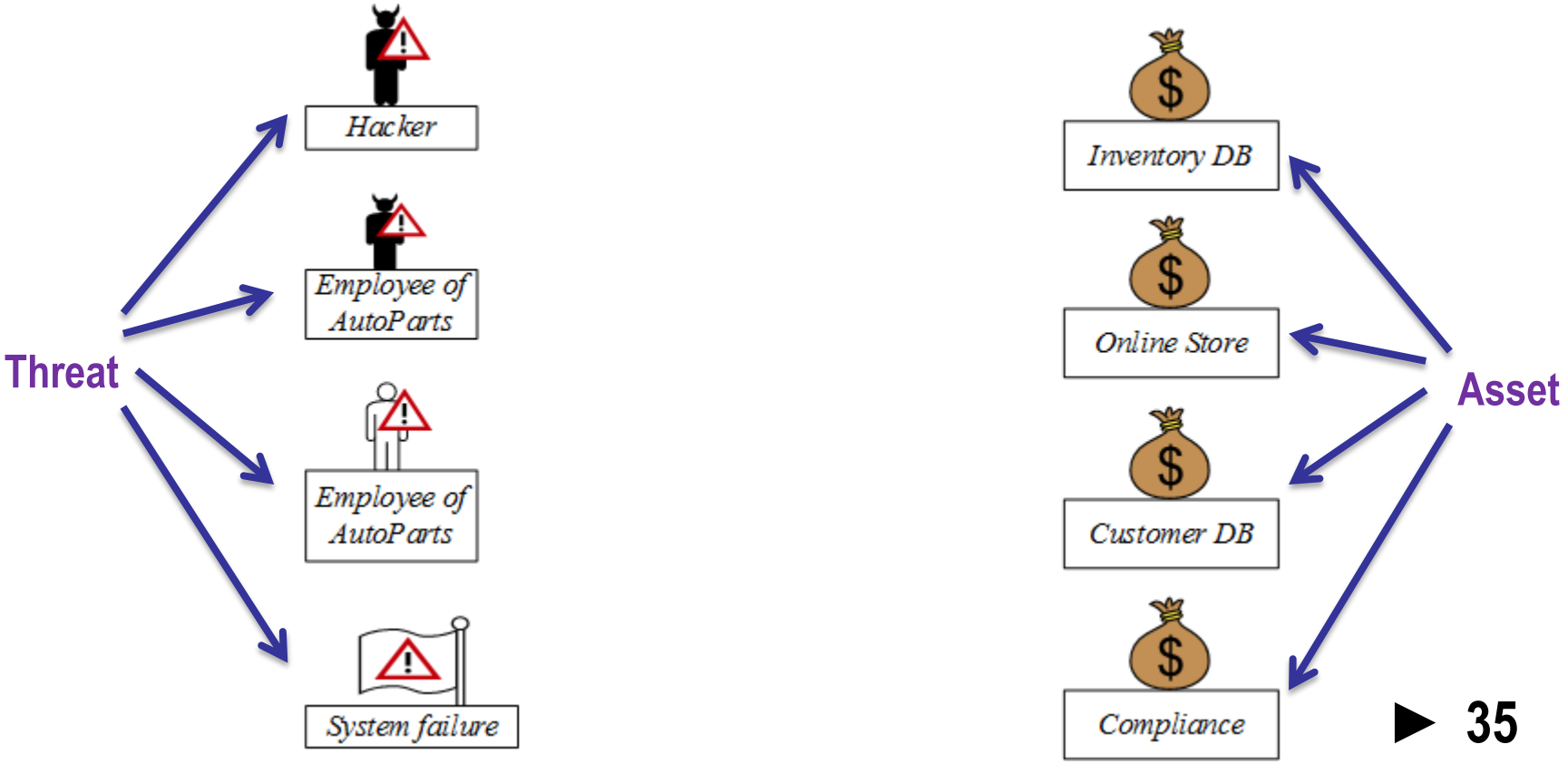
Step 5: Risk Identification using Threat diagrams

- **Notions to be used in Threat Diagram**



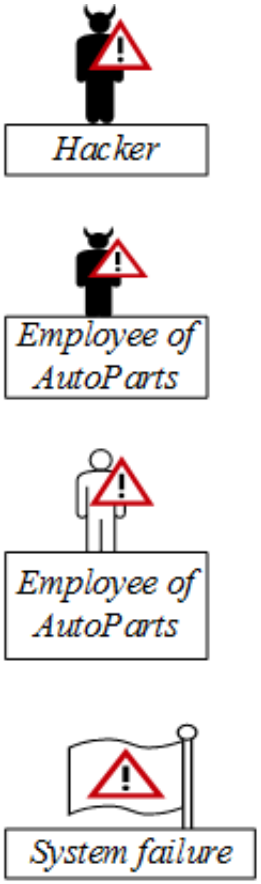
Step 5 - sub step 1: Identify Assets and Threats

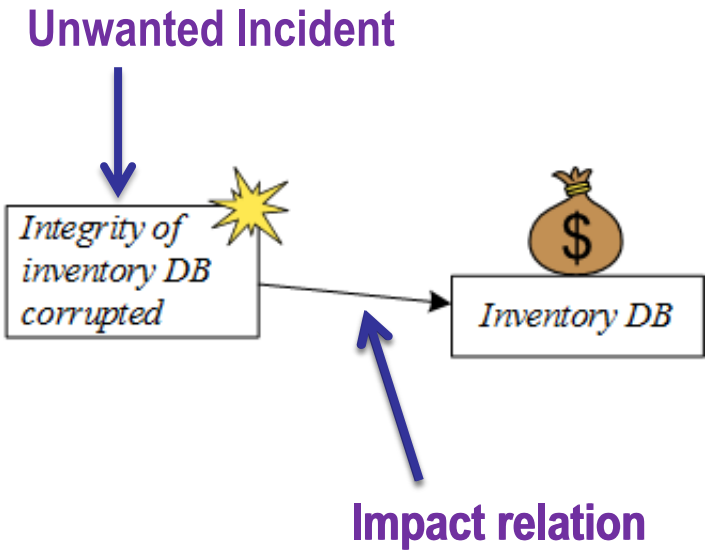
- **Answer the question: "What are the threats?"**
  - Hints:
    - "Accidental threat": users/ roles inside the system
    - Attackers from outside: "deliberate threat"



Step 5 - sub step 2: Identify Unwanted Incidents

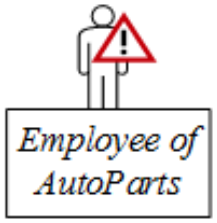
- **Answer the question:**
  - What (unwanted incidents) do we fear will happen?

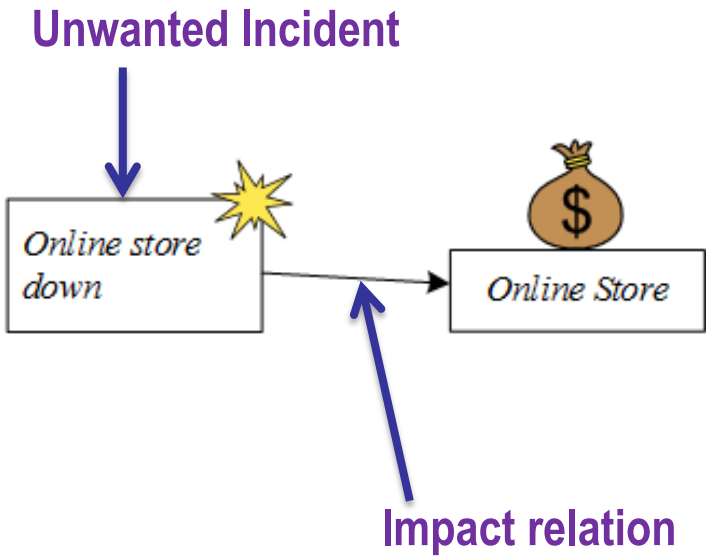




Step 5 - sub step 2: Identify Unwanted Incidents

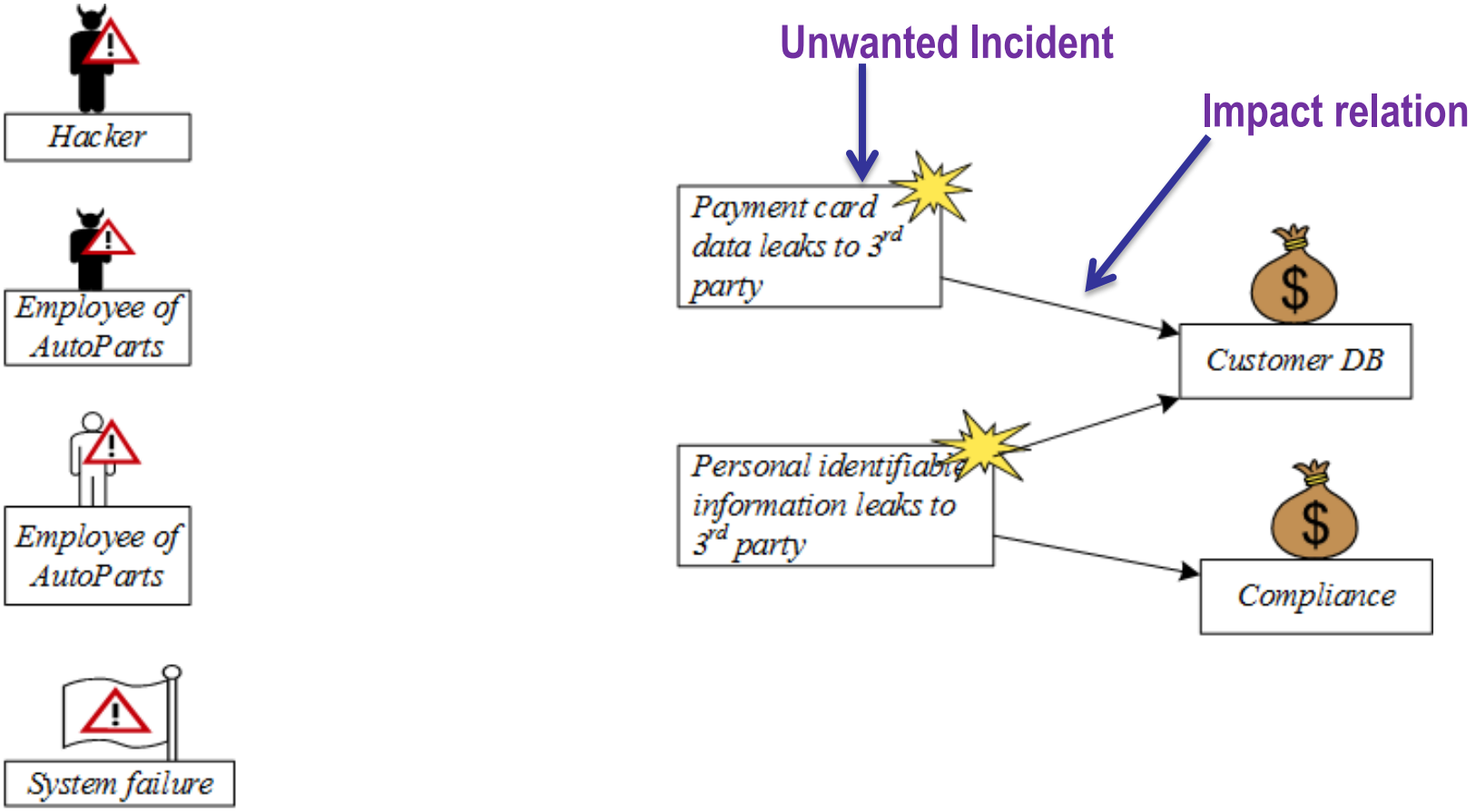
- **Answer the question:**
  - What (unwanted incidents) do we fear will happen?





Step 5 - sub step 2: Identify Unwanted Incidents

- **Answer the question:**
  - What (unwanted incidents) do we fear will happen?

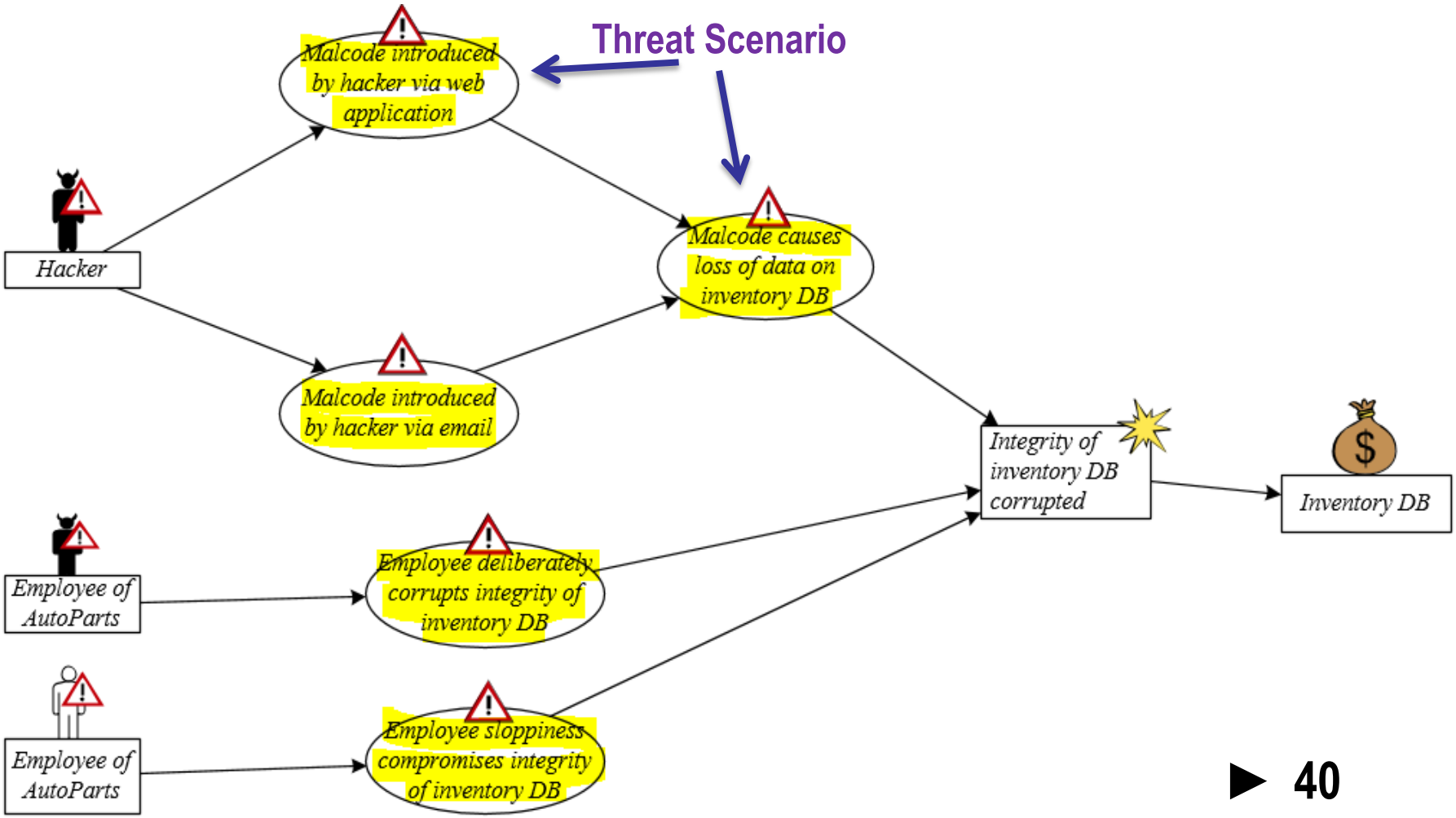


Step 5 - sub step 3: Identify Threat Scenarios

- **Answer the question:**
  - How does it happen? It happens by which threat scenarios?

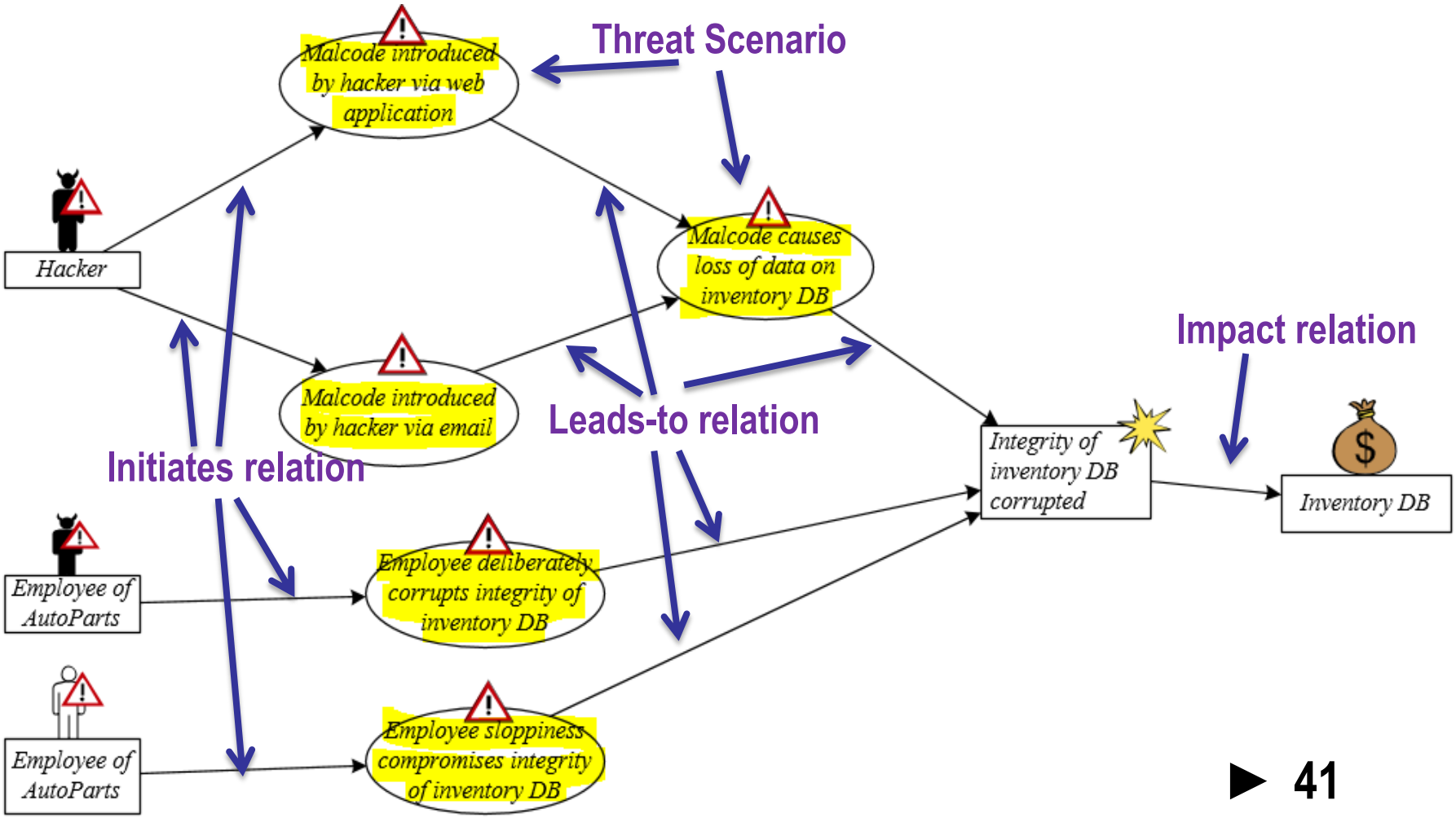
Step 5 - sub step 3: Identify Threat Scenarios

- **Answer the question:**
  - How does it happen? It happens by which threat scenarios?



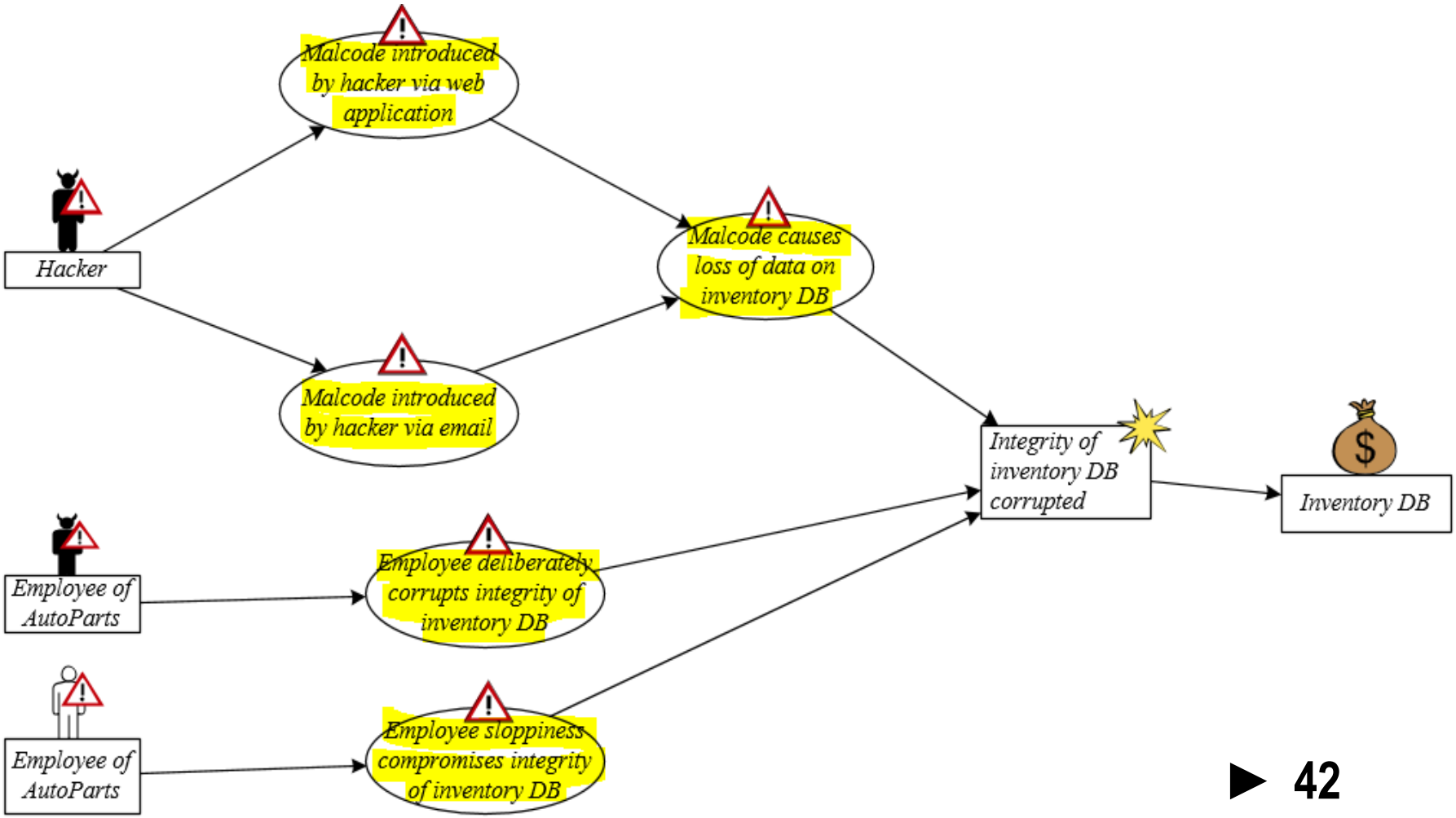
Step 5 - sub step 3: Identify Threat Scenarios

- **Answer the question:**
  - How does it happen? It happens by which threat scenarios?

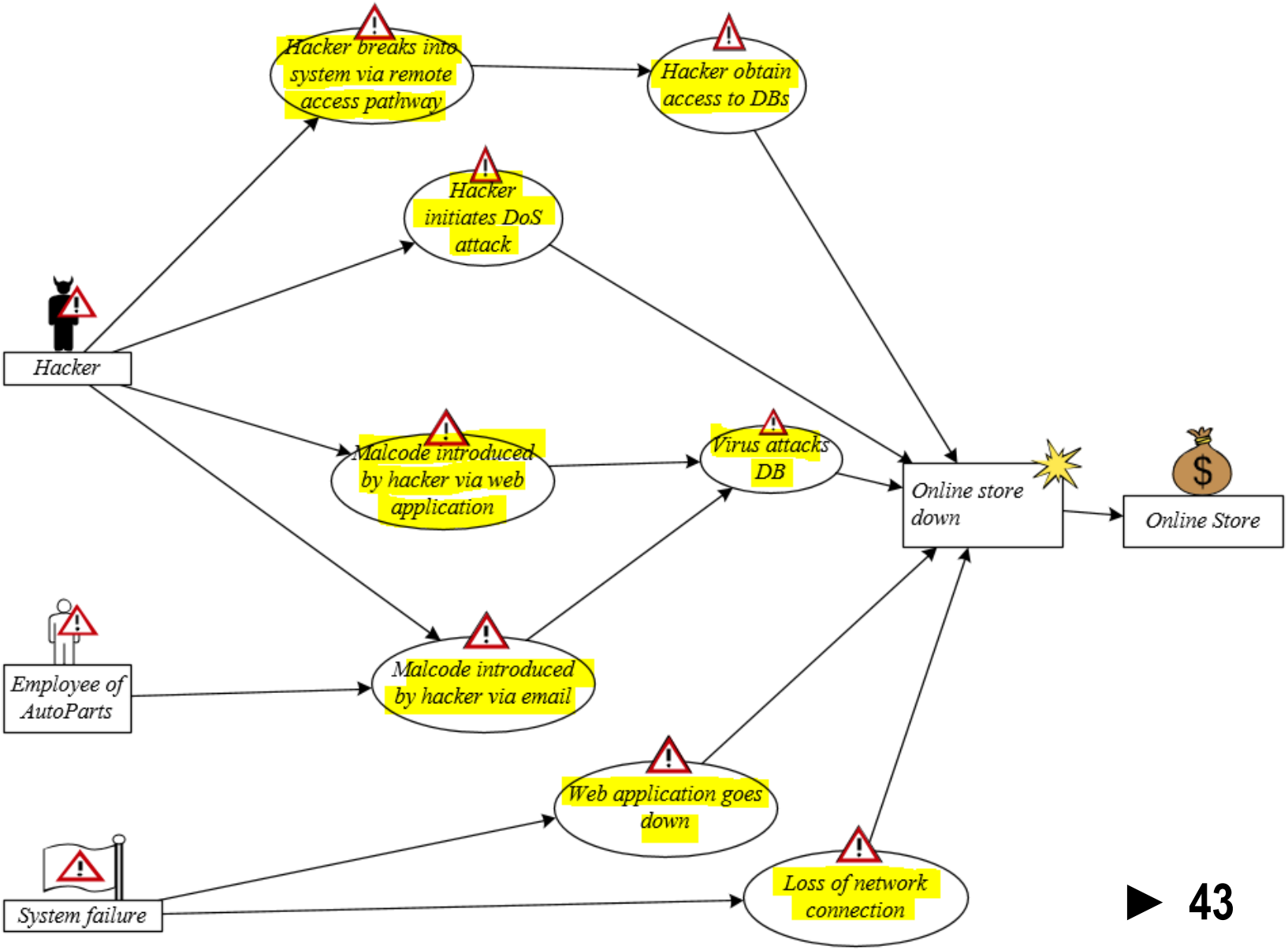


Step 5 - sub step 3: Identify Threat Scenarios

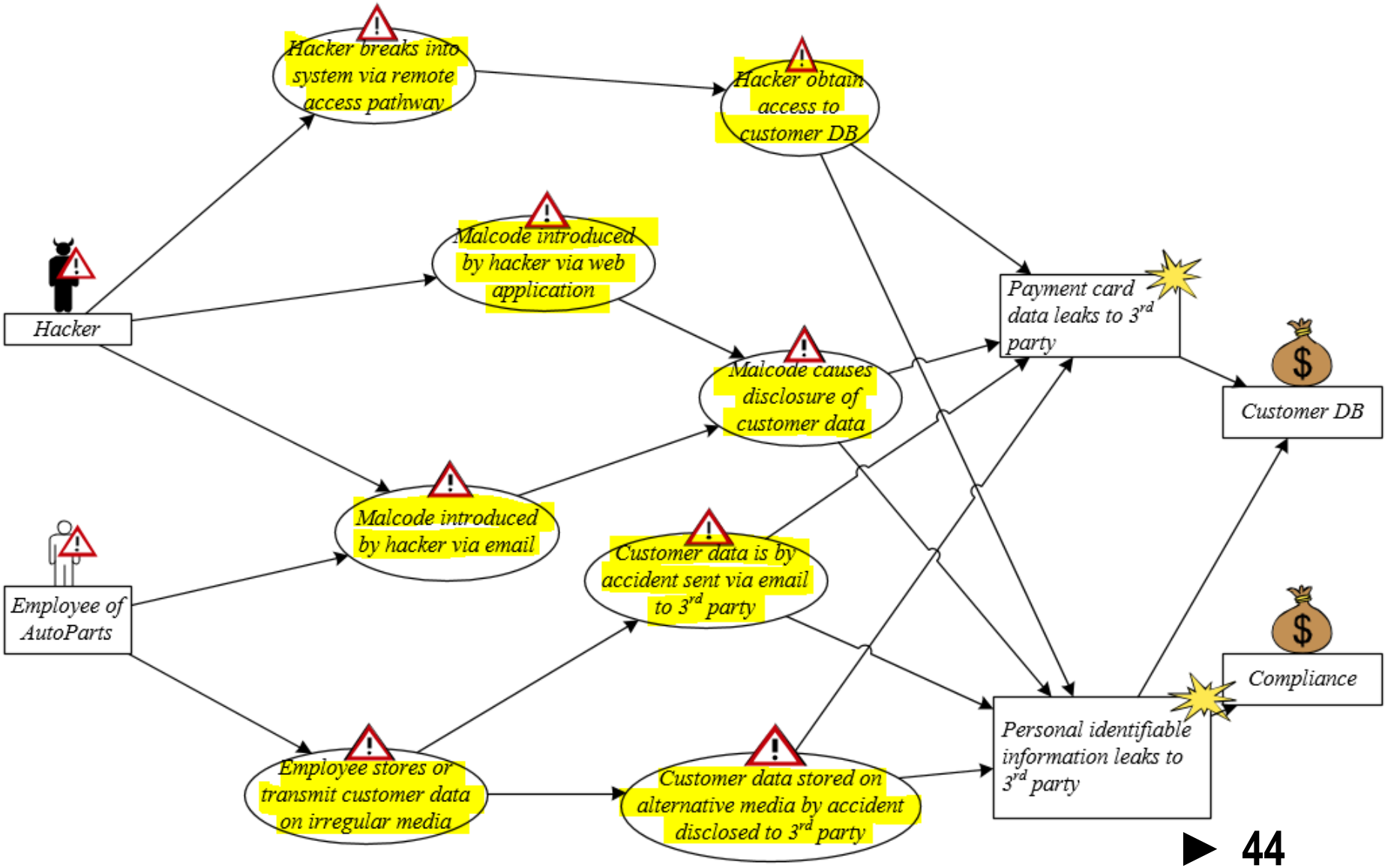
- **Answer the question:**
  - How does it happen? It happens by which threat scenarios?



Step 5 - sub step 3: Identify Threat Scenarios



Step 5 - sub step 3: Identify Threat Scenarios

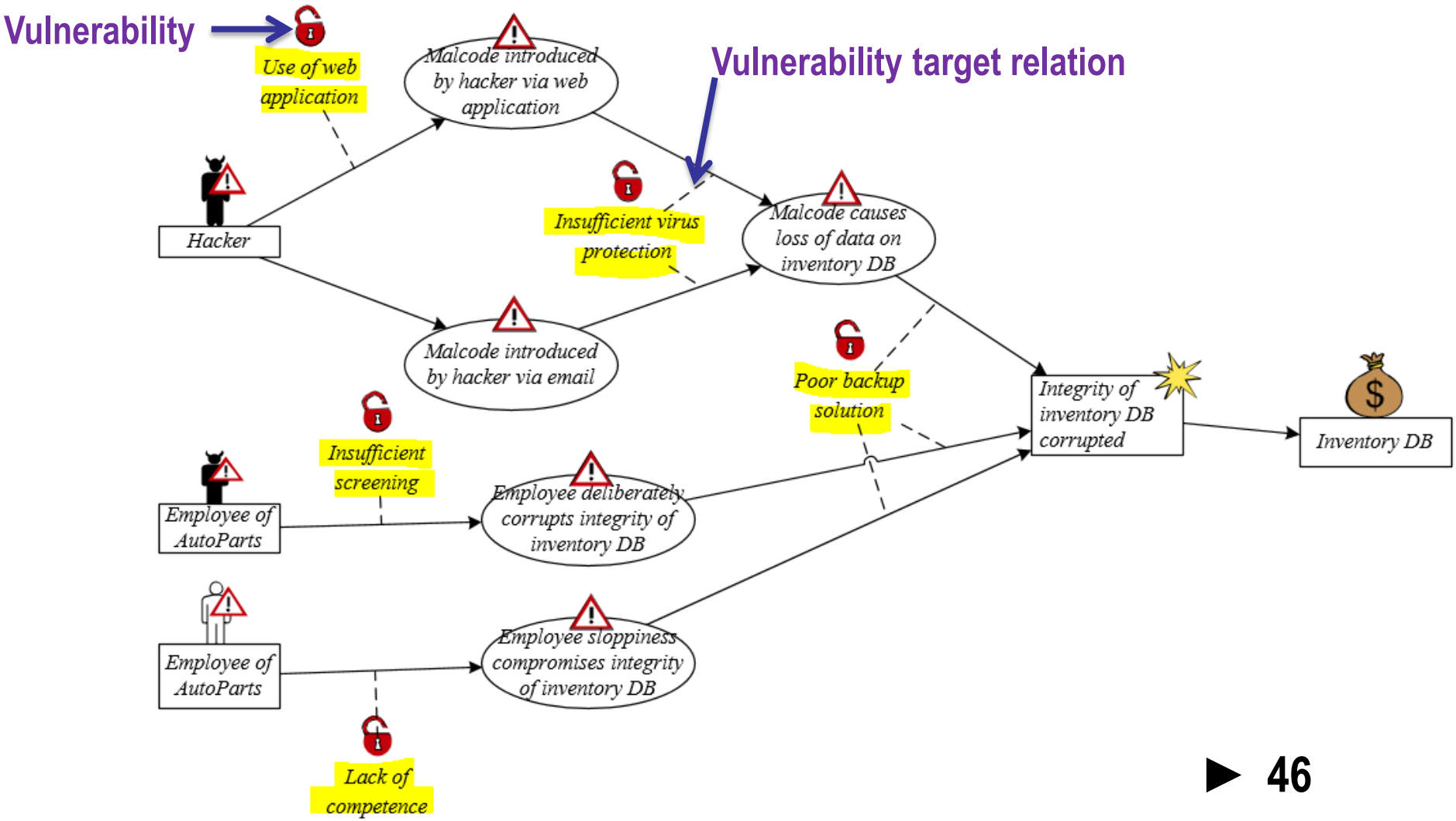


Step 5 - sub step 4: Identify Vulnerabilities

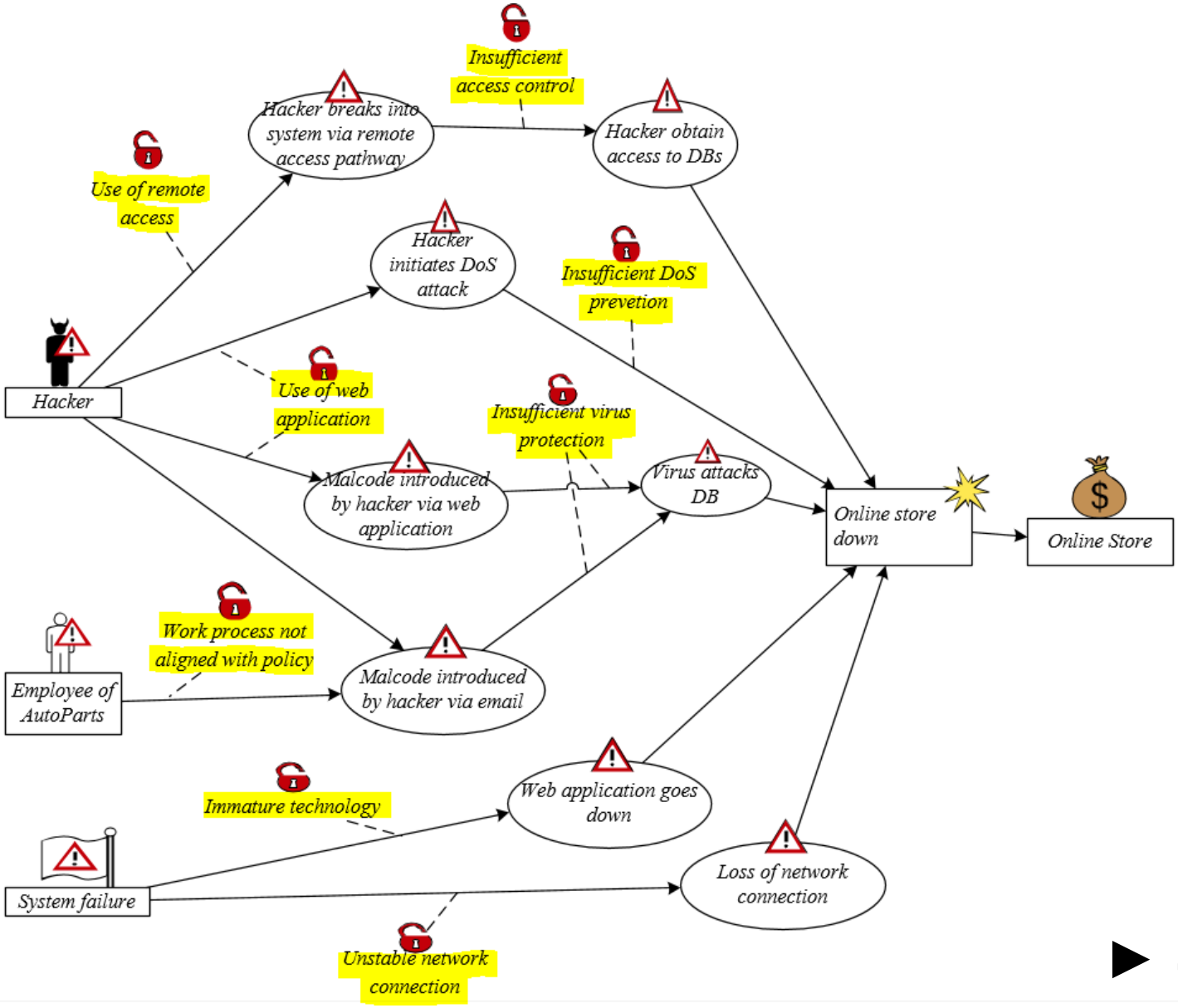
- **Answer the question:**
  - Which vulnerabilities make this possible?

Step 5 - sub step 4: Identify Vulnerabilities

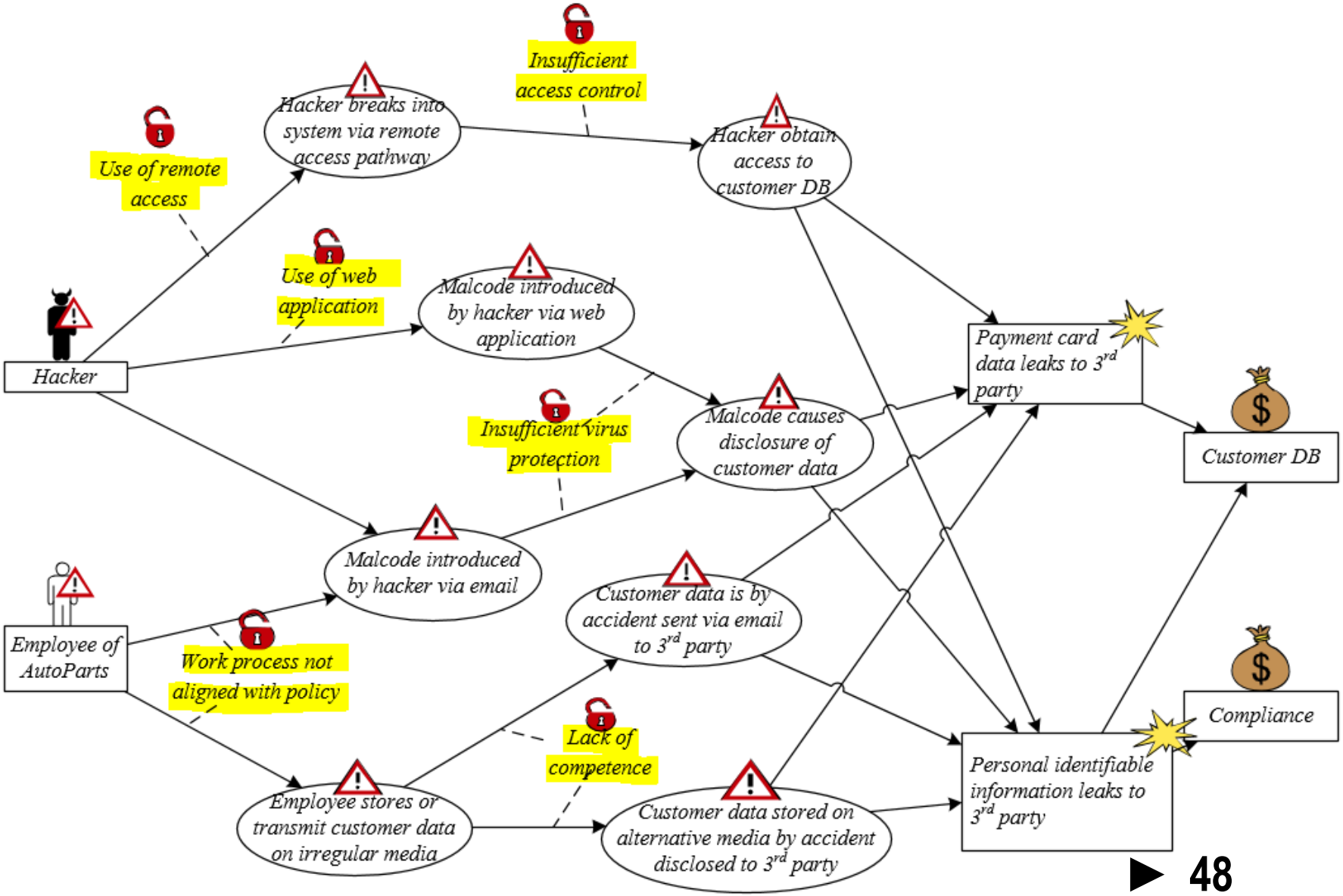
- **Answer the question:**
  - Which vulnerabilities make this possible?



Step 5 - sub step 4: Identify Vulnerabilities



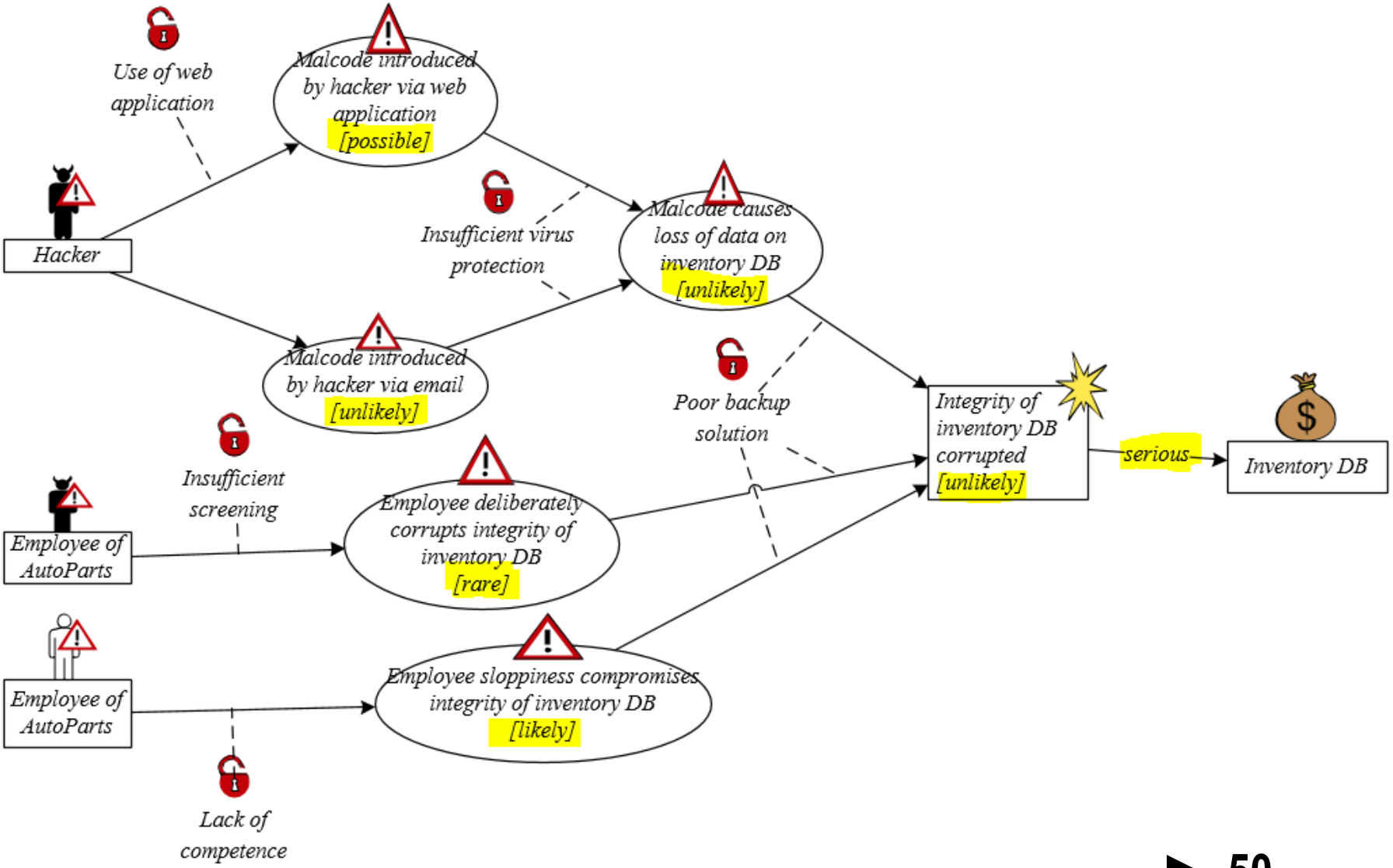
Step 5 - sub step 4: Identify Vulnerabilities



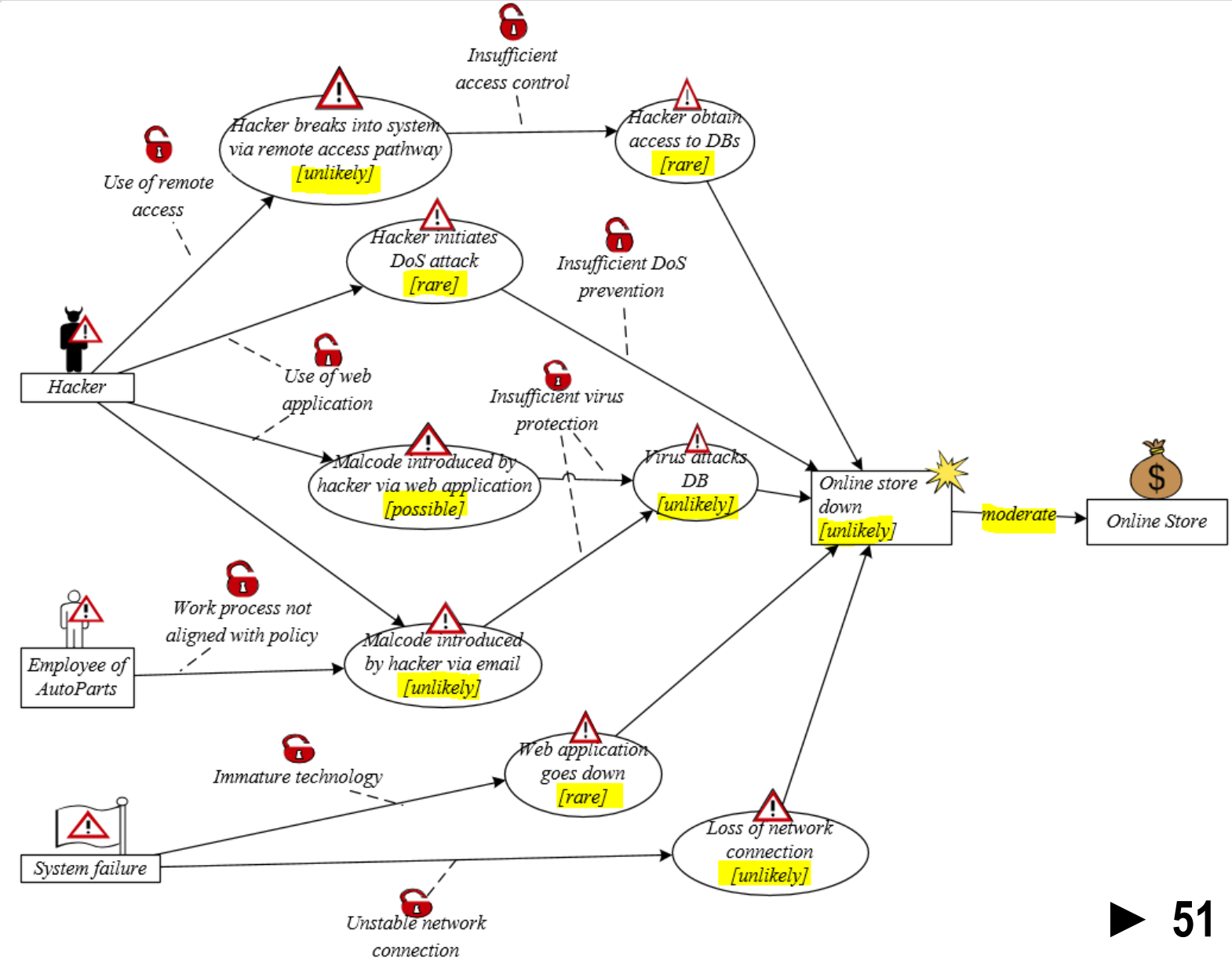
Step 6: Risk estimation using threat diagrams

- **Objective: determine risk level of the identified risks**
- **Tasks: base on likelihood and consequence scale approved in Step 4**
  - 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 to be produced:**
  - Completed Threat diagrams with likelihood and consequences assigned

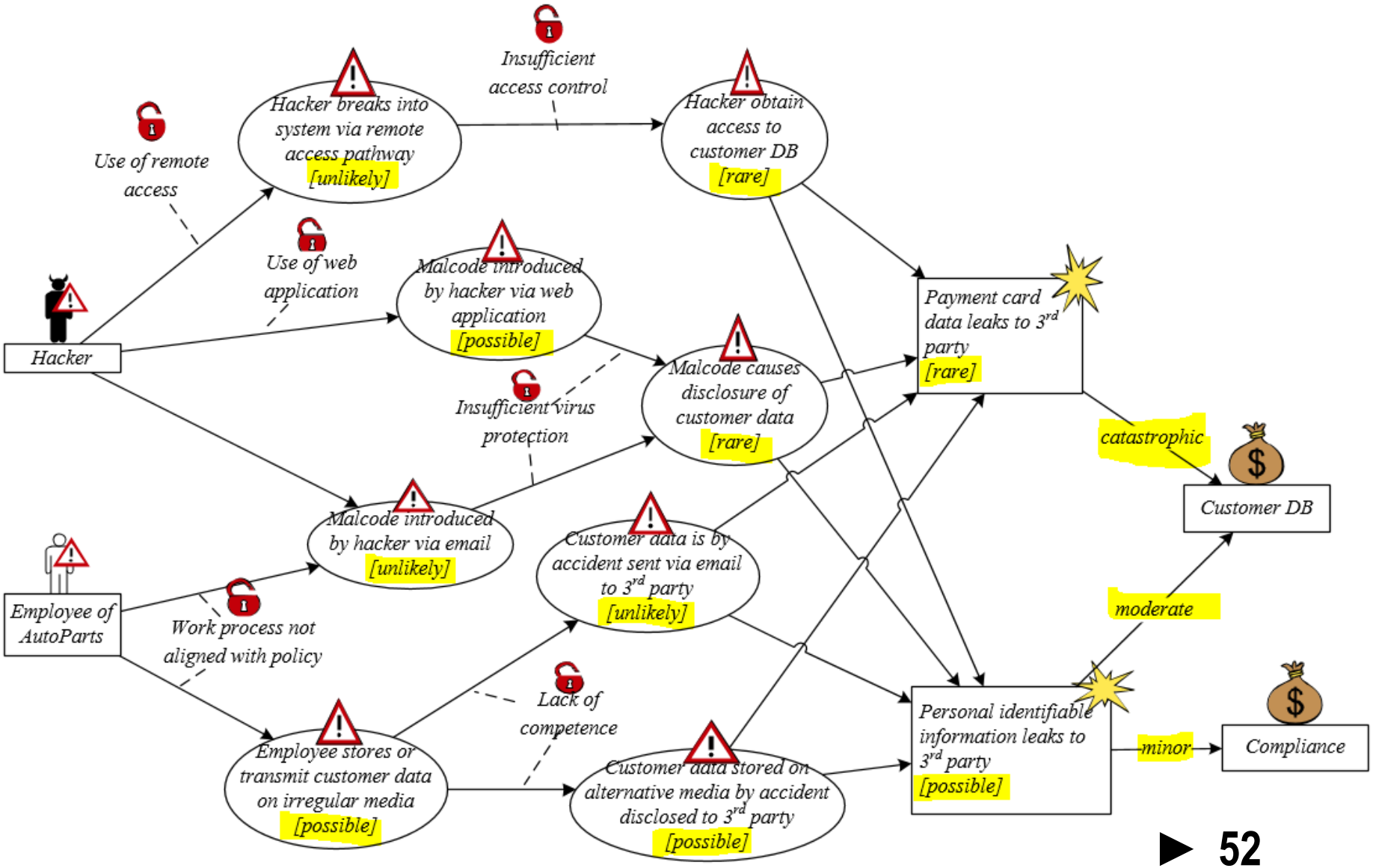
Example: Assign Likelihood and Consequence



Example: Assign Likelihood and Consequence



Example: Assign Likelihood and Consequence



Step 7: Risk evaluation using Risk diagram

- **Objective: decide which of the identified risks are acceptable and which must be further evaluated for possible treatment**
- **Tasks:**
  - Evaluate the identified risks:
    - Enter 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 to be produced:**
  - Completed Risk Function
  - Risk Diagram with evaluation result
-

Example: Completed Risk Function

Risk Function (Inventory DB)					
Consequence/ Likelihood	**Insignificant**	**Minor**	**Moderate**	**Serious**	**Catastrophic**
Rare					
Unlikely				*R1:Integrity of inventory DB corrupted*	
Possible					
Likely					
Certain					

Acceptable

Monitor

Need to be treated

Example: Completed Risk Function

Risk Function (Online Store)					
Consequence/ Likelihood	**Insignificant**	**Minor**	**Moderate**	**Serious**	**Catastrophic**
Rare					
Unlikely			*R2:Online store down*		
Possible					
Likely					
Certain					

Acceptable

Monitor

Need to be treated

Example: Completed Risk Function

Risk Function (Customer DB)					
Consequence/ Likelihood	**Insignificant**	**Minor**	**Moderate**	**Serious**	**Catastrophic**
Rare					*R3: Payment card data leaks to 3rd party*
Unlikely					
Possible			*R4: Personal identifiable information leaks to 3rd party*		
Likely					
Certain					

Acceptable

Monitor

Need to be treated

Example: Completed Risk Function

Risk Function (Compliance)					
Consequence/ Likelihood	**Insignificant**	**Minor**	**Moderate**	**Serious**	**Catastrophic**
Rare					
Unlikely					
Possible		*R5: Personal identifiable information leaks to 3rd party*			
Likely					
Certain					

Acceptable

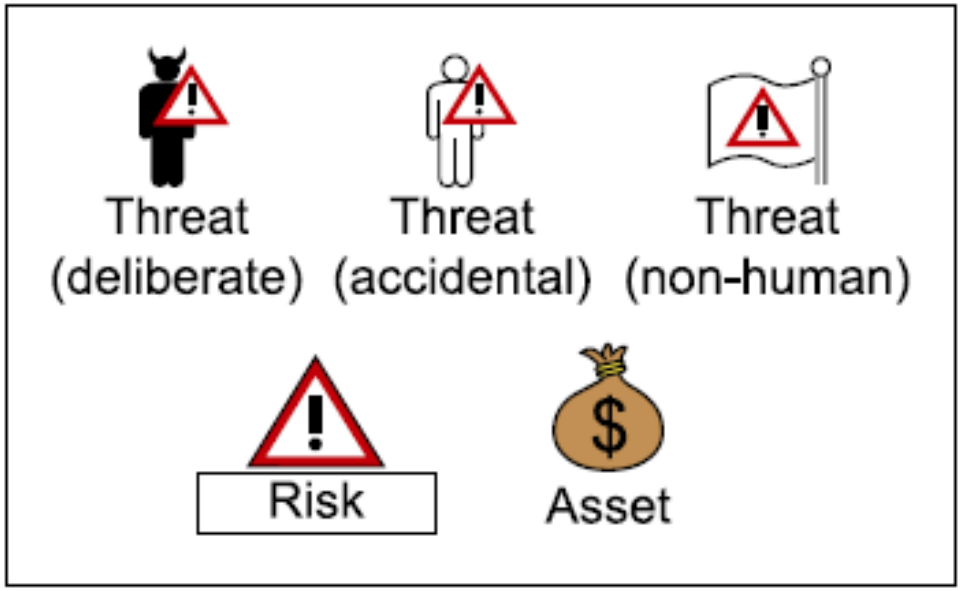
Monitor

Need to be treated

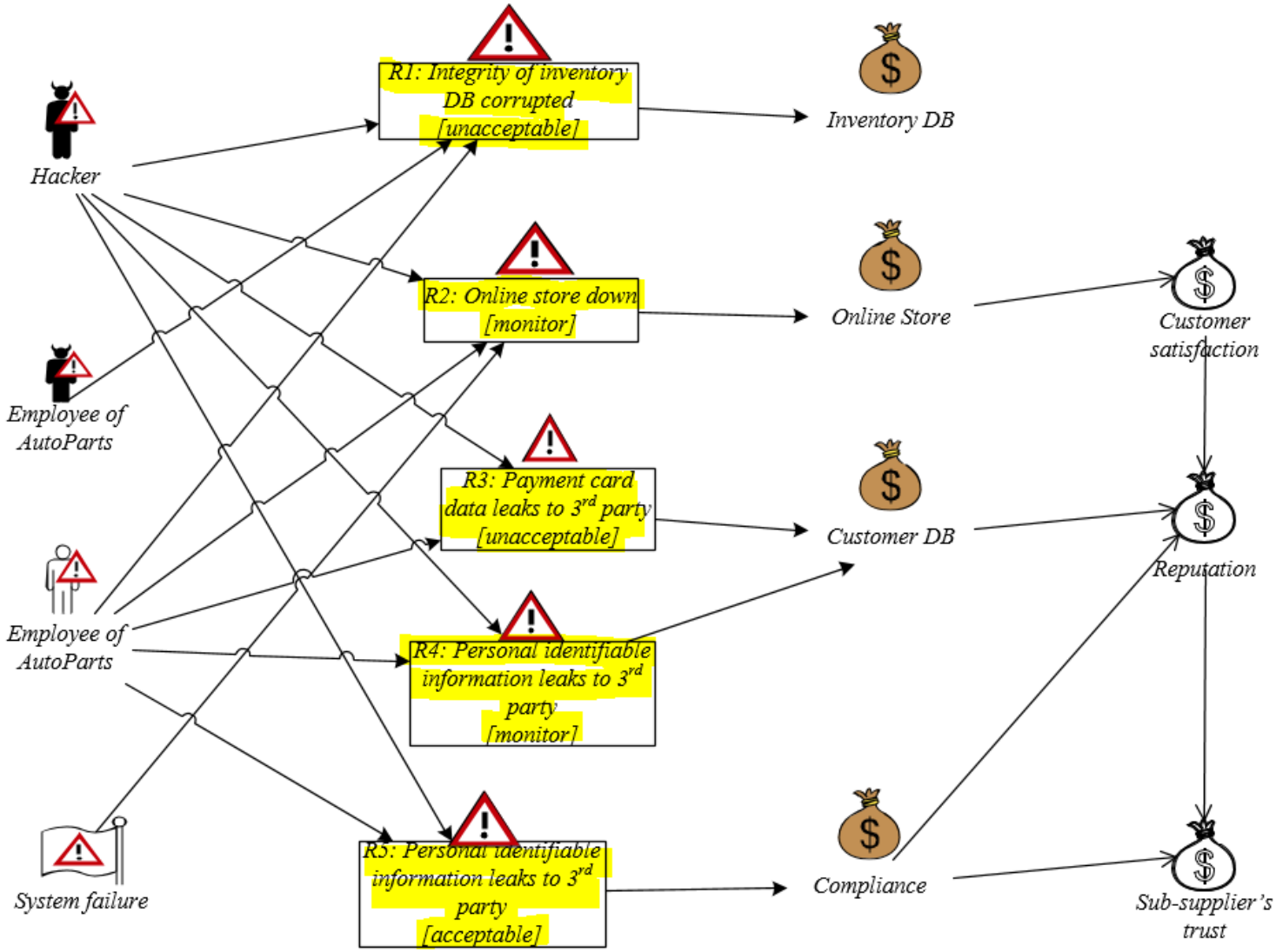
Summarizing the Risk picture

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

- Notions to be used in Risk diagram:



Example: Risk diagram

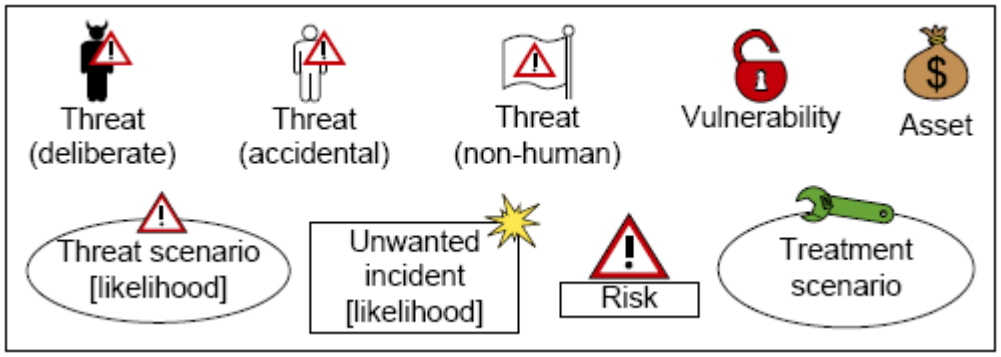


Step 8: Risk treatment using Treatment diagram

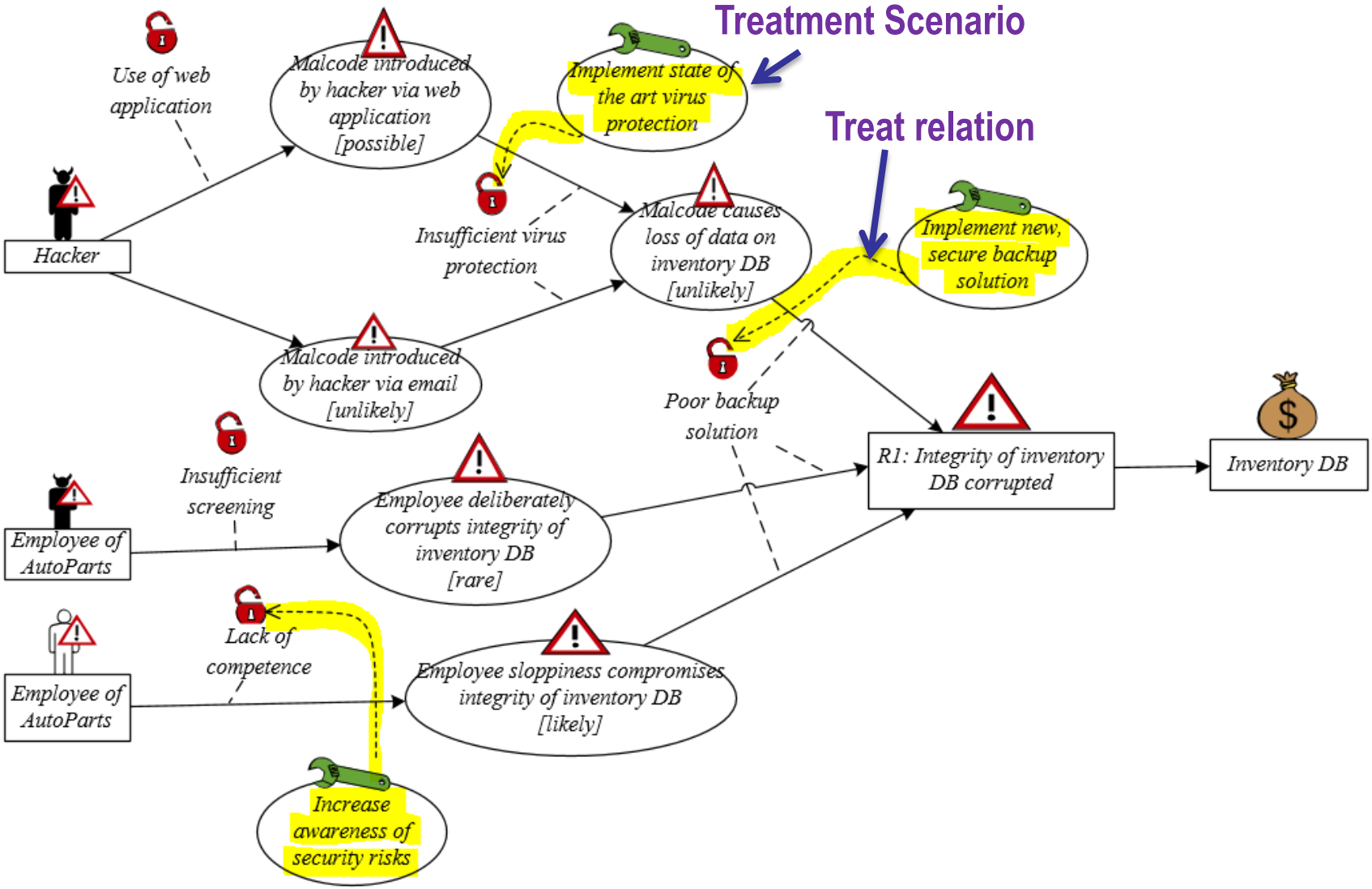
- **Objective: identify cost effective treatments for the unacceptable risks**
- **Task:**
  - Identify Treatment Scenario for unacceptable risks:
    - What can we do to reduce the risks to an acceptable (or monitor) level?
  - Create Treatment diagram
  - Summarize by Treatment Overview diagram
  - Evaluate treatment: estimate the cost-benefit of each treatment, and decide which ones to implement
- **Artifacts to be produced:**
  - Treatment diagram (=Threat diagram with Treatment added)
  - Treatment Overview diagram
  - Treatment evaluation

Step 8: Risk treatment using treatment diagram

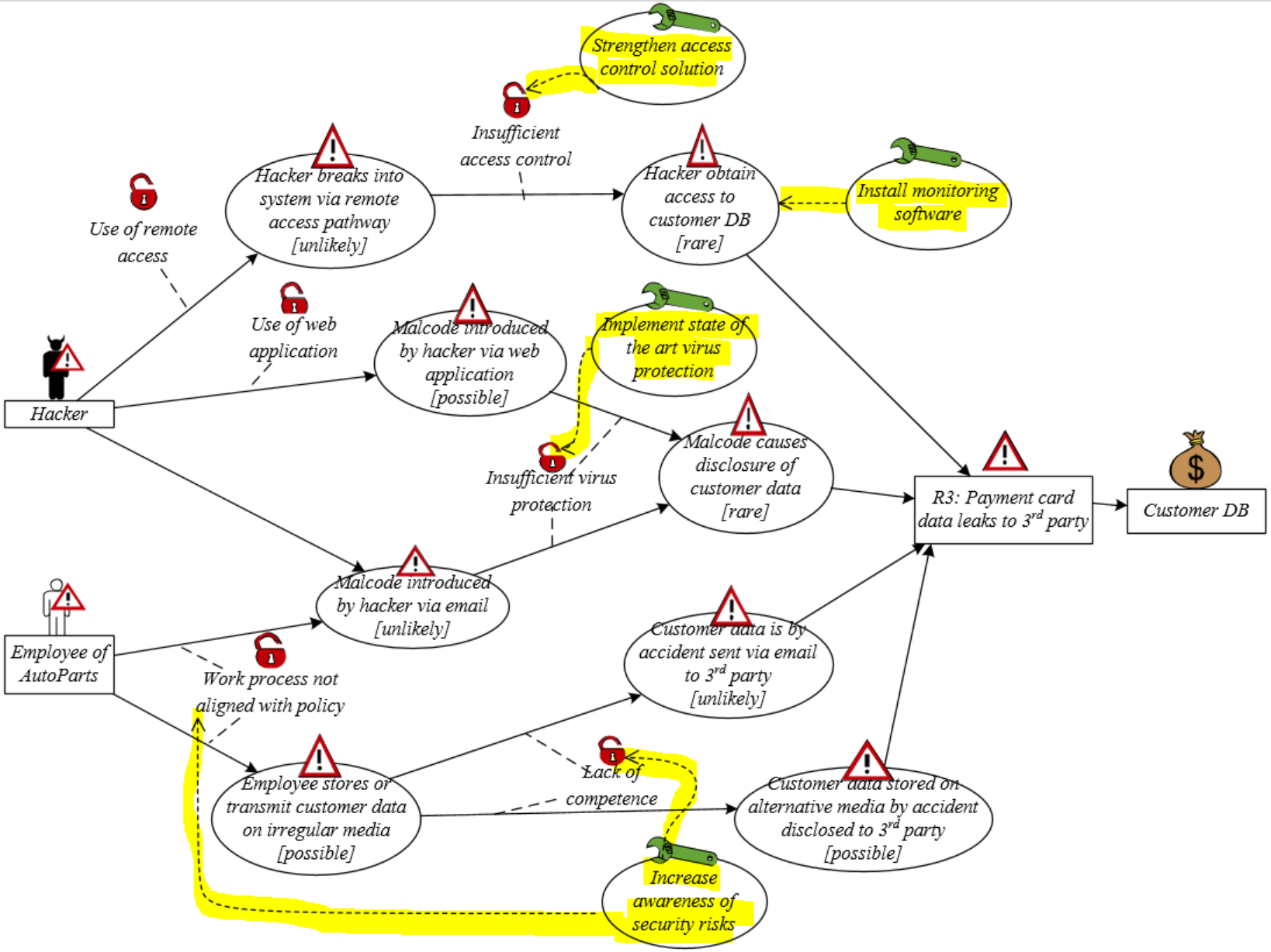
- **Notions to be used in Treatment Diagram**



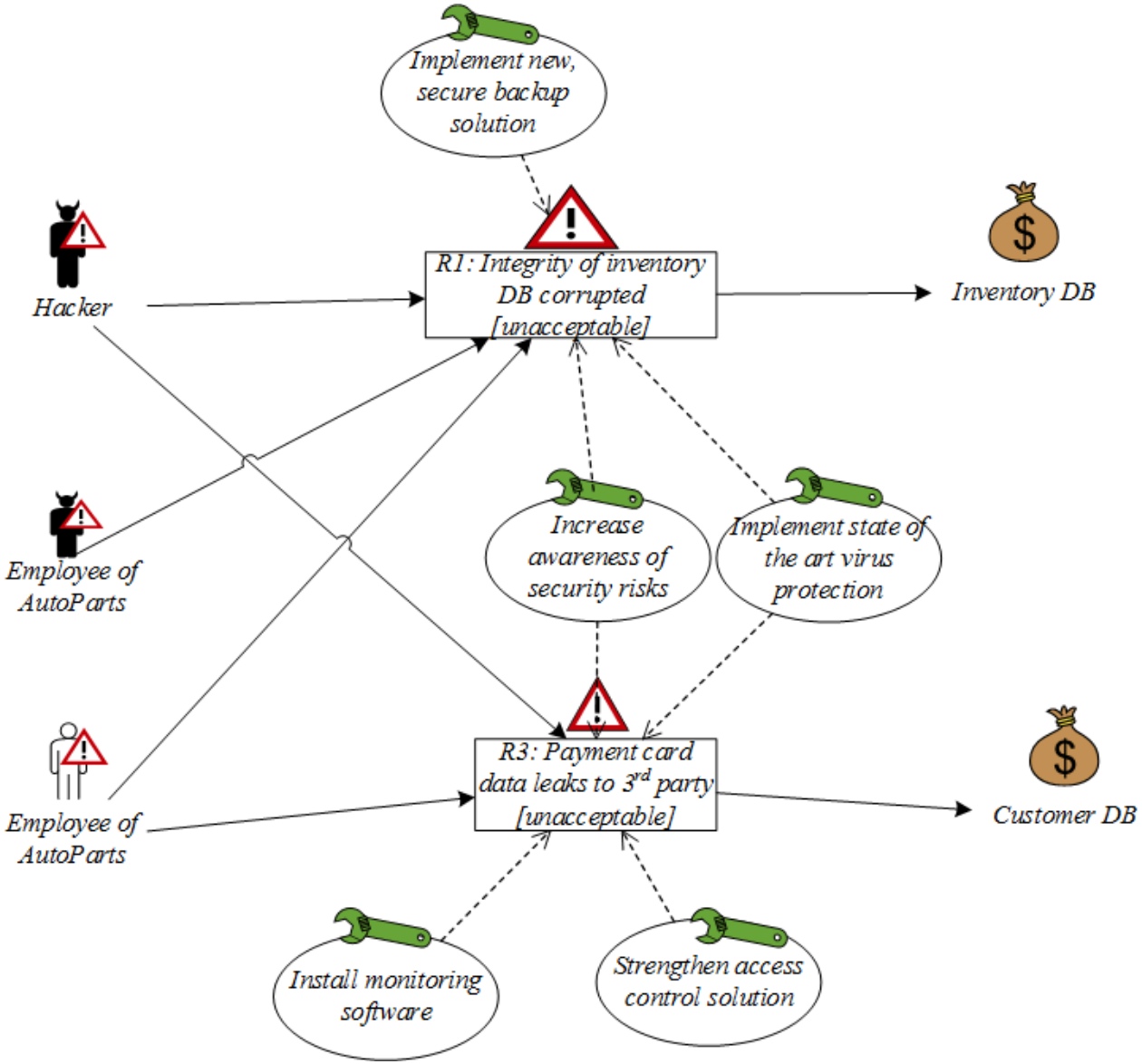
Example: Treatment Diagram



Example: Treatment Diagram



Example: Treatment Overview Diagram



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
T1: Implement new, secure backup solution	High	R1	R1: Unacceptable to Acceptable	No
T2: Increase awareness of security risks	Low	R1	R1: Unacceptable to Monitor	Yes
		R3	R3: Unacceptable to Acceptable	
T3: Implement state of the art virus protection	Low	R1	R1: Unacceptable to Monitor	Yes
		R3	R3: Unacceptable to Monitor	
T4: Install monitoring software	Medium	R3	R3: Unacceptable to Acceptable	Yes
T5: Strengthen access control solution	High	R3	R3: Unacceptable to Monitor	No

Example: Treatment Evaluation

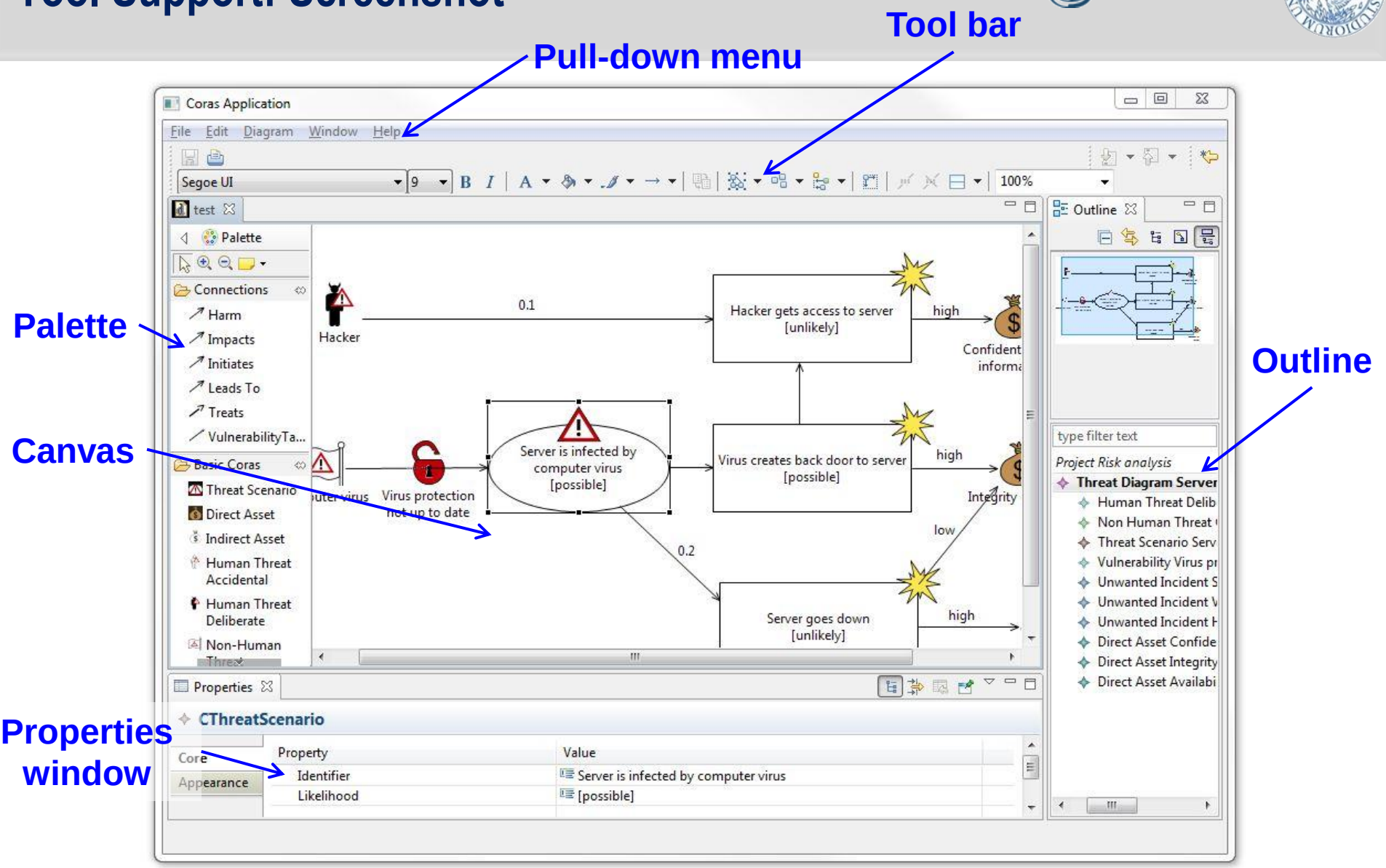
Final recommendations to customer

Treatment	Cost	Risk	Risk reduction	Select to implement
secure backup solution			to Acceptable	No
T2: Increase awareness of security risks	Low	R1	R1: Unacceptable to Monitor	Yes
		R3	R3: Unacceptable to Acceptable	
T3: Implement state of the art virus protection	Low	R1	R1: Unacceptable to Monitor	Yes
		R3	R3: Unacceptable to Monitor	
T4: Install monitoring software	Medium	R3	R3: Unacceptable to Acceptable	Yes
T5: Strengthen access control solution	High	R3	R3: Unacceptable to Monitor	No

Tool Support and Demo

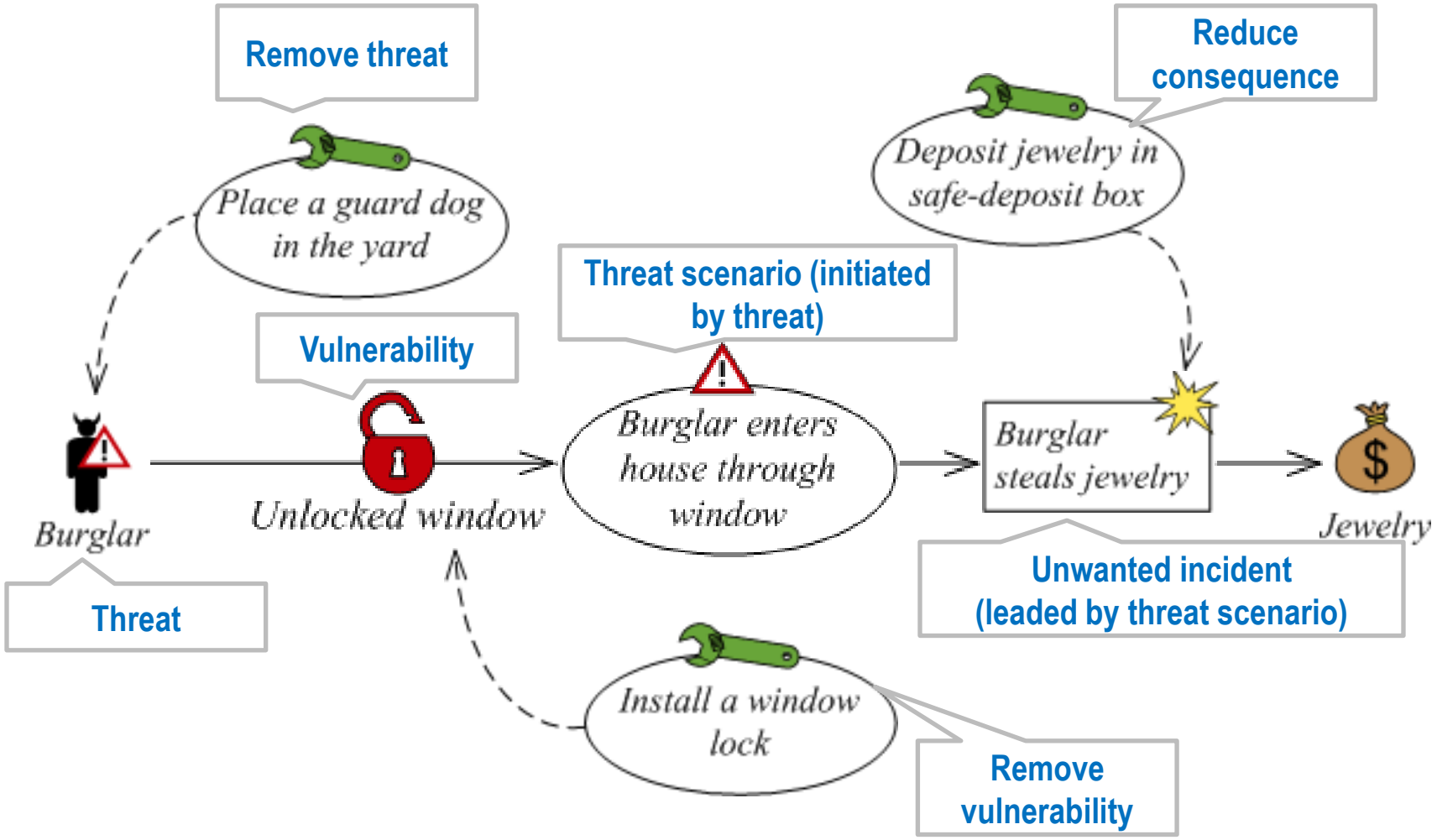
- The CORAS tool is a diagram editor
- Support for making all kinds of CORAS diagrams
- Design for on-the-fly modeling during structured brainstorming at analysis workshops
- Ensures syntactically correct diagrams
- Used during all steps of the risk analysis
  - Input to the various tasks
  - Gathering and structuring of information during the tasks
  - Documentation of analysis results
- Available for download: http://coras.sourceforge.net/

Tool Support: Screenshot



Summary

- **CORAS risk model in a nutshell**



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 a well-established and precisely defined conceptual framework
- Based on internationally established standards

- Book: http://www.springer.com/computer/swe/book/978-3-642-12322-1
- CORAS tool demo: http://coras.sourceforge.net/coras-tool-demo.htm
- Download:
  - Tool:http://coras.sourceforge.net/downloads.html (CORAS editor v1.1)
  - **Microsoft Visio stencil for the CORAS Language: http://coras.sourceforge.net/downloads.html (see CORAS_visio_stencil_20060714.vss) (recommended)**

Credits

- M.Lund, B.Solhaug, K.Stolen, Model-Driven Risk Analysis: The CORAS approach. Springer 2011.
- Heidi E.I.Dahl, ESSCaSS 2008, NODES Tutorial.
- Atle Refsdal, ERISE 2011 tutorial.

From Treatments to Security Requirements

Terms and Concepts (1)

- **Security goal:**
  - is an expression of the need to protect an asset from harm

- **Security requirements:**
  - are functional or non-functional requirements that need to be satisfied in order to achieve the security goals on a system

Terms and Concepts (2)

- **Security control:**
  - is safeguard or countermeasure to avoid, counteract or minimize the risks on the assets
  - By implementing the security controls, the security requirements can be satisfied, and hence, also the security goals

- **Types of security controls:**
  - Physical controls:
    - Example: guard dog, fences, doors, locks, fire extinguishers,…
  - Procedure controls
    - Example: security awareness and training, incident response processes, management oversight…
  - Technical controls:
    - Example: access controls, antivirus software, firewall, user authentication …
  - Legal and regulatory or compliance controls:
    - Example: privacy laws, policies and clauses

- **The treatments in CORAS can be considered as security controls**

From Risks to Security goals

- **Identify security goals from (unacceptable) risks**
- **Example**

Risks	Asset that is harmed	Security Goals
R1: Integrity of inventory DB corrupted	Inventory DB	SG1: The inventory DB needs to be properly protected from flaw manipulations
R3: Payment card data leaked to 3rd party	Customer DB	SG2: the customer DB needs to be properly protected from the leakage

- *Note: the number of security goals may not need to be identical with the number of risks (i.e., you can have 5 risks, and 3 security goals, or vice versa)*

From Treatments to Security Requirements (1)

- Identify security requirements from treatments.
- These security requirements can be satisfied by implementing proper treatments
- The security goals are hence achieved when the security requirements are satisfied

From Treatments to Security Requirements (2)

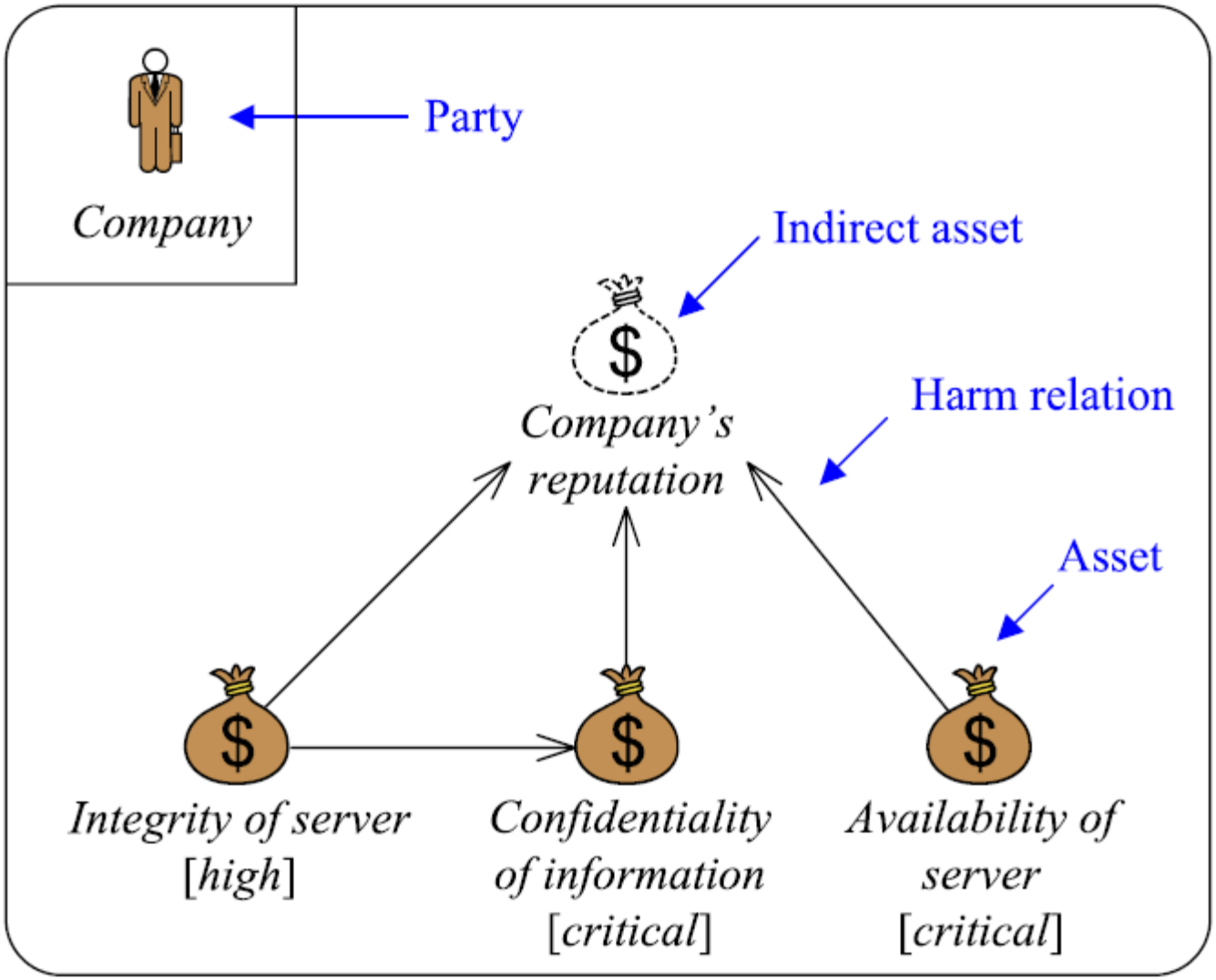
- **Example (for all treatments, also including the ones which are finally not recommended to the customer):**

Treatments (Security controls)	Security Requirements	Security Goals
T1:Implement new, secure backup solution	SR1: The Online Store system should have the backup mechanism for any database	SG1
T2: Increase awareness of security risks	SR2: The employee of Online Store should have a proper background, in a security sense, relating to their tasks in the company	SG1, SG2
T3: implement state of the art virus protection	SR3: The Online Store system should be able to detect any malicious code or malicious software	SG1, SG2
T4: install monitoring software	SR4: The database and web application of Online Store should be monitored and scanned to ensure no suspicious activity, tampering or malicious software	SG2
T5: strengthen access control solution	SR5: The Online Store system should have a proper access control mechanism to ensure for authentication and authorization	SG2

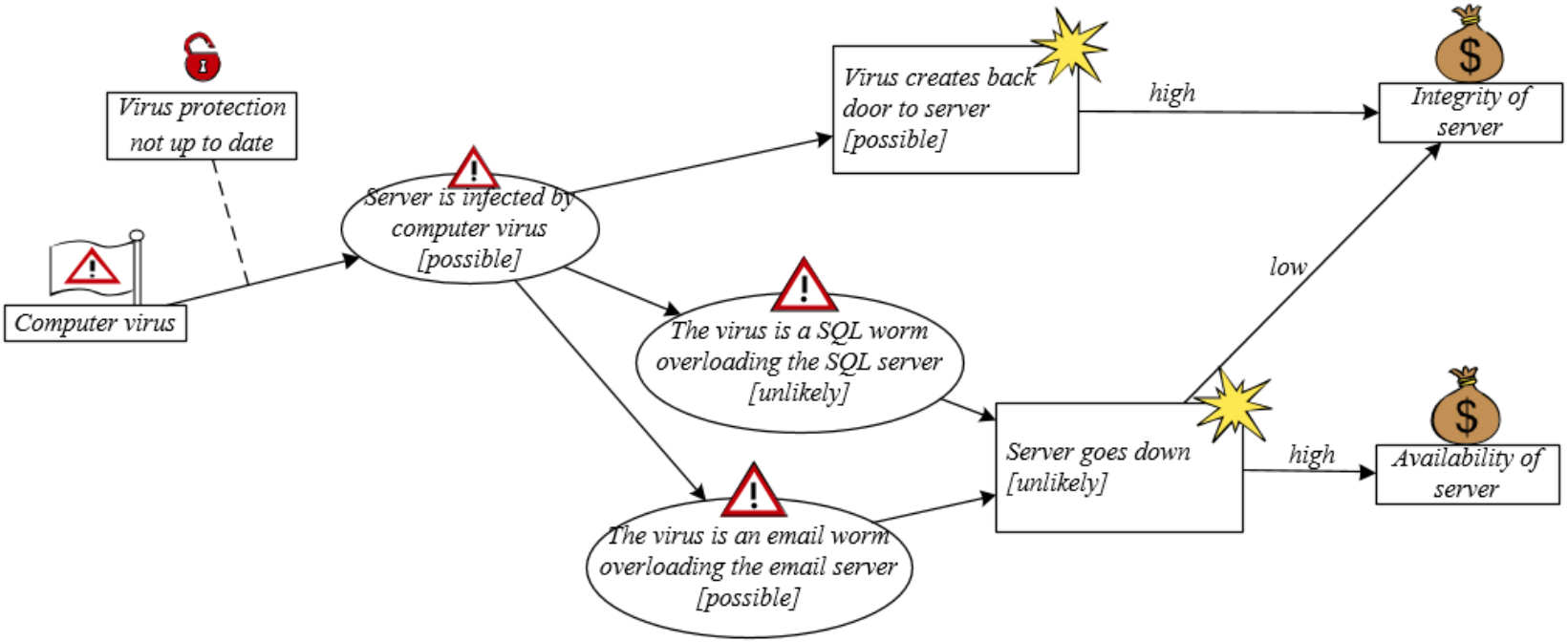
- *Note: the number of security requirements may not need to be identical with the number of treatments (i.e., you can have more security requirements than treatments, or vice versa.)*
  - *One treatment can be implemented to satisfy more than one security requirement(s)*
  - *One security requirement can be satisfied by implementing more than one treatment(s)*

More examples on CORAS diagrams

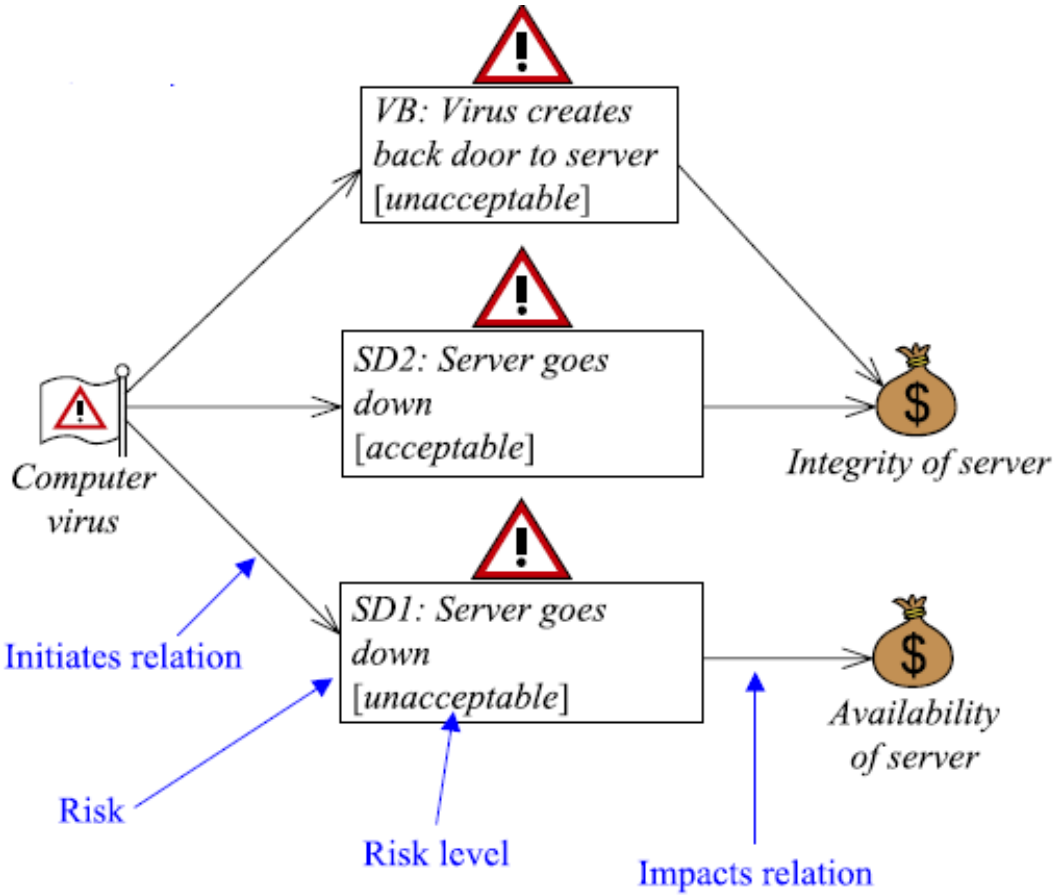
- **Asset Diagram**



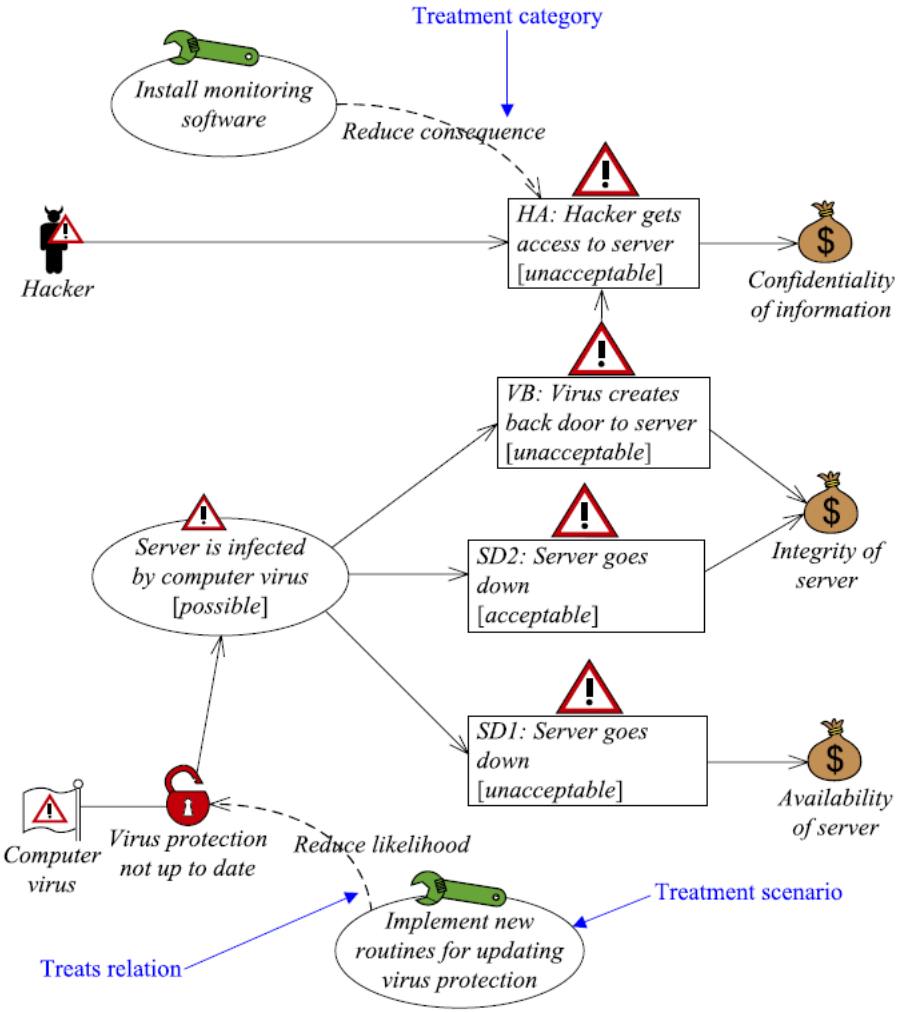
- **Threat Diagram**



- **Risk Diagram**

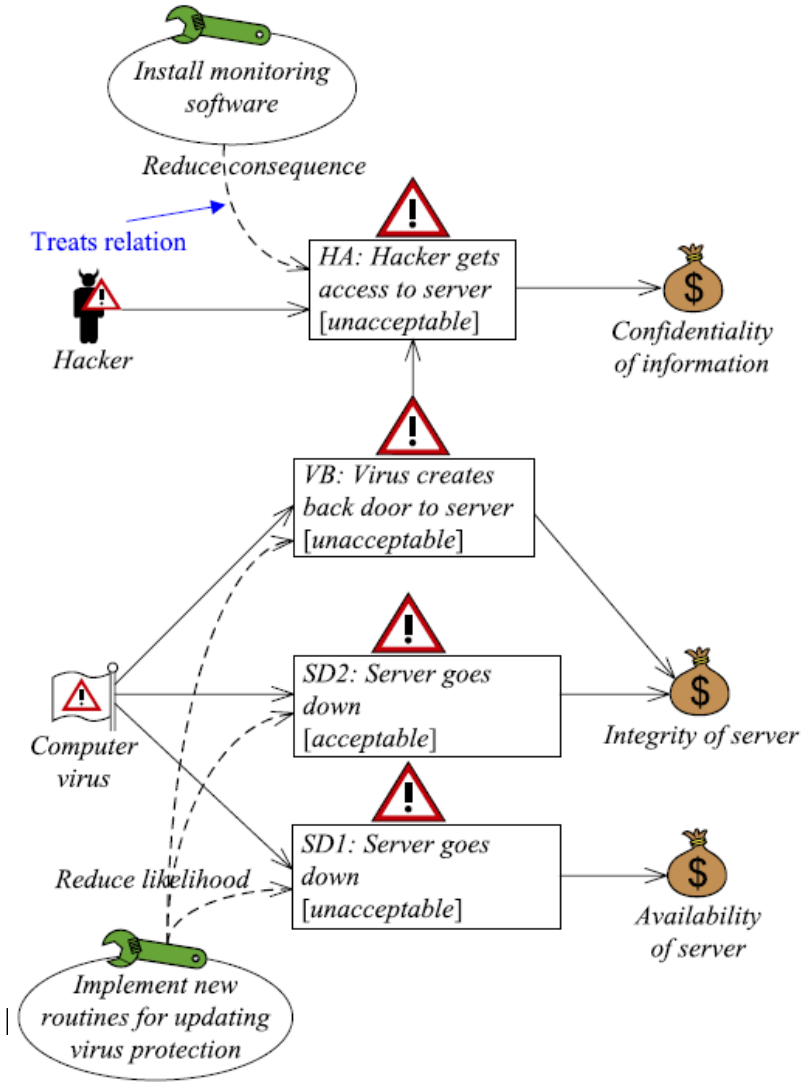


- **Treatment Diagram**

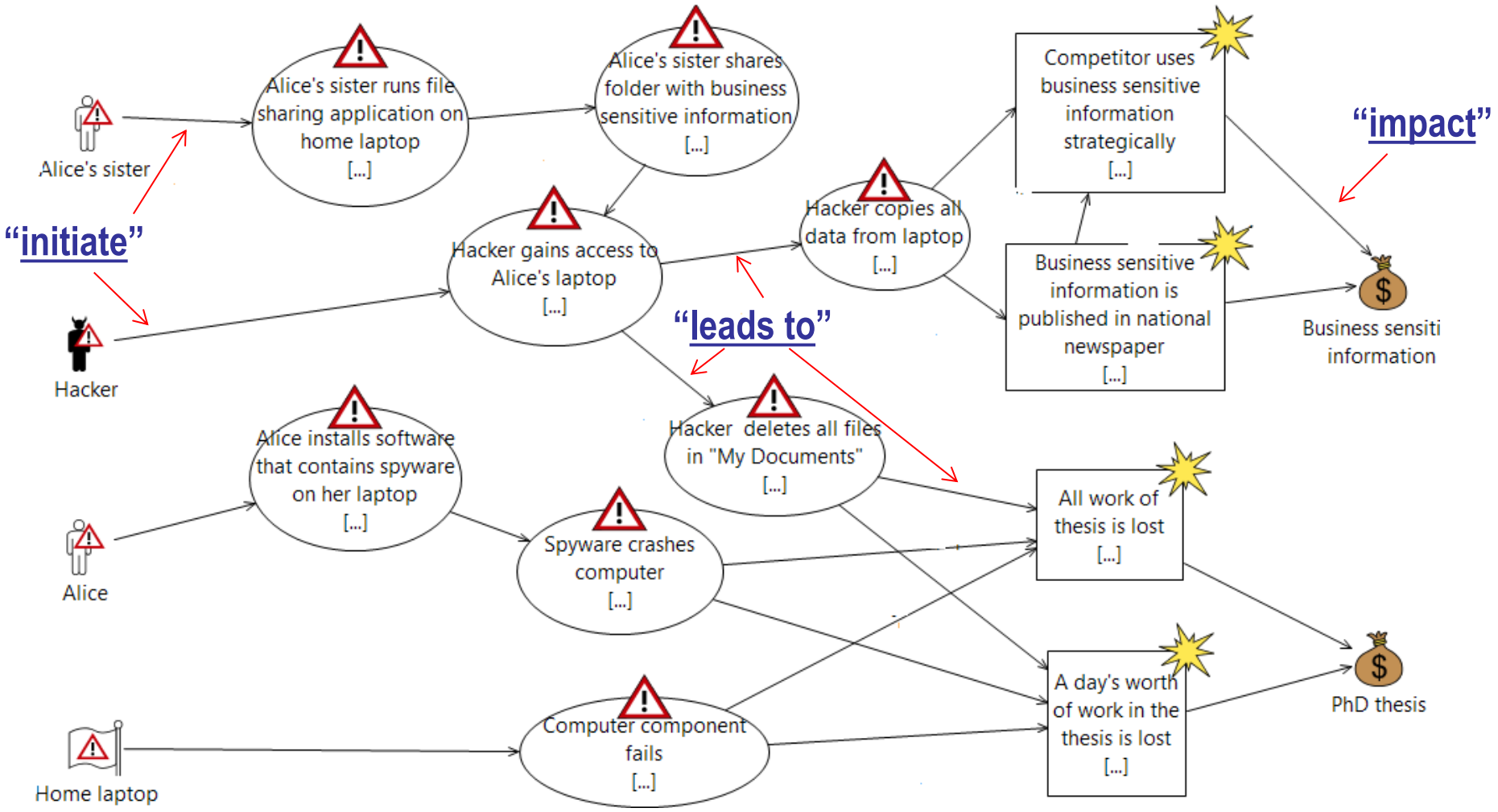


Note: it may not be required to specify the treatment category in this diagram

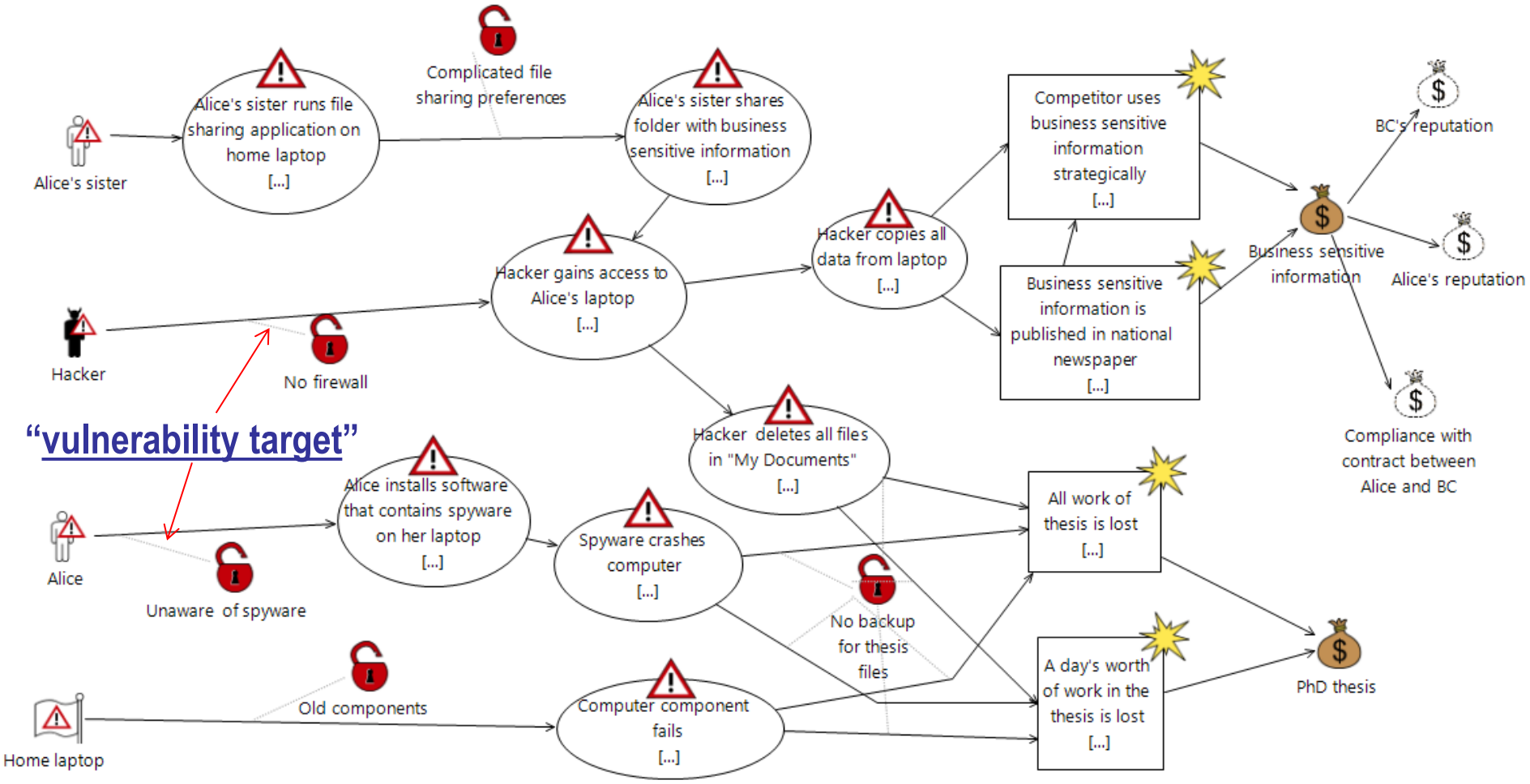
- **Treatment Overview Diagram**



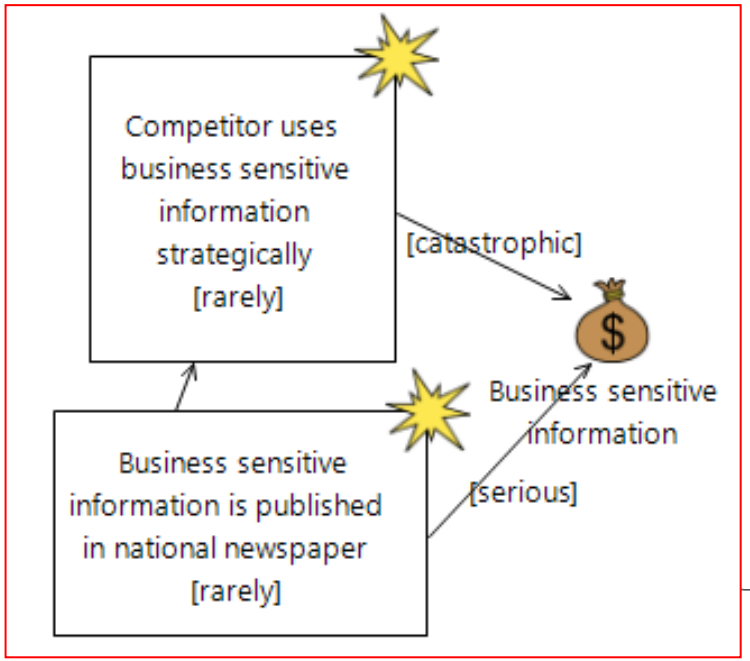
More Example

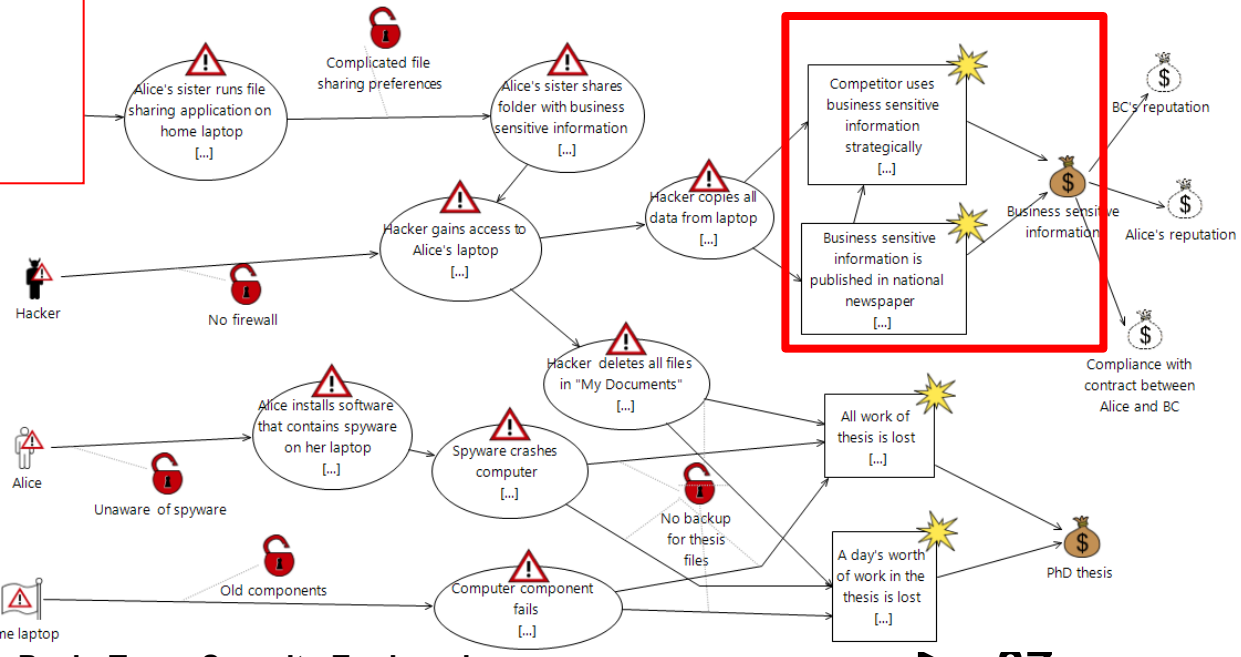


More example

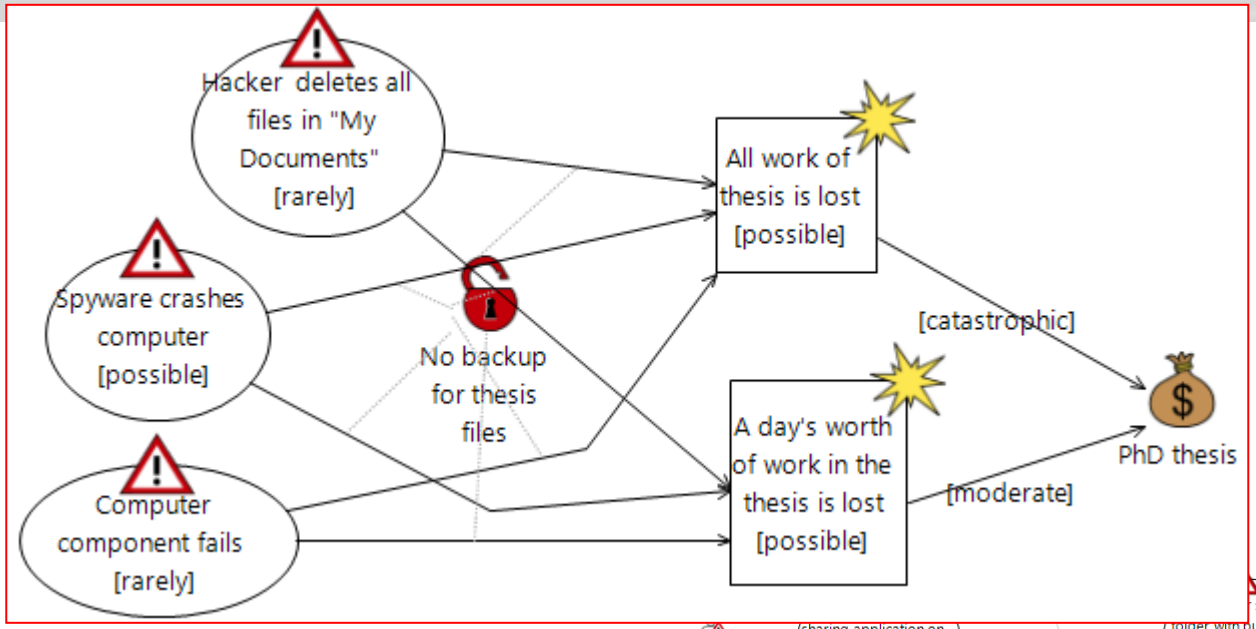


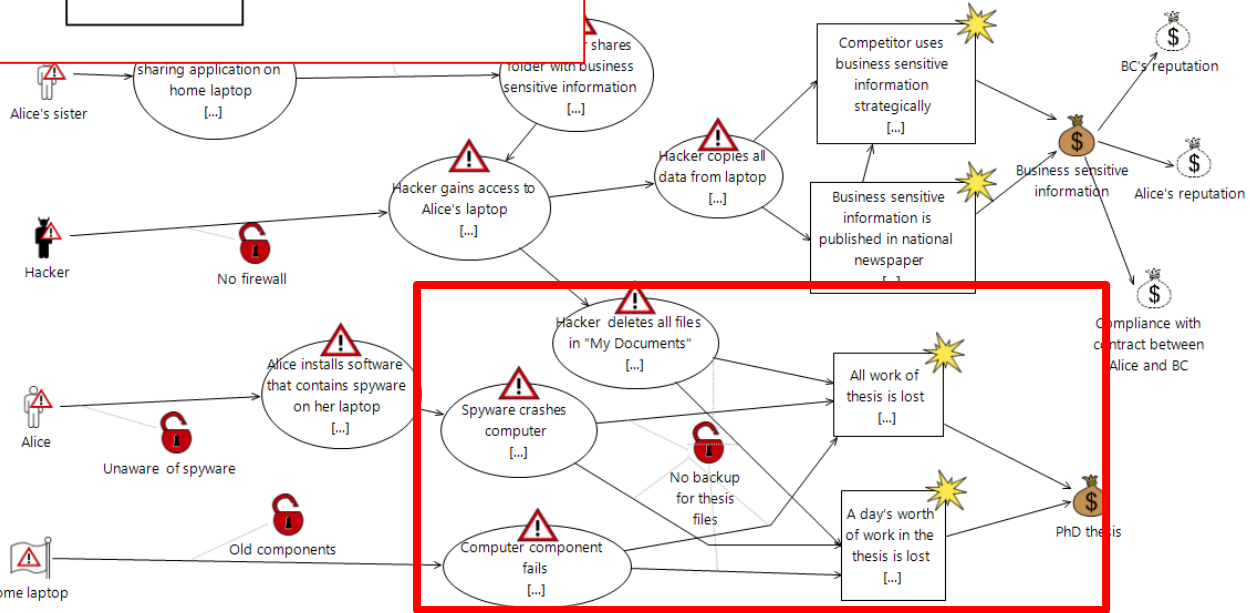
More example: Assign Likelihood and Consequence





More example: Assign Likelihood and Consequence





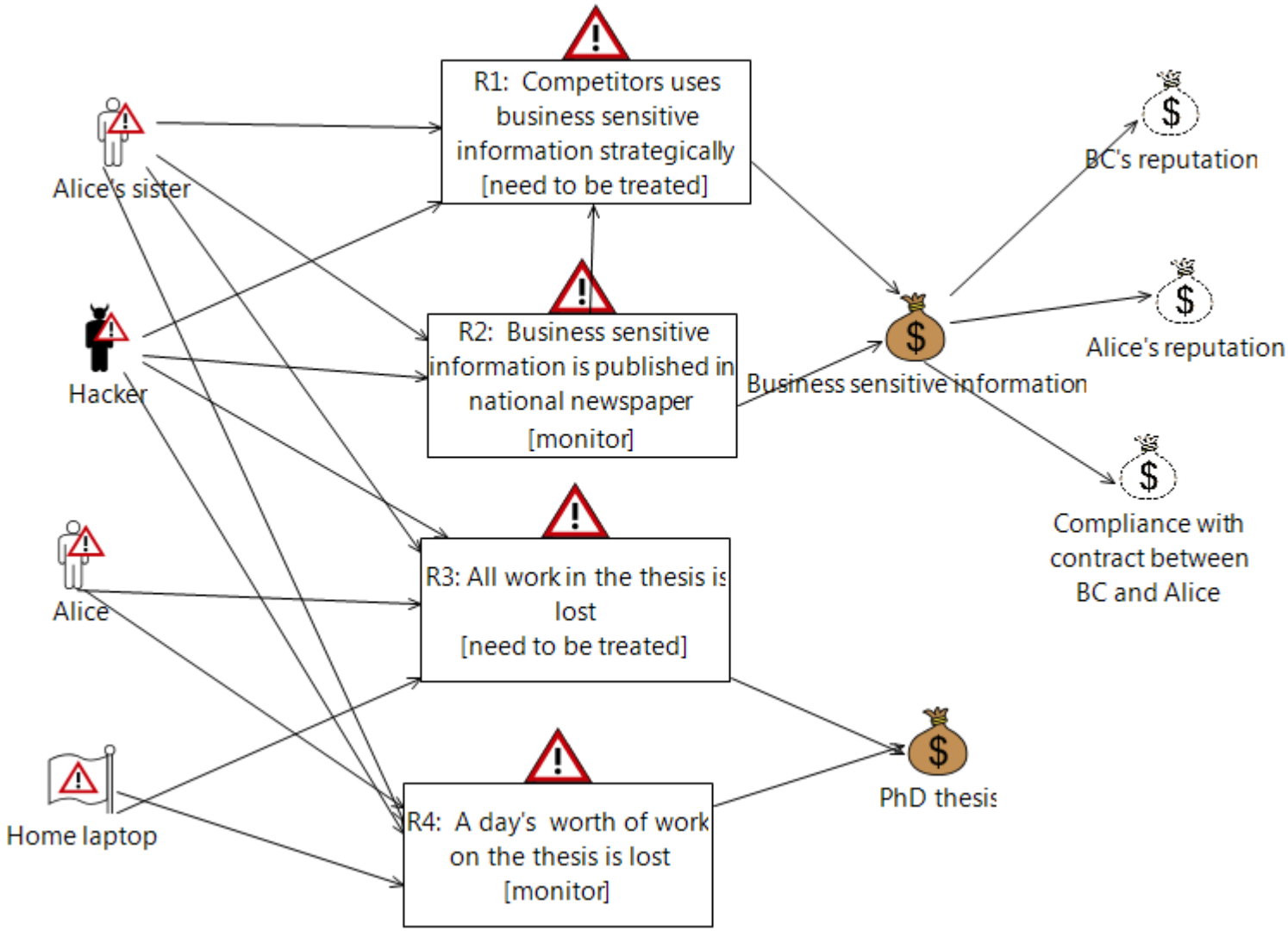
More example: completed Risk Matrix

Risk Matrix (PhD thesis)					
Consequence/ Likelihood	**Insignificant**	**Minor**	**Moderate**	**Serious**	**Catastrophic**
Rarely					
Unlikely					
Possible			A day's worth of work on the thesis is lost		All work on thesis is lost
Likely					
Certain					

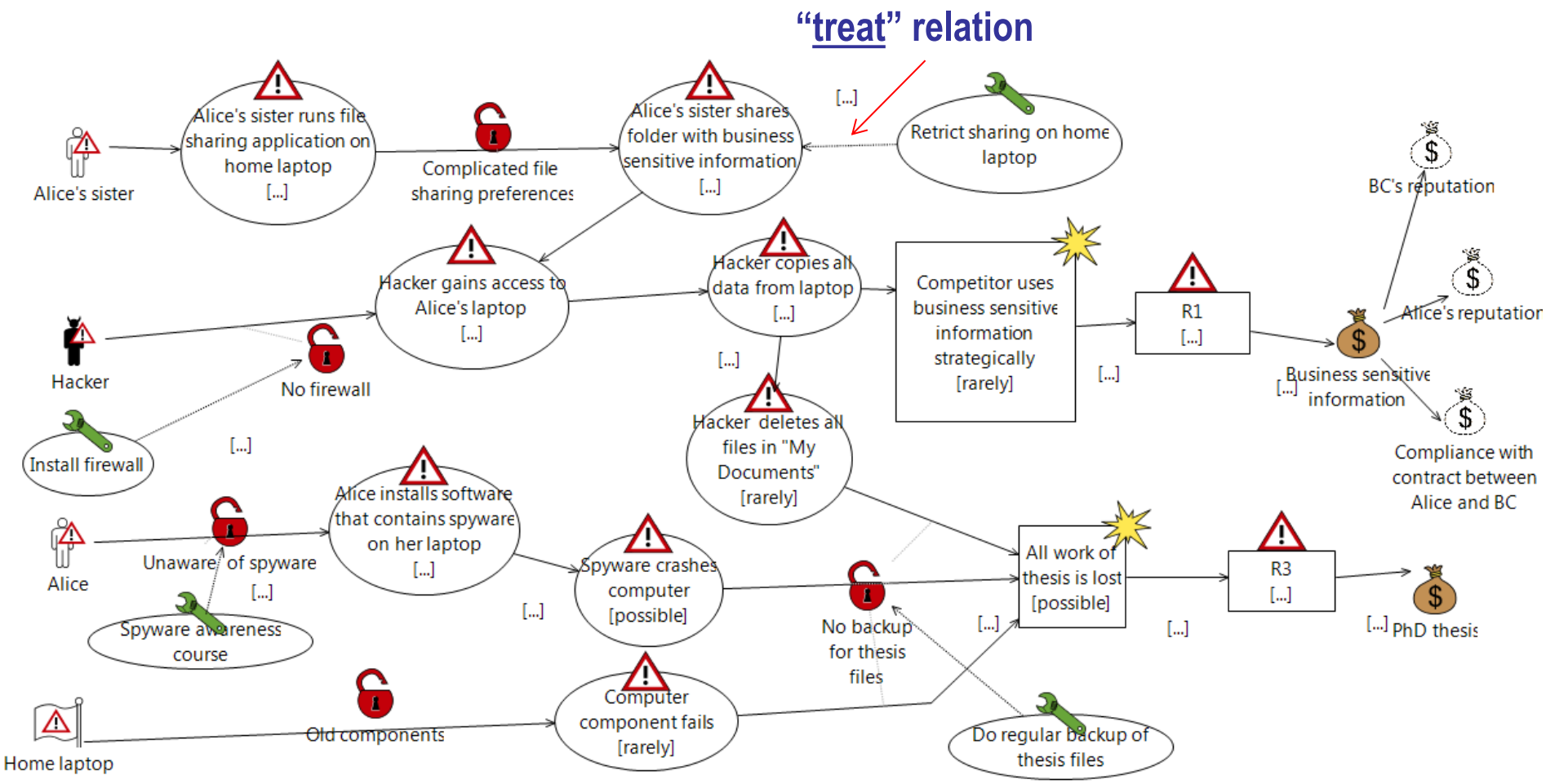
More example: completed Risk Matrix

Risk Matrix (Business sensitive information)					
Consequence/ Likelihood	**Insignificant**	**Minor**	**Moderate**	**Serious**	**Catastrophic**
Rarely				Business sensitive information is published in national newspaper	Competitors uses Business sensitive information strategically
Unlikely					
Possible					
Likely					
Certain					

More example: Risk diagram



More example: Treatment Diagram



More example: Treatment Overview Diagram