



NESSOS E-RISE Challenge 2013

Model-Driven Risk Analysis: The CORAS Approach

Le Minh Sang Tran

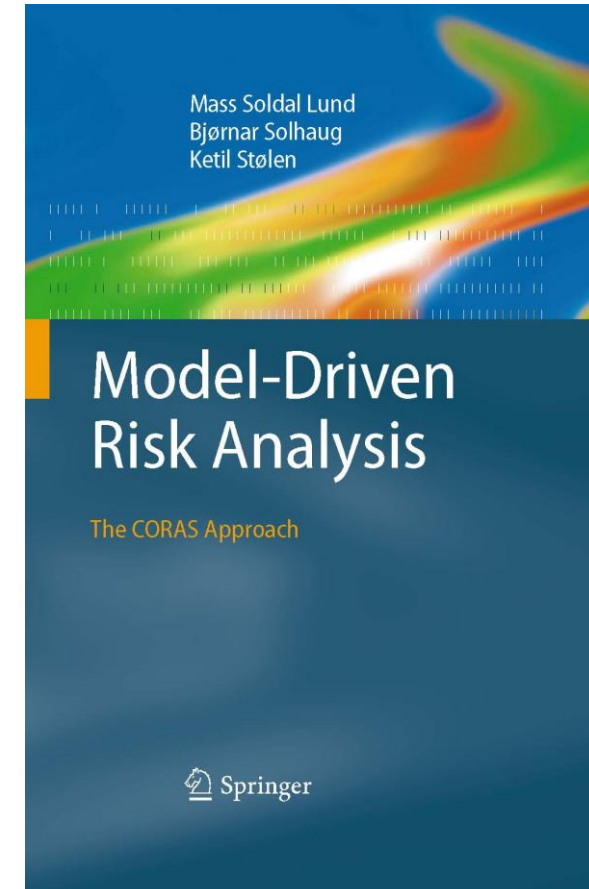
`tran@disi.unitn.it`

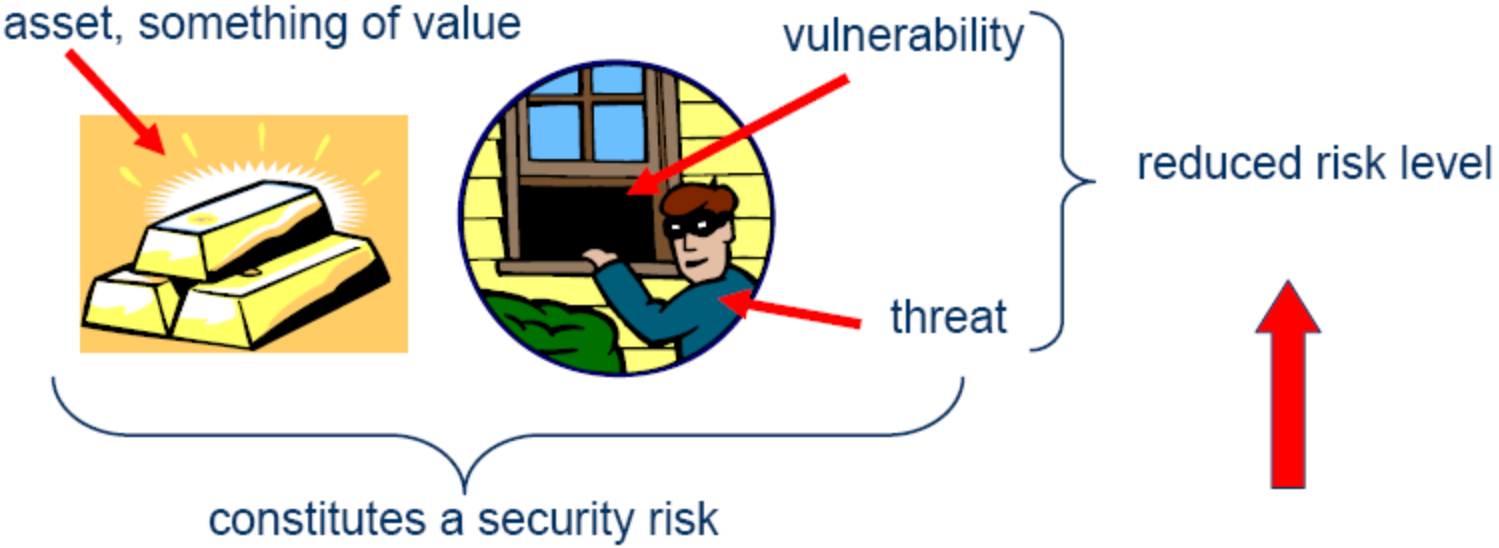


**Università degli
Studi di Trento**

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

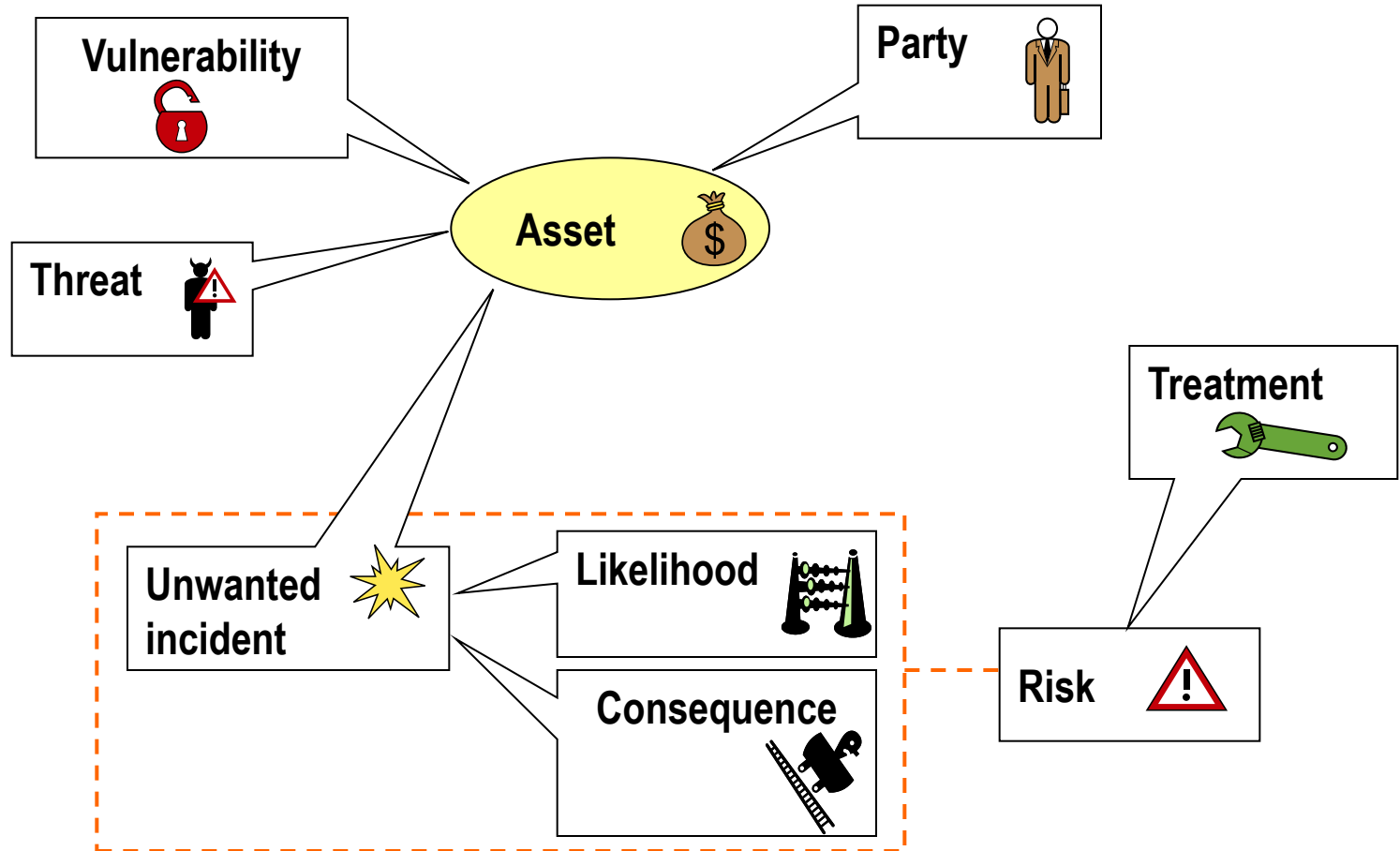
- **The CORAS approach:**
 - A language for risk modeling
 - A tool to support the risk analysis process
 - A method for risk analysis
 - A stepwise, structured and systematic process
 - Asset-driven
 - Concrete tasks with practical guidelines
 - Model-driven
 - Models as basis for and input to analysis 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>



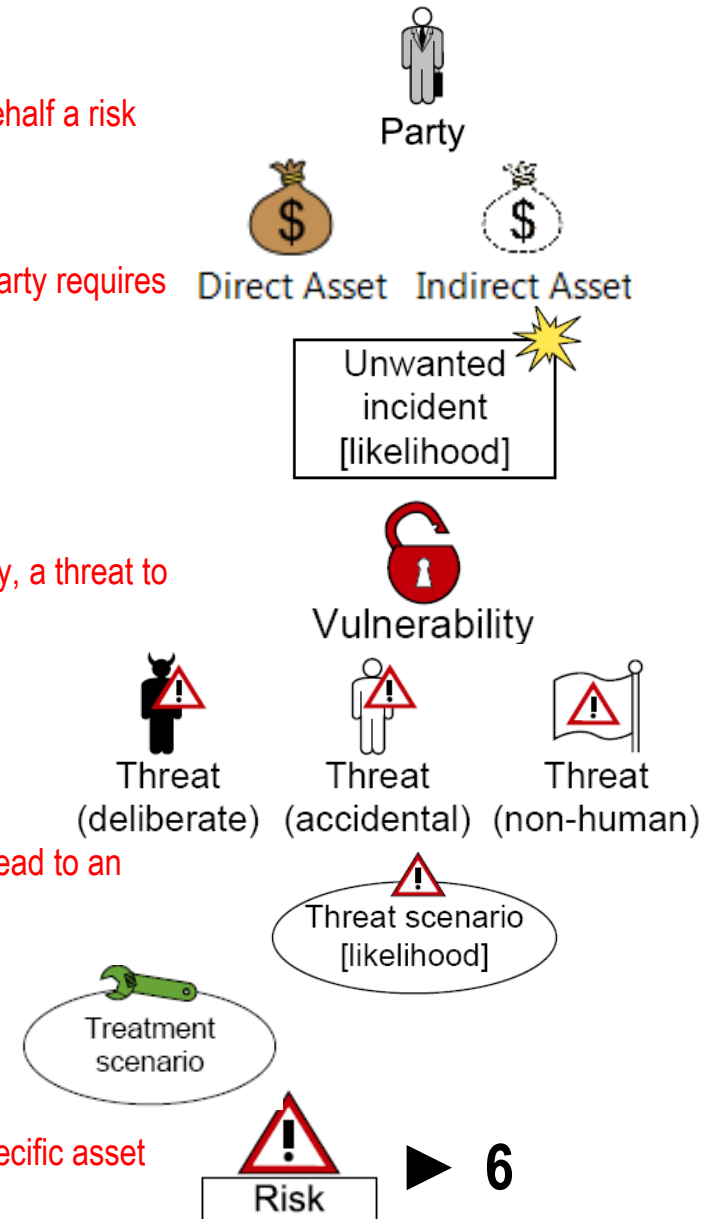


we need to introduce security mechanisms



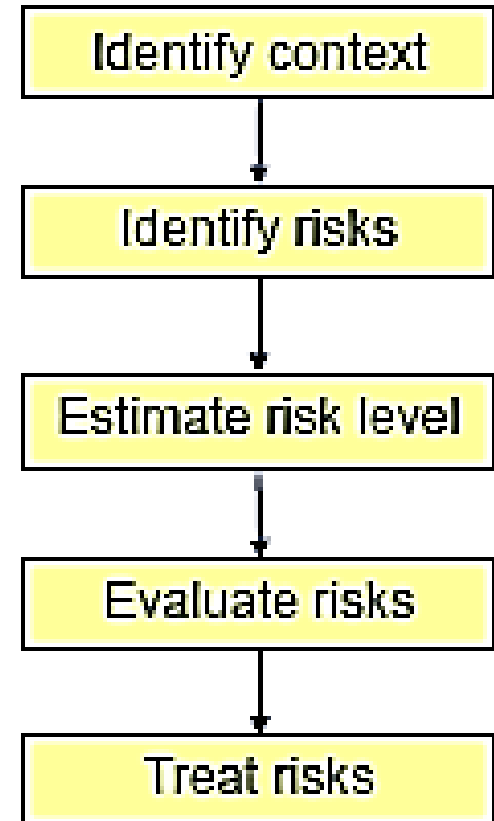


- **Party:**
 - An organization, company, person, group or other body on whose behalf a risk analysis is conducted
- **Asset:**
 - Something to which a party assigns value and hence for which the party requires protection
- **Unwanted incident:**
 - An event that harms or reduces the value of an asset
- **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

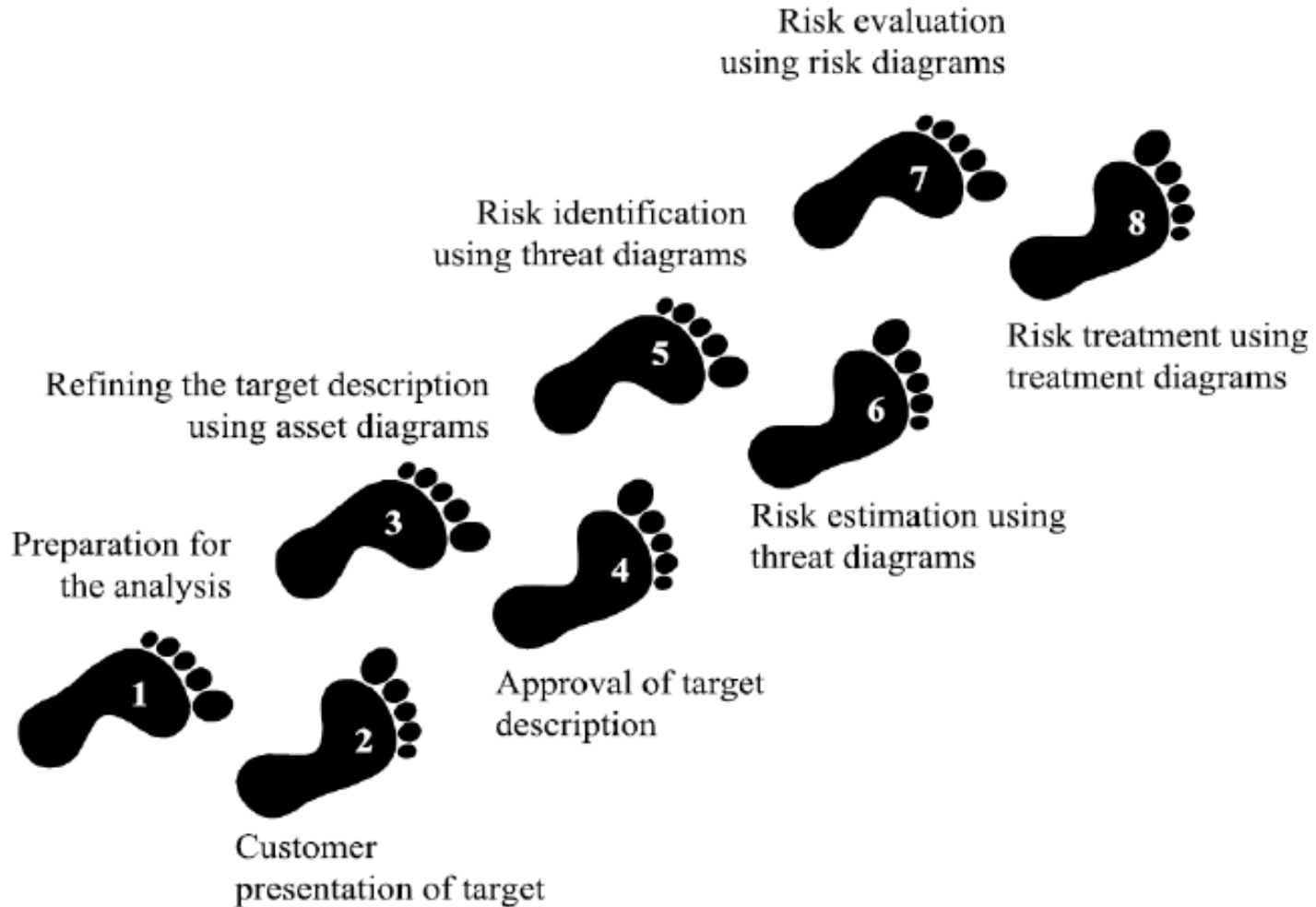


- **The CORAS language consists of five kinds of diagrams**
 - Asset diagrams
 - Threat diagrams
 - Risk diagrams
 - Treatment diagrams
 - Treatment Overview diagrams
- **Each kind of diagram supports specific steps of the risk analysis process**

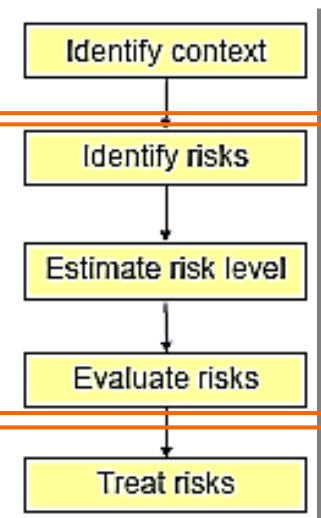
- Risk management process based on *ISO 31000: Risk Management – Principles and Guidelines*
- Provides *processes and guidelines* for risk analysis



The eight steps of a CORAS risk analysis



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



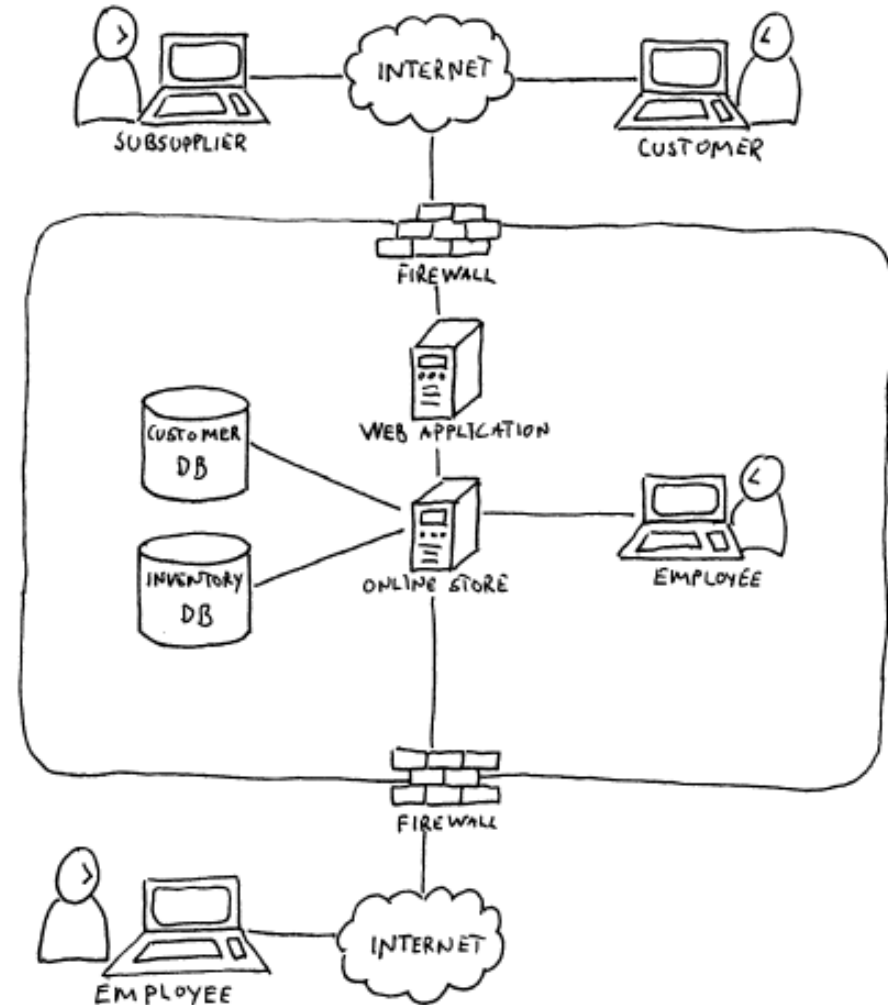
- **Objective: do the necessary initial preparations prior to the actual startup of the analysis**
- **Tasks:**
 - Contact the customer for the case study
 - Roughly setting the scope and focus

- 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.

- **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

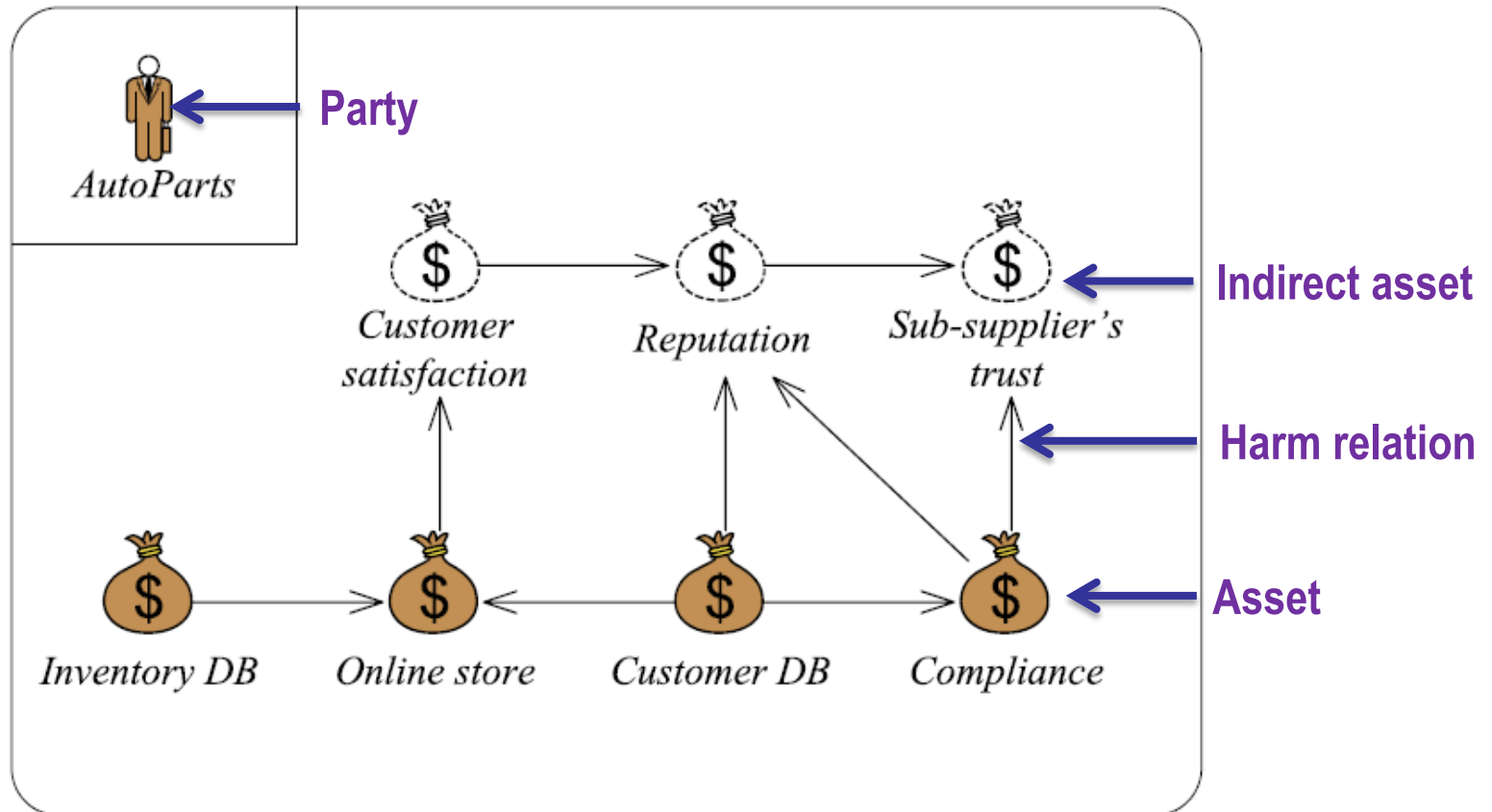
- **Objective:** ensure a common and more precise understanding of the target analysis, including its scope, focus, and main assets
- **Task:**
 - The target is understood by the risk analysts
 - Identify the parties and assets
 - Conduct a high-level analysis:
 - The first threats, vulnerabilities,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

- Identify involving parties
- Identify assets of each party intends to protect:
 - The “THINGS” that are valuable
- Notions to be used in Asset Diagram



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

Example: Asset diagram



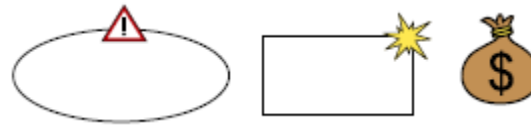
- **Relations between assets**

- Harm in one asset might harm also other assets.

- Preliminary list of Unwanted Incidents



Who/ What is the cause?



How? What may happen?
What does it harm?



What makes this possible?

...

...

.....

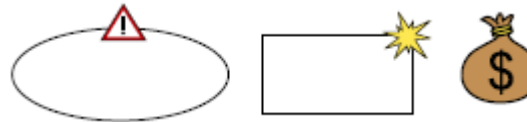
.....

.....

.....



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

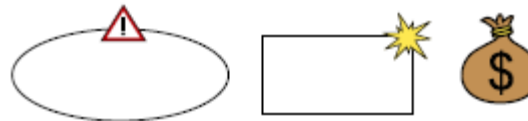
DoS attack causes online store to go down

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

- **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

- **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

- **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
...

- **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

- **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>

- **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

- 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

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

Risk Function (Inventory DB)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Serious	Catastrophic
Rare	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Unlikely	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Possible	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Likely	Acceptable	Monitor	Monitor	Need to be treated	Need to be treated
Certain	Acceptable	Monitor	Need to be treated	Need to be treated	Need to be treated



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

Risk Function (Online Store)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Serious	Catastrophic
Rare	Acceptable	Acceptable	Monitor	Monitor	Need to be treated
Unlikely	Acceptable	Acceptable	Monitor	Monitor	Need to be treated
Possible	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Likely	Acceptable	Monitor	Monitor	Need to be treated	Need to be treated
Certain	Acceptable	Monitor	Need to be treated	Need to be treated	Need to be treated



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

Risk Function (Customer DB)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Serious	Catastrophic
Rare	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Unlikely	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Possible	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Likely	Acceptable	Monitor	Monitor	Need to be treated	Need to be treated
Certain	Acceptable	Monitor	Need to be treated	Need to be treated	Need to be treated



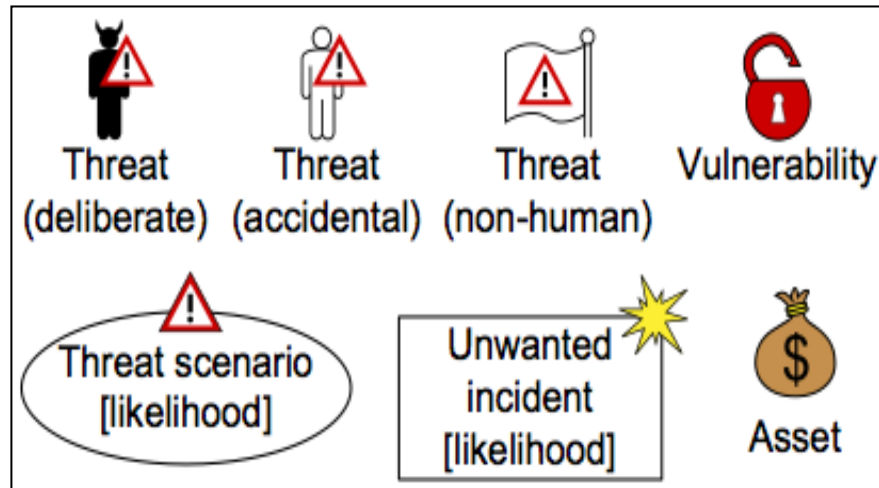
- Determine level of risk as a function of likelihood and consequence

Risk Function (Compliance)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Serious	Catastrophic
Rare	Acceptable	Acceptable	Monitor	Monitor	Monitor
Unlikely	Acceptable	Acceptable	Monitor	Monitor	Need to be treated
Possible	Acceptable	Acceptable	Monitor	Monitor	Need to be treated
Likely	Acceptable	Monitor	Monitor	Monitor	Need to be treated
Certain	Acceptable	Monitor	Monitor	Need to be treated	Need to be treated



- **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

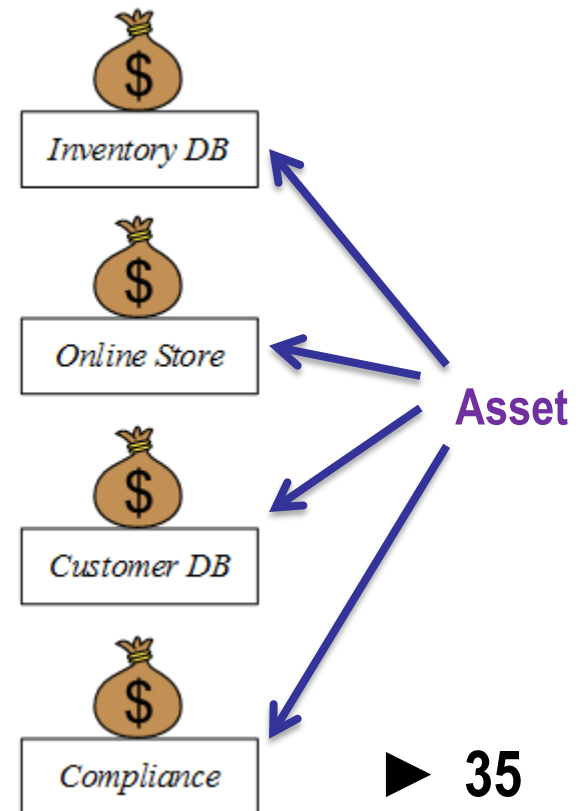
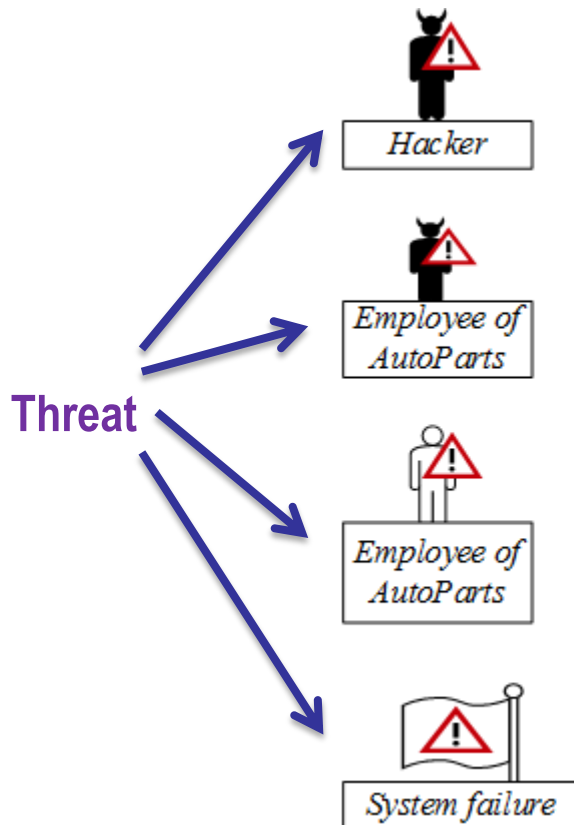
- Notions to be used in Threat Diagram



- Answer the question: “What are the threats?”

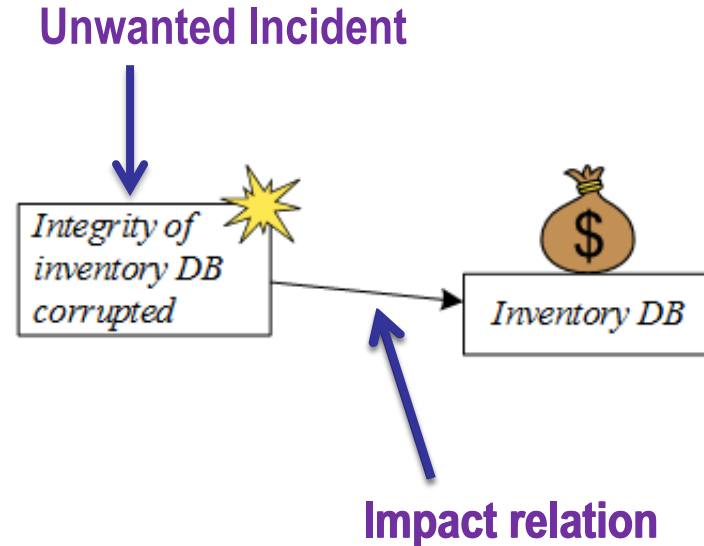
- Hints:

- “Accidental threat”: users/ roles inside the system
- Attackers from outside: “deliberate threat”

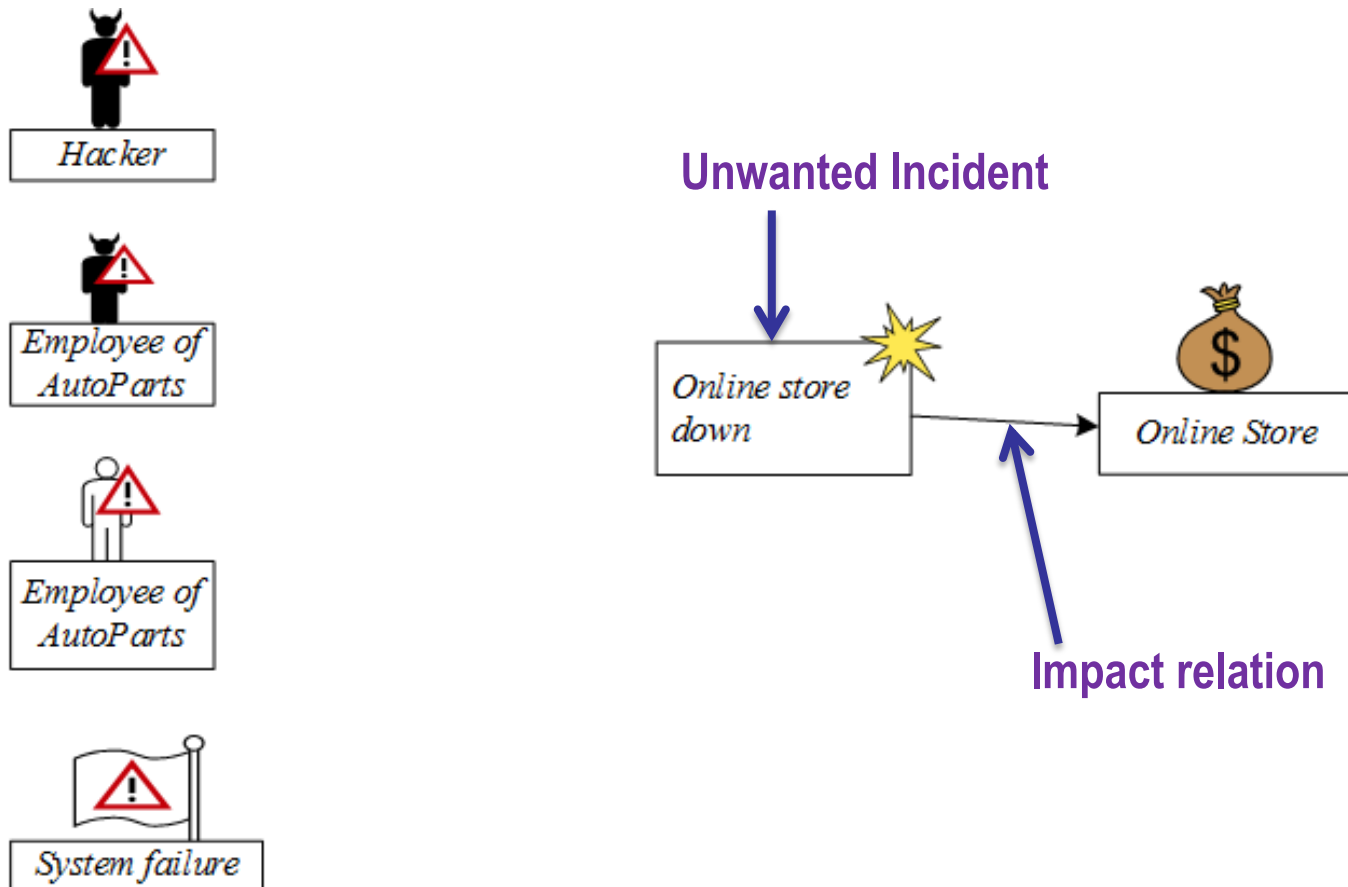


- Answer the question:

- What (unwanted incidents) do we fear will happen?

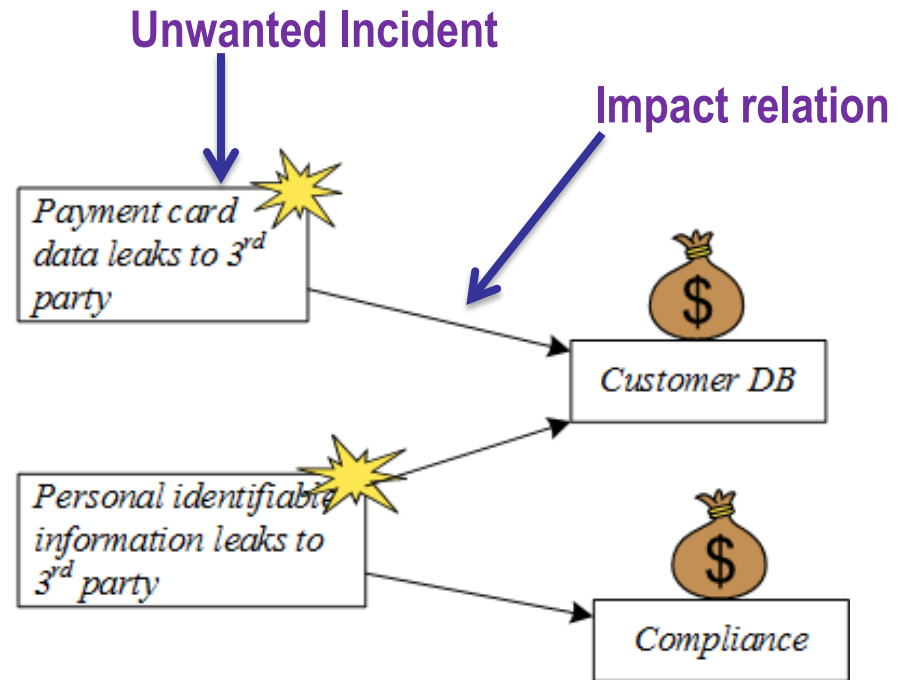
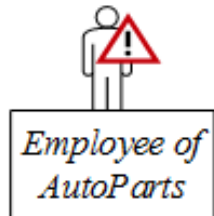


- Answer the question:
 - What (unwanted incidents) do we fear will happen?



- Answer the question:

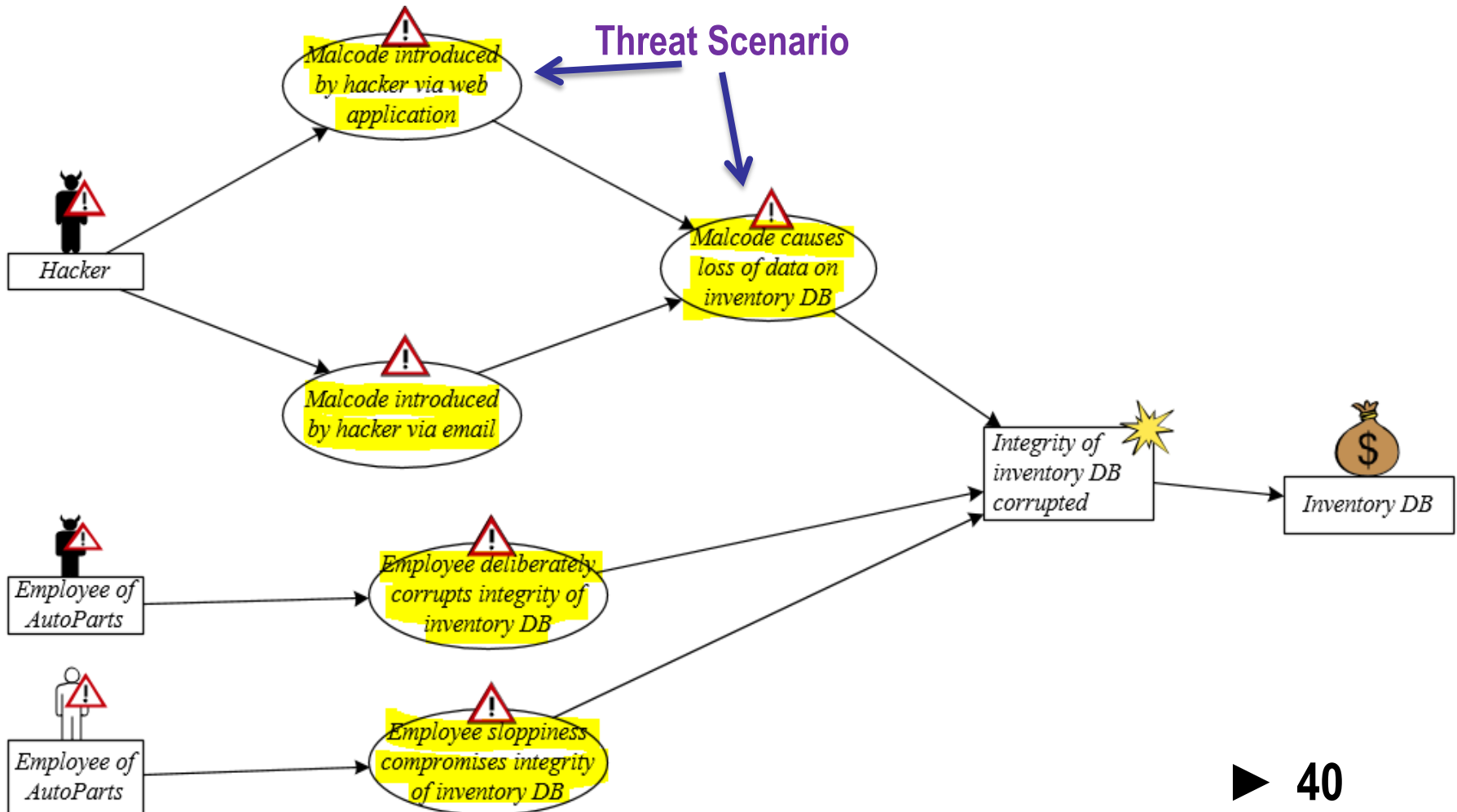
- What (unwanted incidents) do we fear will happen?



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

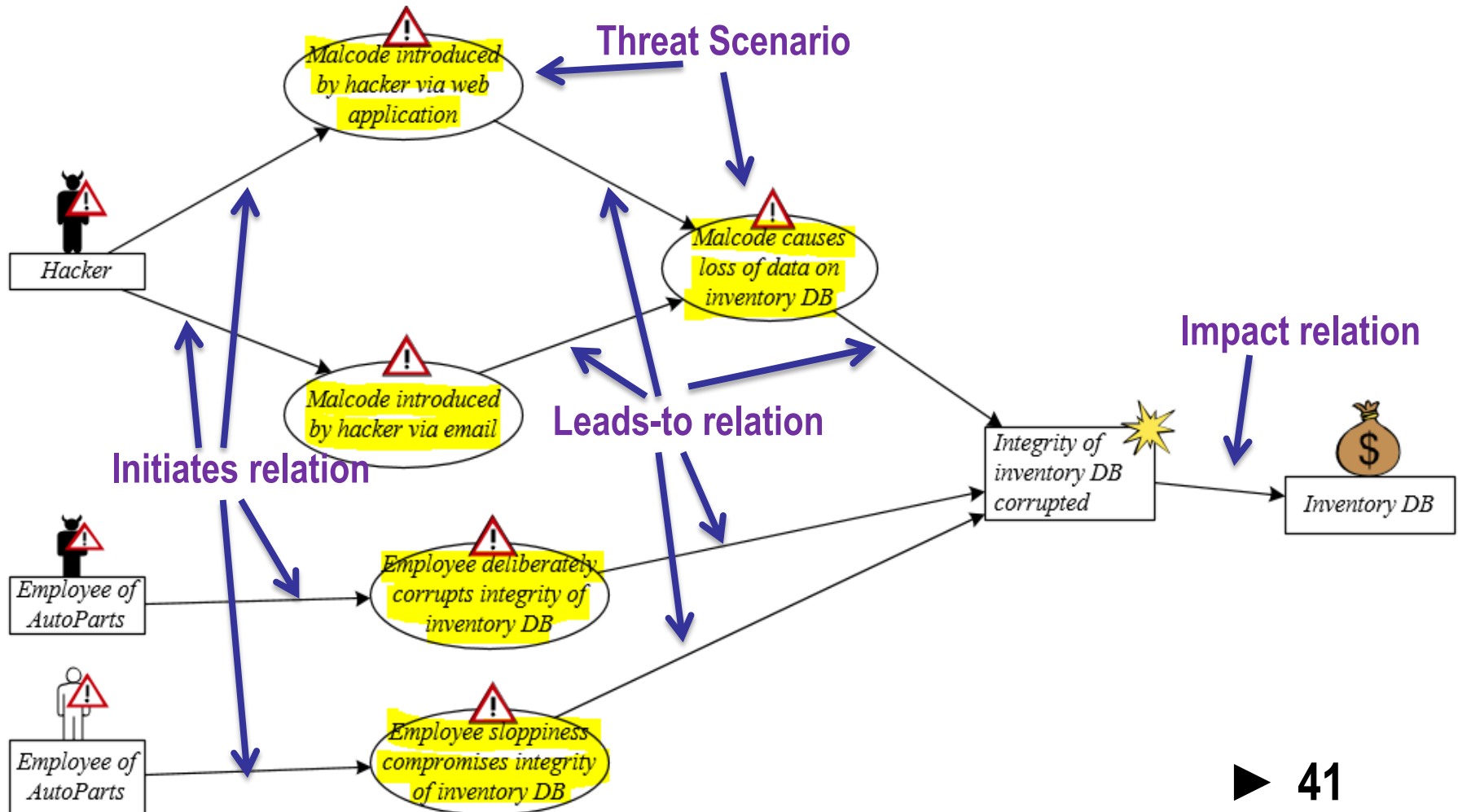
- Answer the question:

- How does it happen? It happens by which threat scenarios?



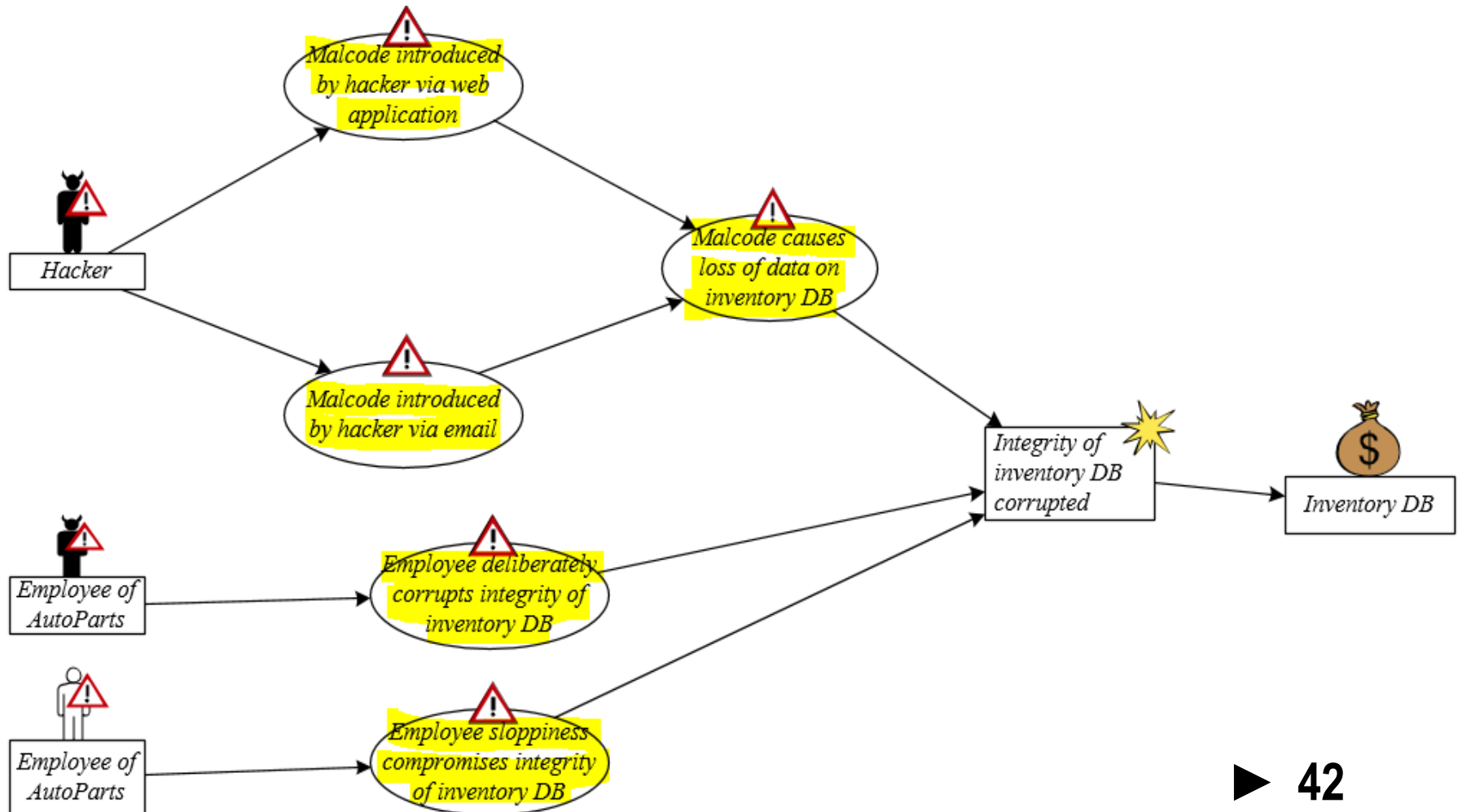
- Answer the question:

- How does it happen? It happens by which threat scenarios?



- Answer the question:

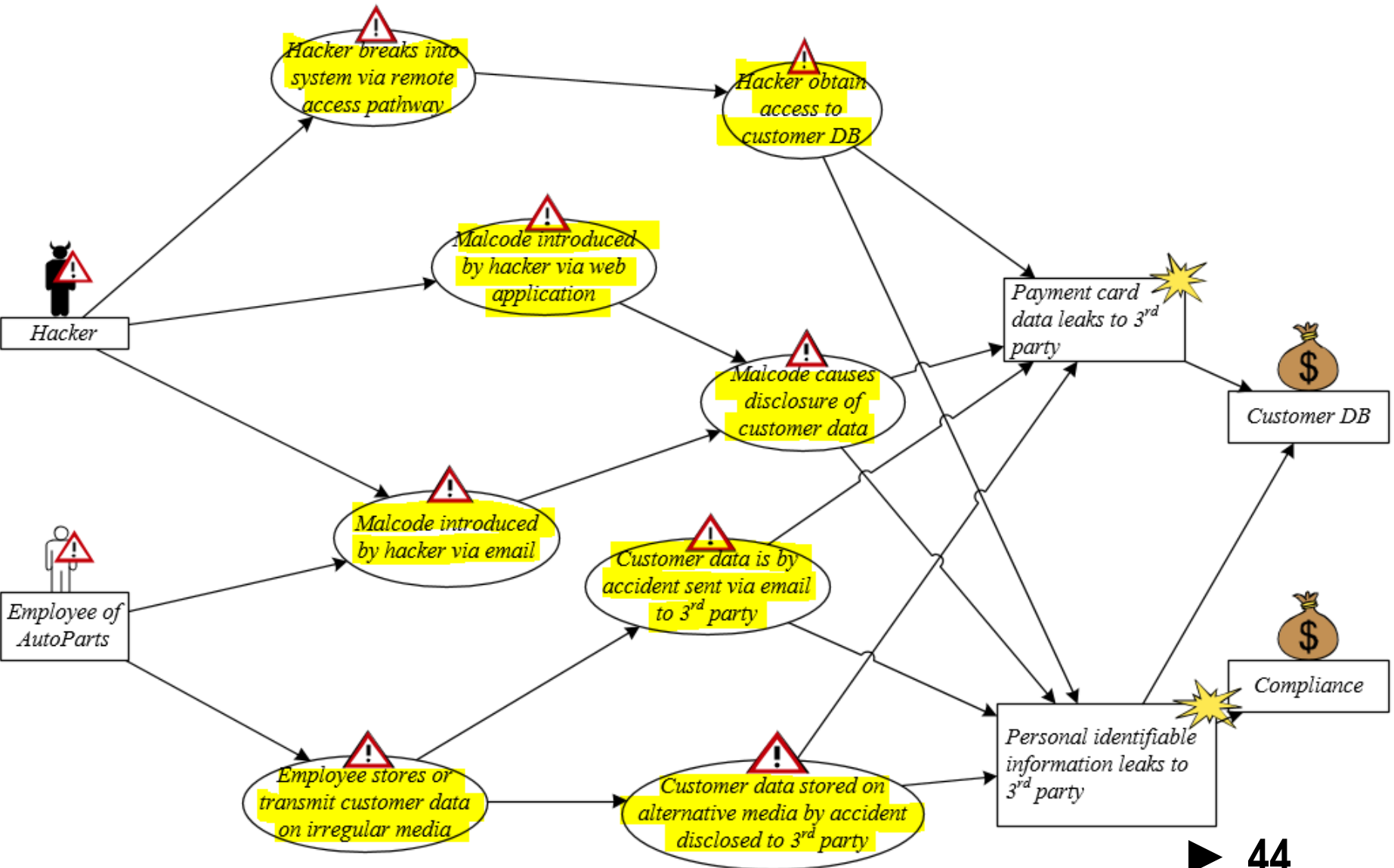
- How does it happen? It happens by which threat scenarios?



Step 5 - sub step 3: Identify Threat Scenarios



Step 5 - sub step 3: Identify Threat Scenarios

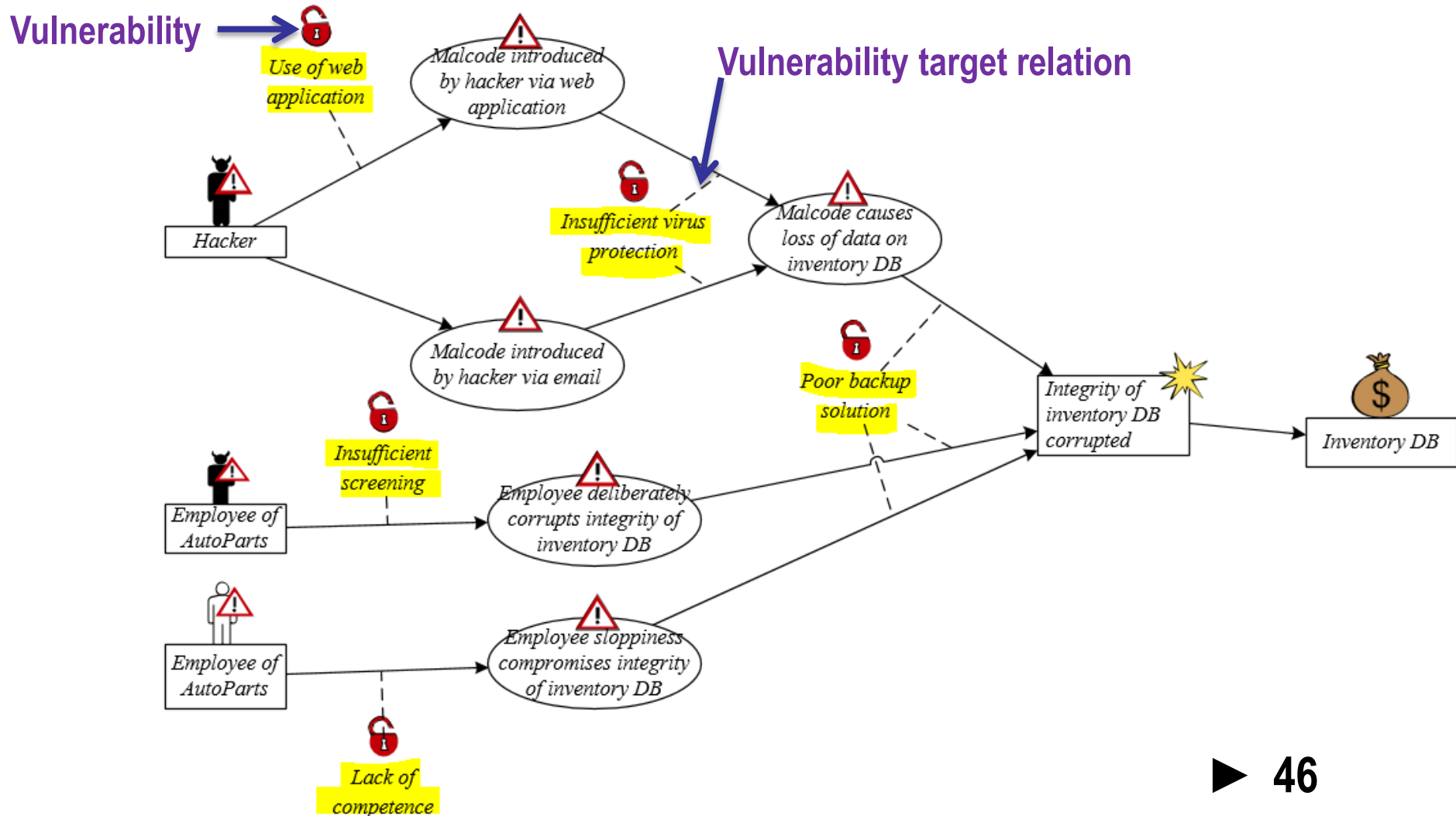


Step 5 - sub step 4: Identify Vulnerabilities

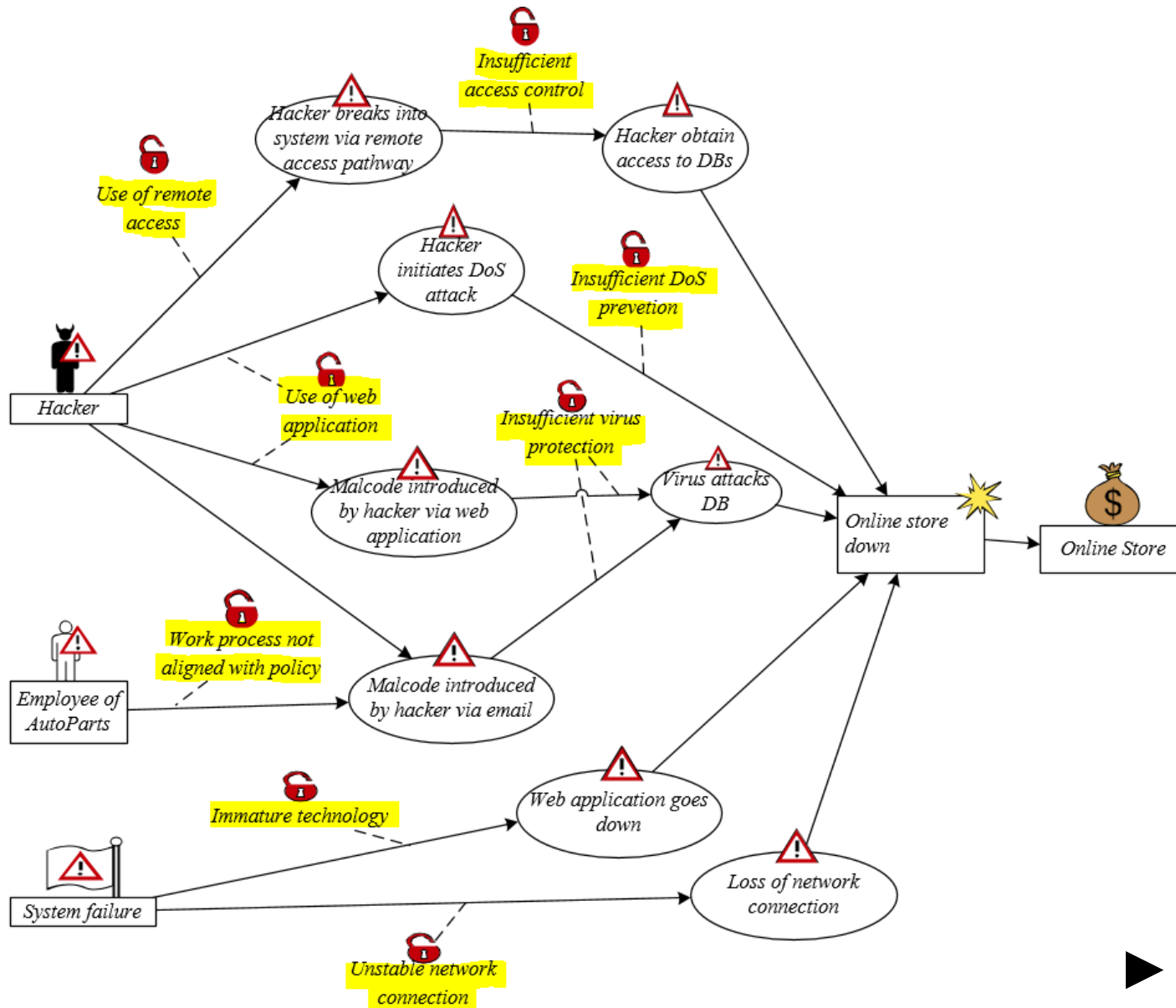
- **Answer the question:**
 - Which vulnerabilities make this possible?

Step 5 - sub step 4: Identify Vulnerabilities

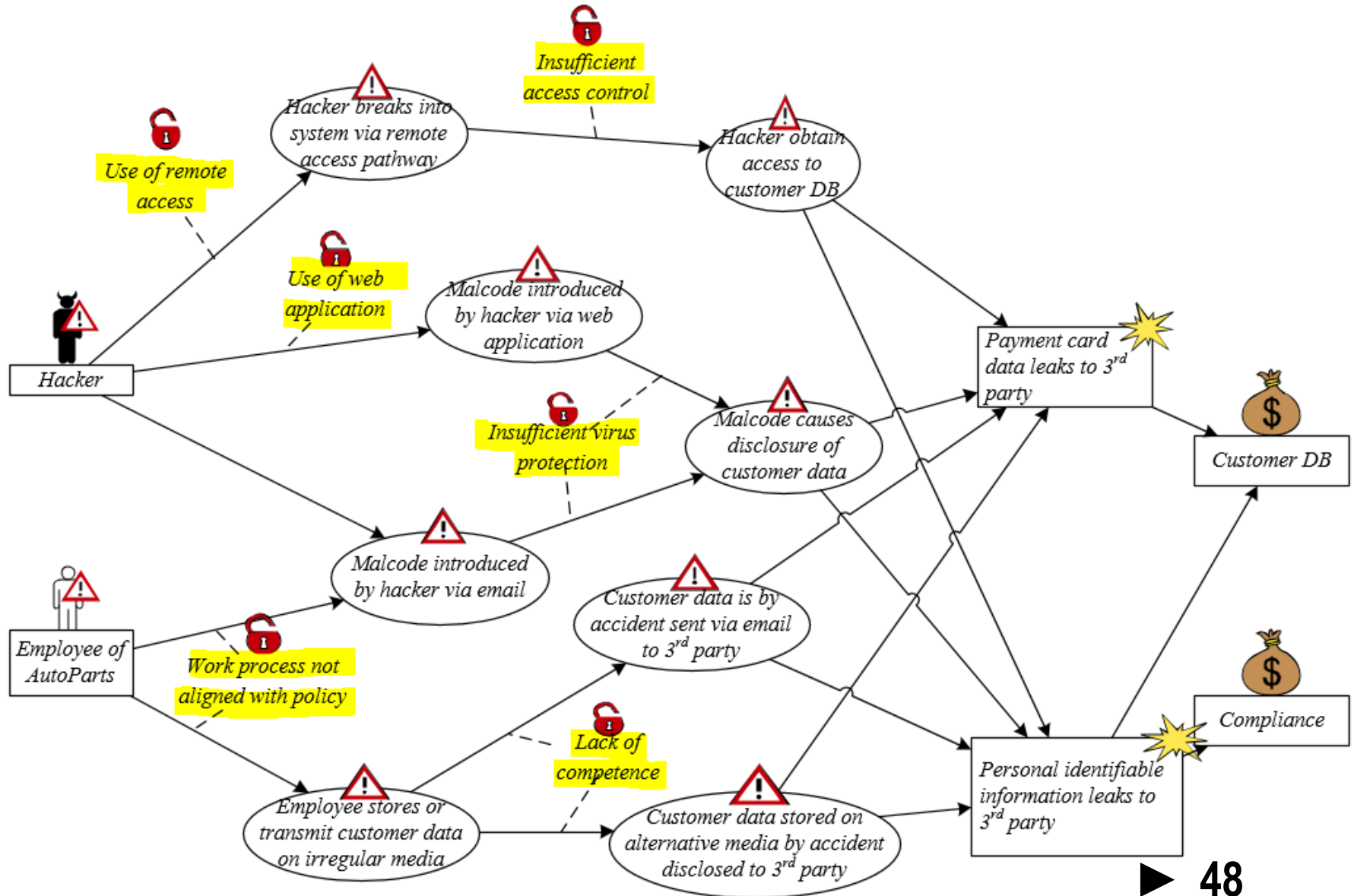
- Answer the question:
 - Which vulnerabilities make this possible?



Step 5 - sub step 4: Identify Vulnerabilities

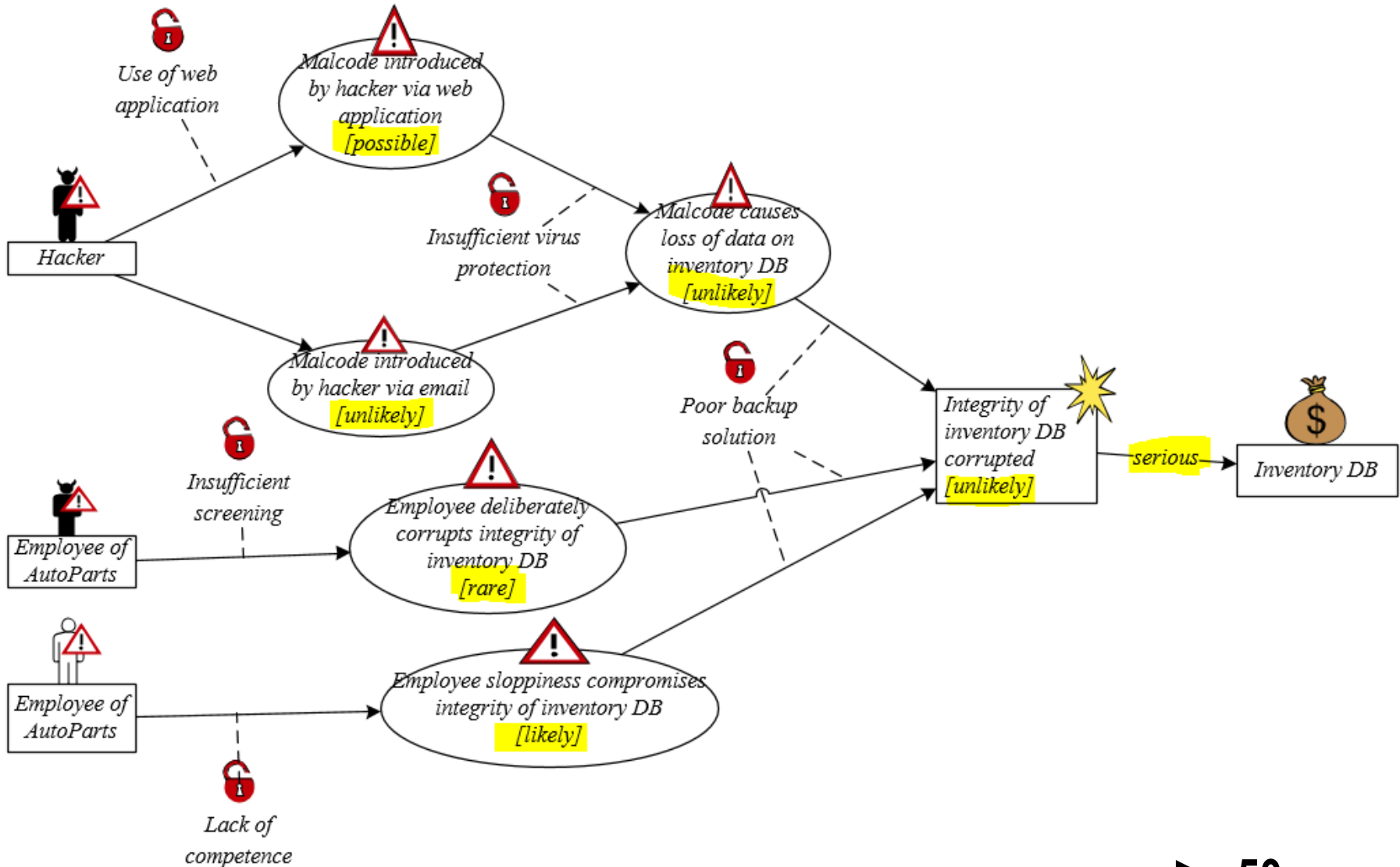


Step 5 - sub step 4: Identify Vulnerabilities

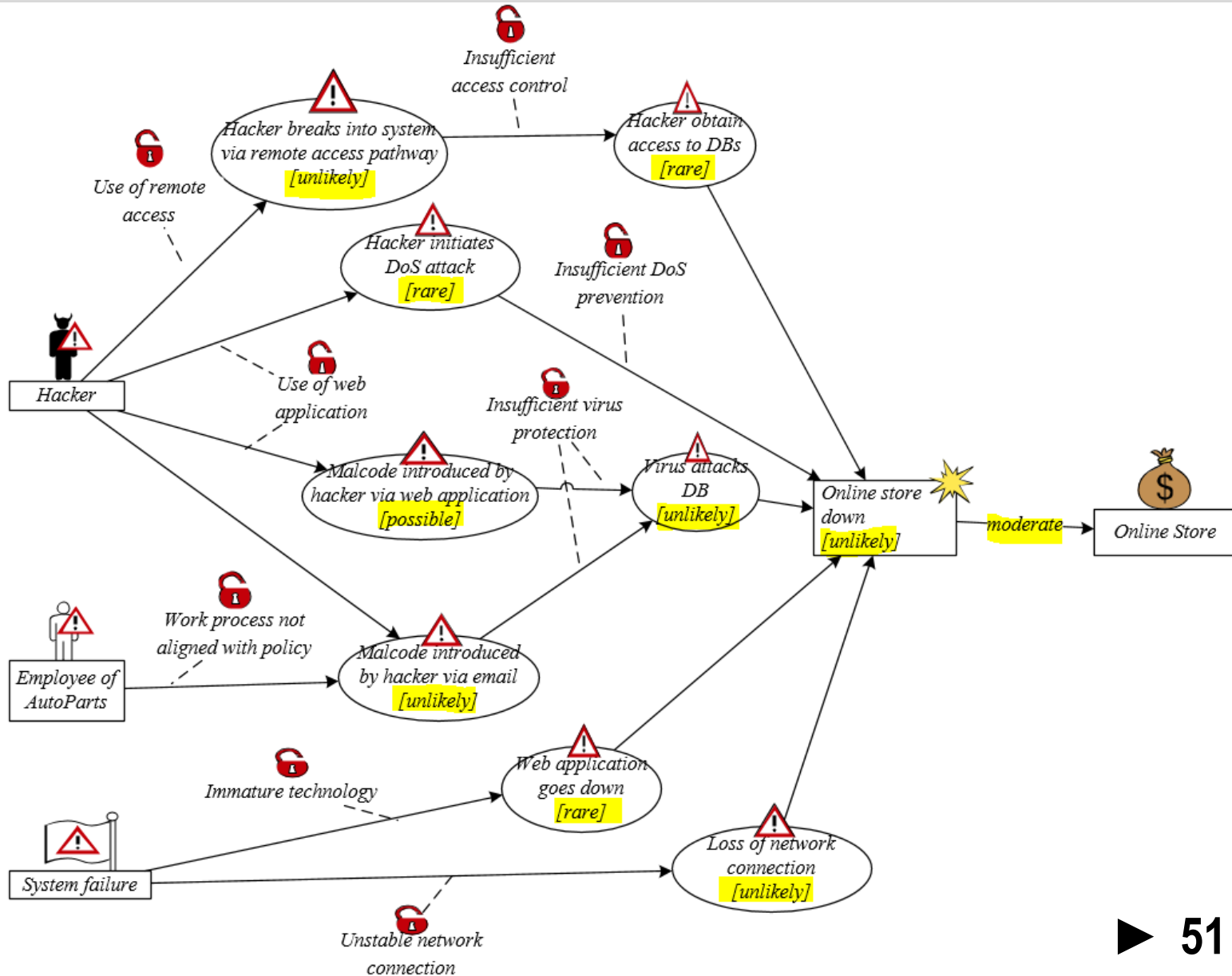


- **Objective: determine risk level of the identified risks**
- **Tasks: base on likelihood and consequence scale approved in Step 4**
 - Assign likelihood estimated for each Threat Scenario
 - Assign likelihood estimated for each Unwanted Incidents
 - Assign consequence caused by each Unwanted Incidents on each Asset (the consequence is denoted on “impact” relation)
- **Artifacts to be produced:**
 - Completed Threat diagrams with likelihood and consequences assigned

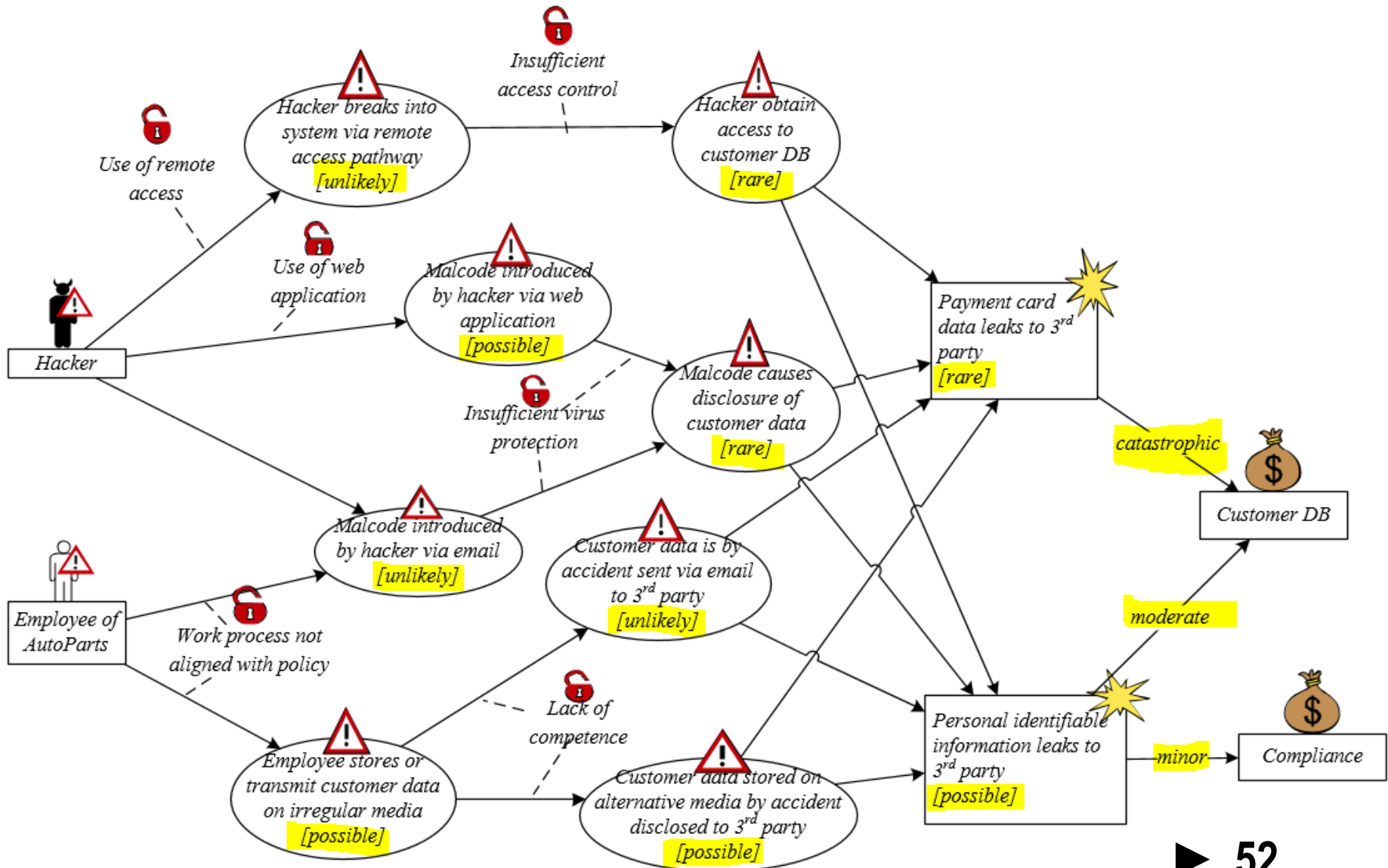
Example: Assign Likelihood and Consequence



Example: Assign Likelihood and Consequence



Example: Assign Likelihood and Consequence



- **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	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Unlikely	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Possible	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Likely	Acceptable	Monitor	Monitor	Need to be treated	Need to be treated
Certain	Acceptable	Monitor	Need to be treated	Need to be treated	Need to be treated



Example: Completed Risk Function

Risk Function (Online Store)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Serious	Catastrophic
Rare	Acceptable	Acceptable	Monitor	Monitor	Need to be treated
Unlikely	Acceptable	Acceptable	<i>R2:Online store down</i>	Monitor	Need to be treated
Possible	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Likely	Acceptable	Monitor	Monitor	Need to be treated	Need to be treated
Certain	Acceptable	Monitor	Need to be treated	Need to be treated	Need to be treated



Example: Completed Risk Function

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

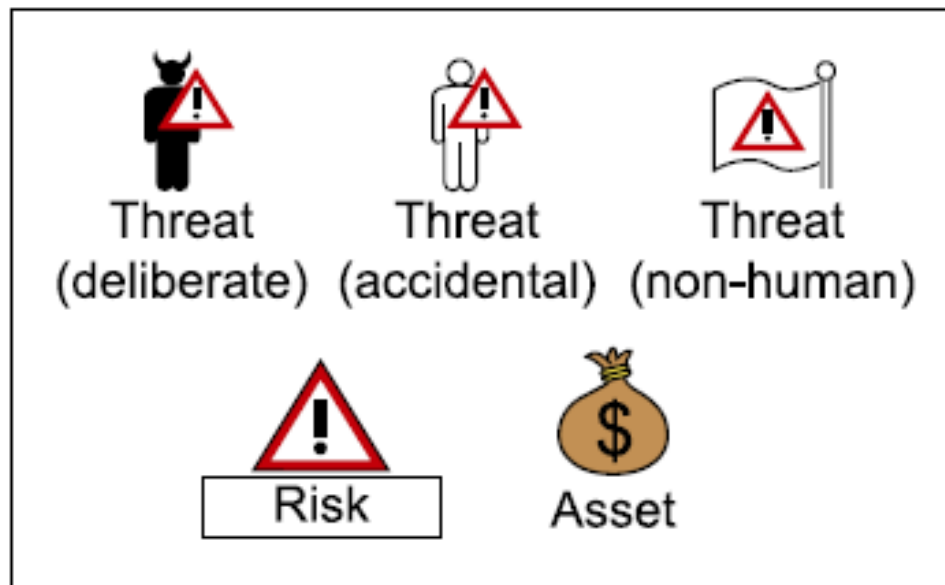
	Acceptable
	Monitor
	Need to be treated

Example: Completed Risk Function

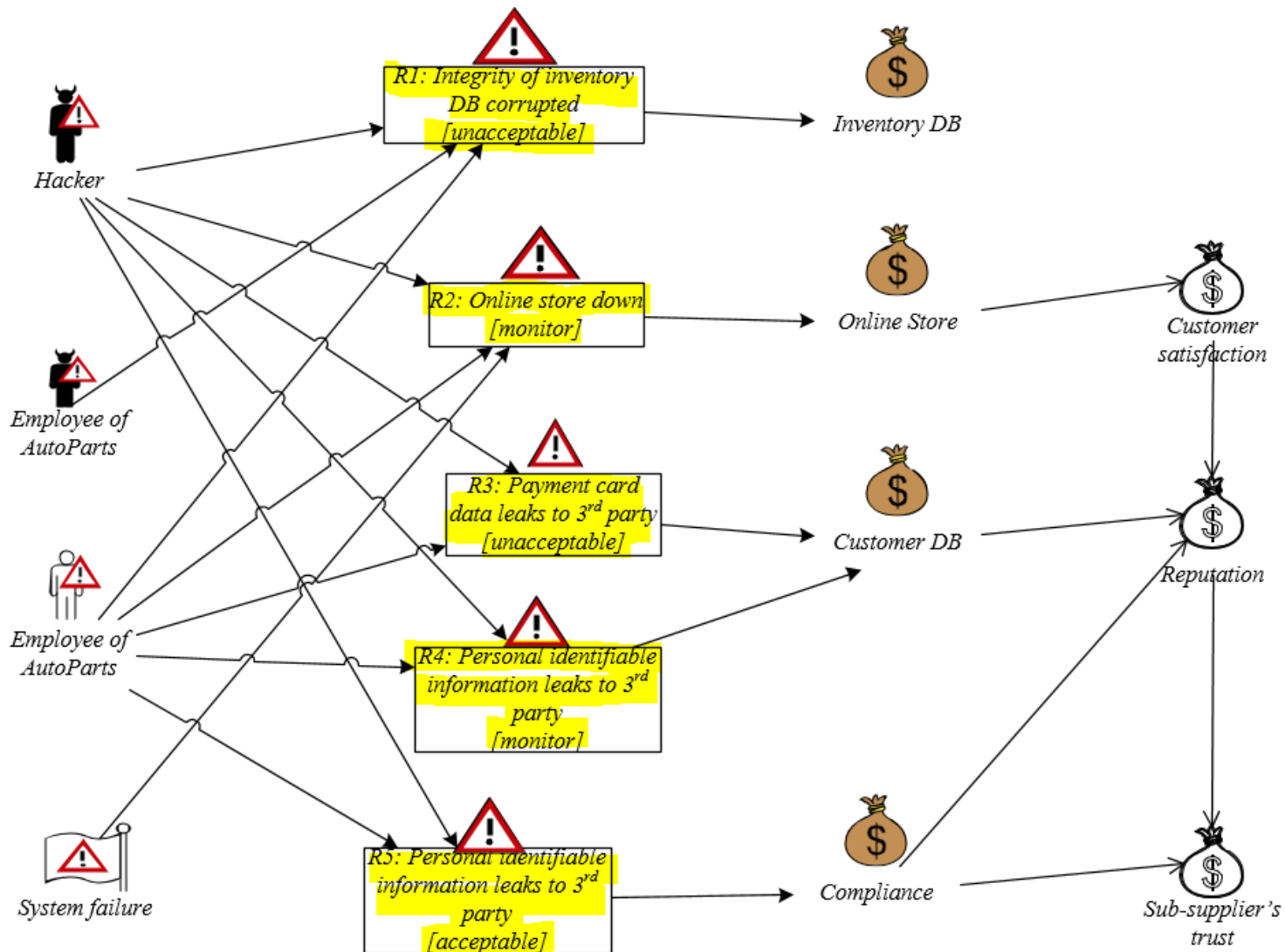
Risk Function (Compliance)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Serious	Catastrophic
Rare	Acceptable	Acceptable	Monitor	Monitor	Monitor
Unlikely	Acceptable	Acceptable	Monitor	Monitor	Need to be treated
Possible	Acceptable	<i>R5: Personal identifiable information leaks to 3rd party</i>	Monitor	Monitor	Need to be treated
Likely	Acceptable	Monitor	Monitor	Monitor	Need to be treated
Certain	Acceptable	Monitor	Monitor	Need to be treated	Need to be treated



- We use Risk diagram to show how Threats pose Risks to the Assets
- Notions to be used in Risk diagram:

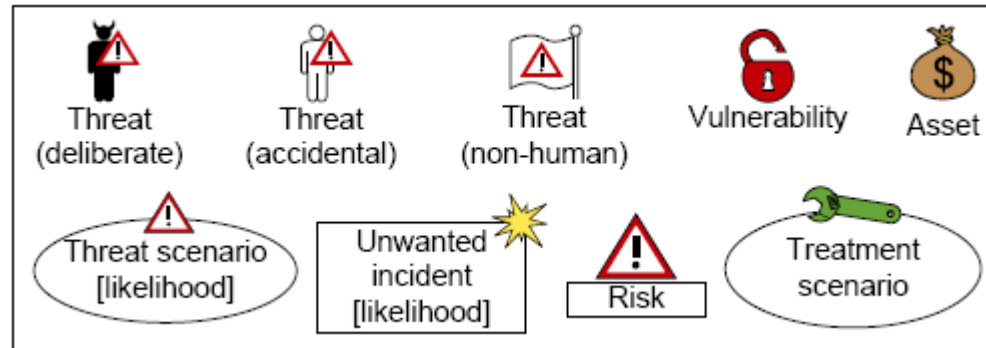


Example: Risk diagram

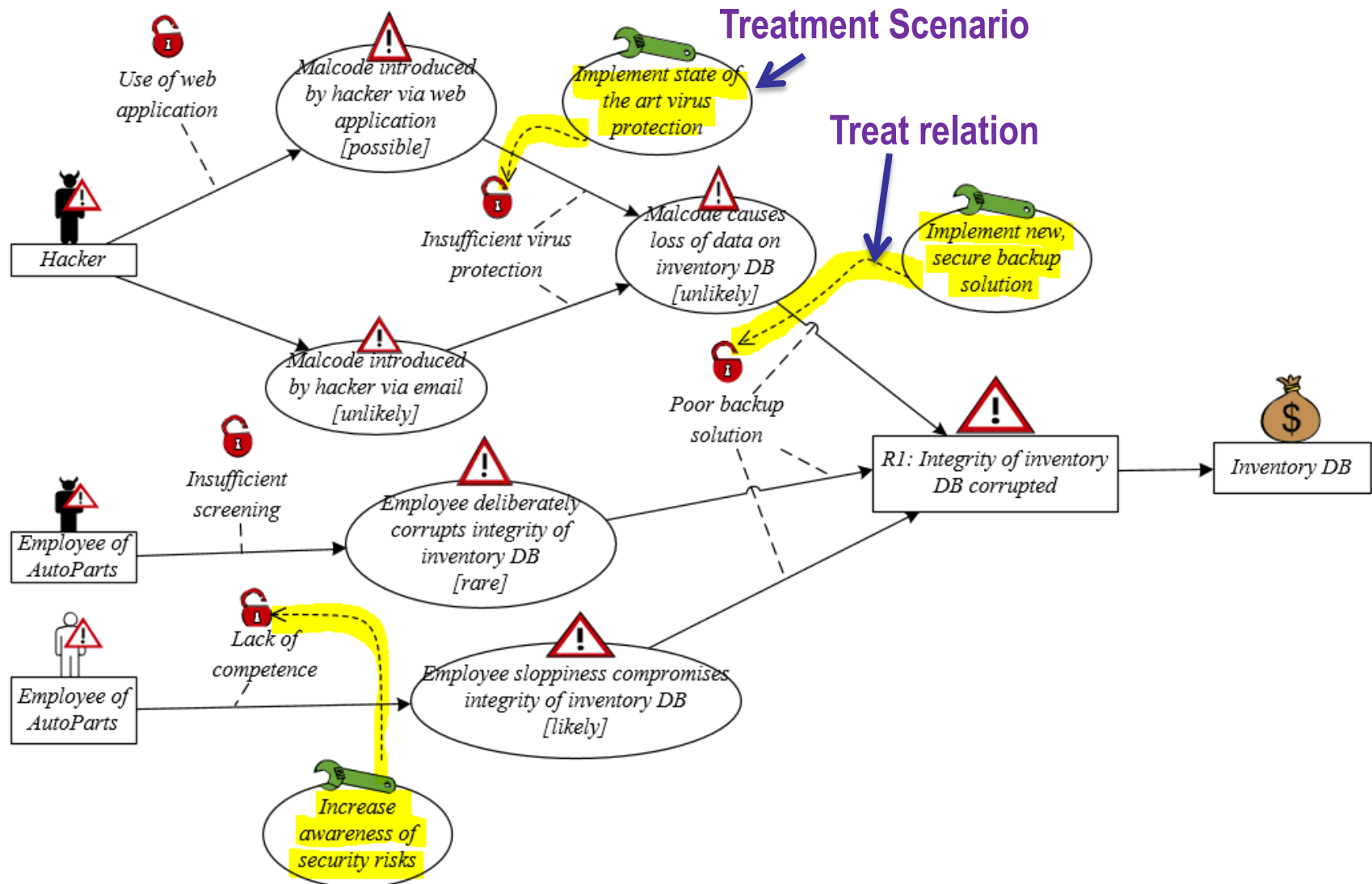


- **Objective: identify cost effective treatments for the unacceptable risks**
- **Task:**
 - Identify Treatment Scenario for unacceptable risks:
 - What can we do to reduce the risks to an acceptable (or monitor) level?
 - Create Treatment diagram
 - Summarize by Treatment Overview diagram
 - Evaluate 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

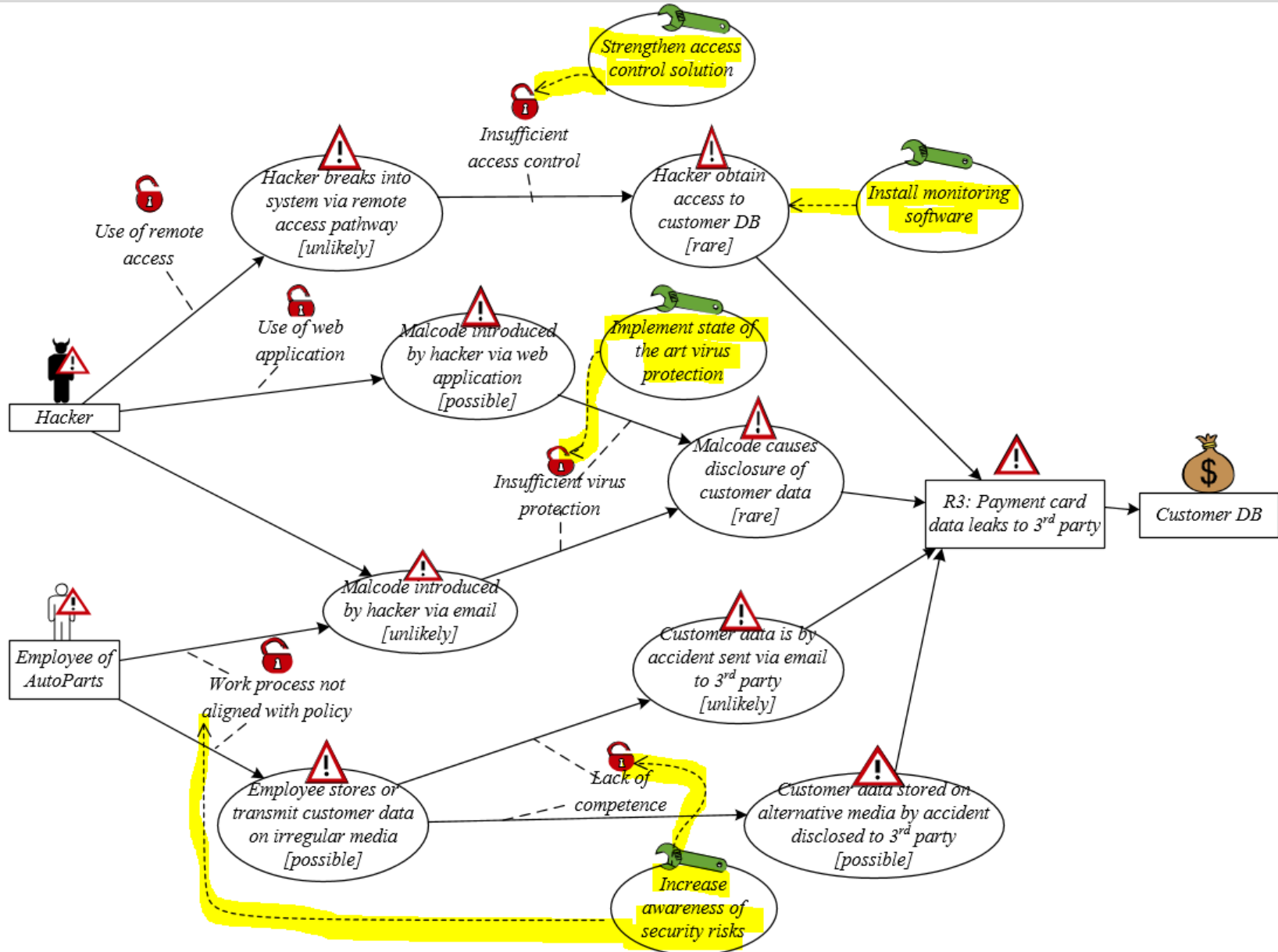
- Notions to be used in Treatment Diagram



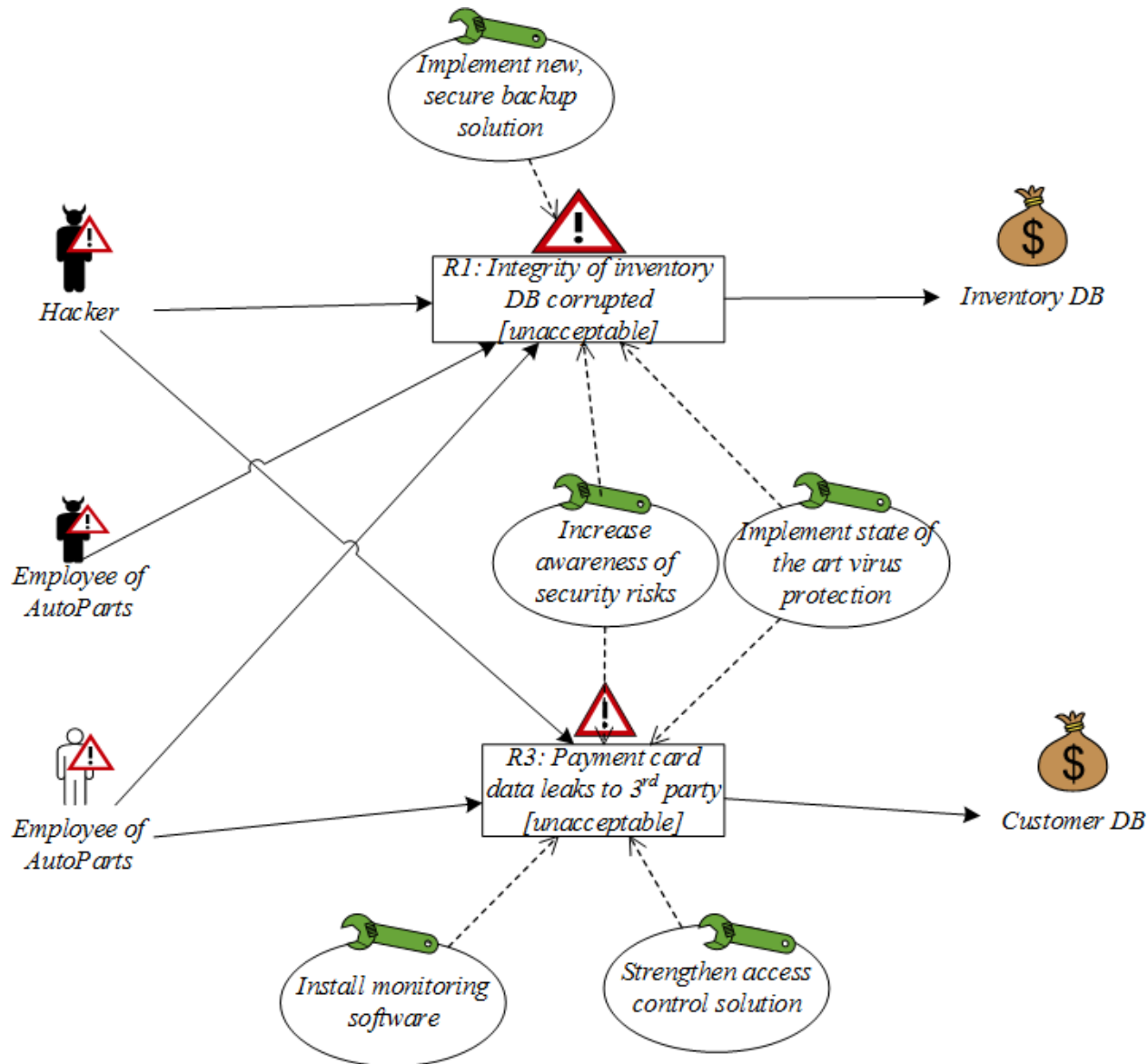
Example: Treatment Diagram



Example: Treatment Diagram



Example: Treatment Overview Diagram



- 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
		R2	R2: Unacceptable to Acceptable	
T3: Implement state of the art virus protection	Low	R1	R1: Unacceptable to Monitor	Yes
		R2	R1: Unacceptable to Monitor	
T4: Install monitoring software	Medium	R2	R2: Unacceptable to Acceptable	Yes
T5: Strengthen access control solution	High	R2	R2: Unacceptable to Monitor	No

Treatment	Cost	Risk	Risk reduction	Select to implement
-----------	------	------	----------------	---------------------

Final recommendations to customer

T2: Increase awareness of security risks	Low	R1	R1: Unacceptable to Monitor	Yes
--	-----	----	-----------------------------	-----

R2	R2: Unacceptable to Acceptable
----	--------------------------------

T3: Implement state of the art virus protection	Low	R1	R1: Unacceptable to Monitor	Yes
---	-----	----	-----------------------------	-----

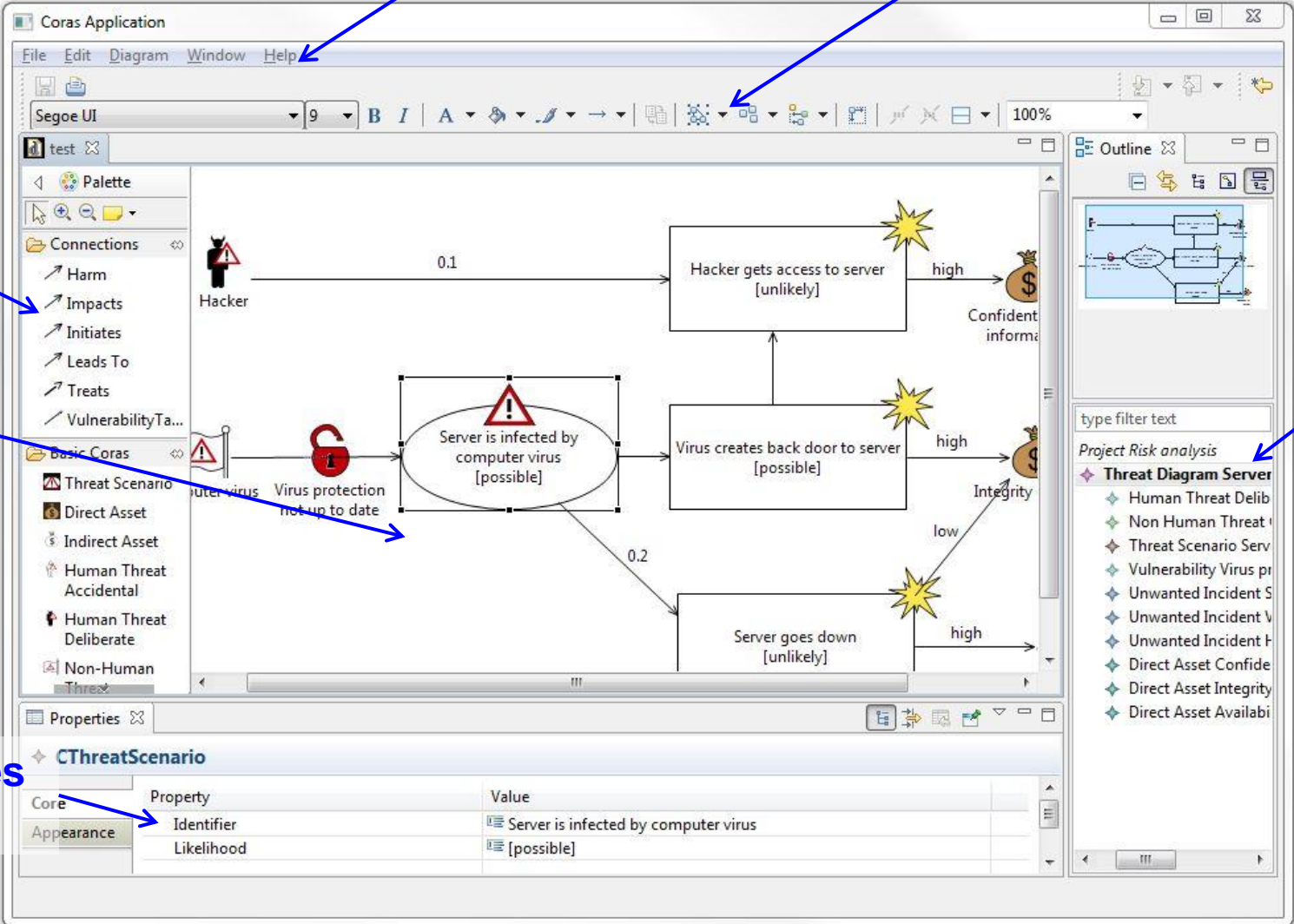
R2	R1: Unacceptable to Monitor
----	-----------------------------

T4: Install monitoring software	Medium	R2	R2: Unacceptable to Acceptable	Yes
---------------------------------	--------	----	--------------------------------	-----

T5: Strengthen access control solution	High	R2	R2: Unacceptable to Monitor	No
--	------	----	-----------------------------	----

- 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



The screenshot shows the Coras Application interface with several annotations:

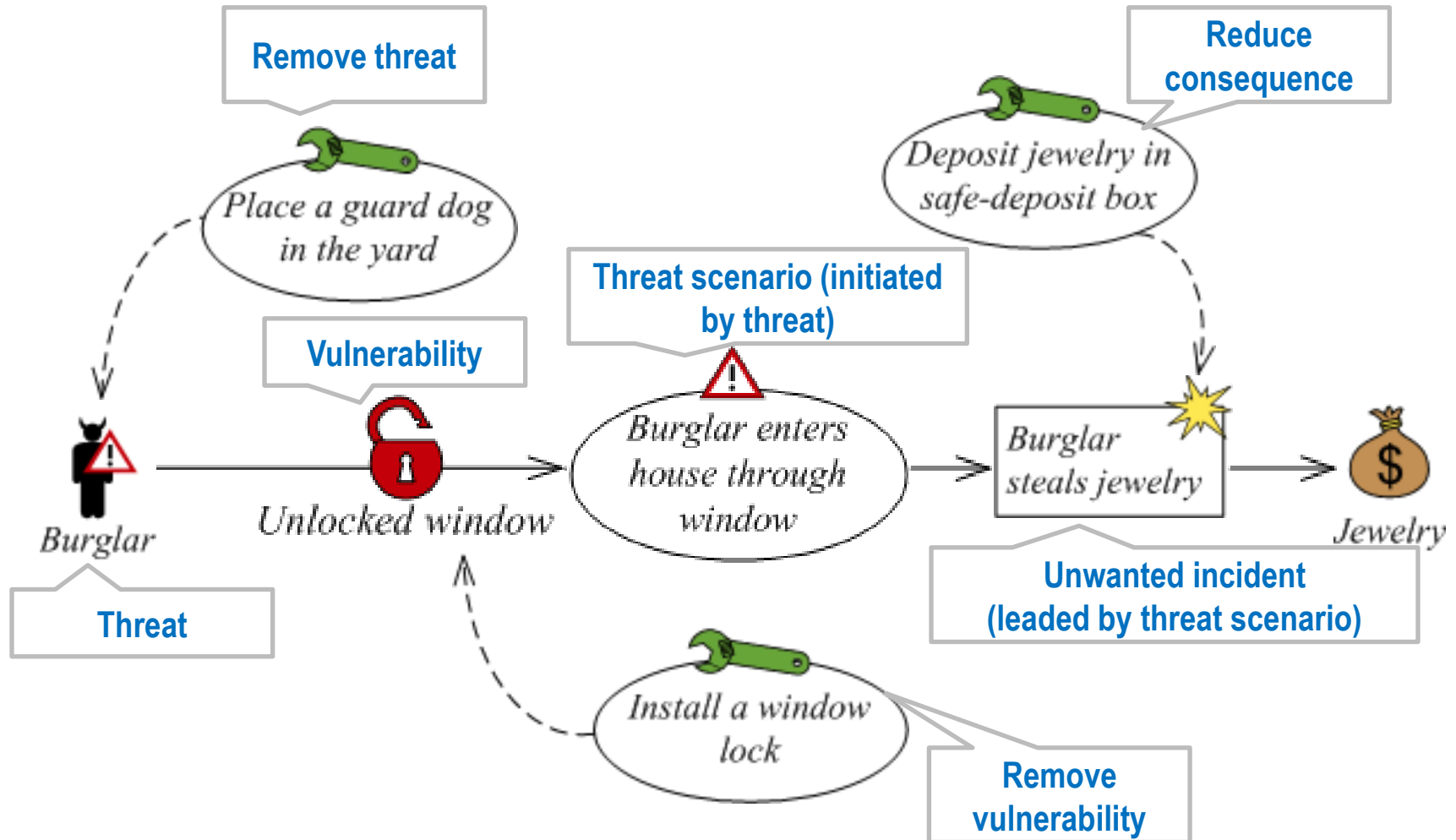
- Pull-down menu:** Points to the menu bar (File, Edit, Diagram, Window, Help).
- Tool bar:** Points to the toolbar containing various diagram editing tools.
- Palette:** Points to the left sidebar containing a list of threat scenarios and assets.
- Canvas:** Points to the central workspace where the threat diagram is being constructed.
- Outline:** Points to the right sidebar showing a hierarchical tree of the diagram's elements.
- Properties window:** Points to the bottom window showing the properties of the selected element.

The diagram on the canvas illustrates a threat scenario starting with a **Hacker** (actor) who initiates an event: **Hacker gets access to server [unlikely]** (likelihood 0.1). This leads to **Confident information** (asset) with a **high** impact. Another path shows **Server is infected by computer virus [possible]** (likelihood 0.2), which leads to **Virus creates back door to server [possible]** (likelihood 0.2), resulting in **Integrity** (asset) with a **high** impact. A third path shows **Server goes down [unlikely]** (likelihood 0.2), resulting in **Integrity** (asset) with a **high** impact. A fourth path shows **Server goes down [unlikely]** (likelihood 0.2), resulting in **Confident information** (asset) with a **low** impact. The diagram also includes a **Computer virus** (actor) and **Virus protection not up to date** (condition).

Properties window:

Core	Property	Value
Appearance	Identifier	Server is infected by computer virus
	Likelihood	[possible]

- CORAS risk model in a nutshell**

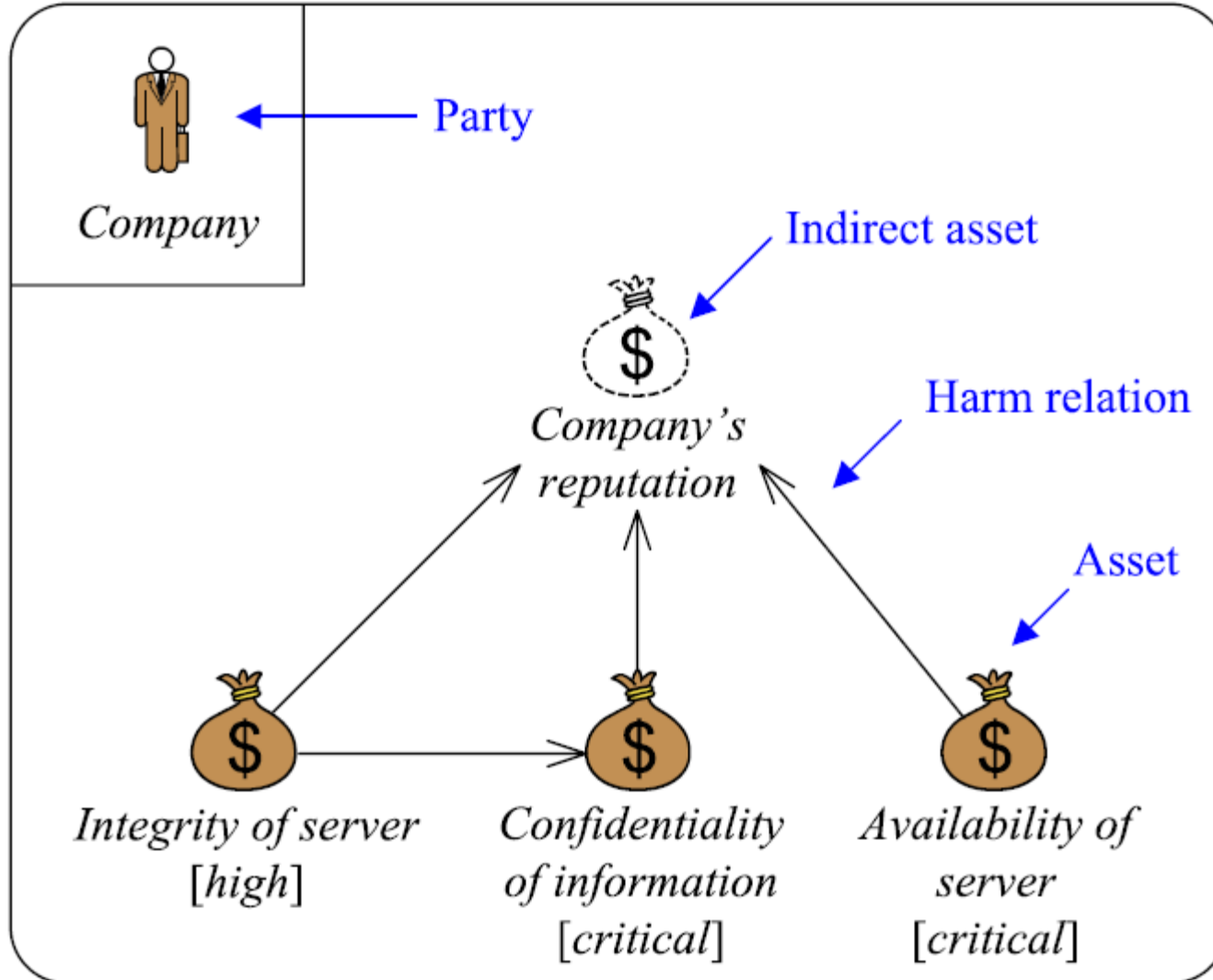


- **CORAS consists of three parts**
 - Method
 - Language
 - Tool
- **Model-driven and asset-driven**
- **Concrete guidelines for how to conduct risk analysis in practice**
- **Based on a well-established and precisely defined conceptual framework**
- **Based on internationally established standards**

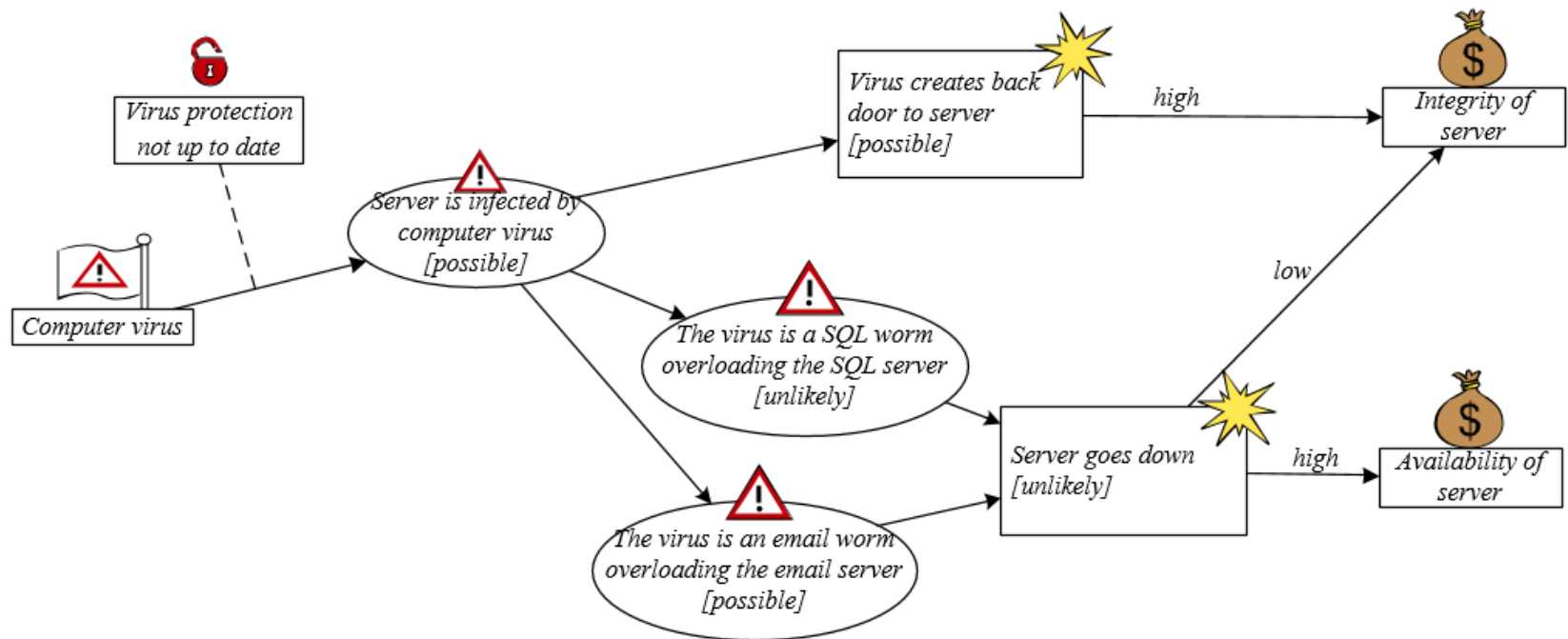
- **Book:** <http://www.springer.com/computer/swe/book/978-3-642-12322-1>
- **CORAS tool demo:** <http://coras.sourceforge.net/coras-tool-demo.htm>
- **Download:**
 - Tool: <http://coras.sourceforge.net/downloads.html> (CORAS editor v1.1)
 - Microsoft Visio stencil for the CORAS Language: <http://coras.sourceforge.net/downloads.html>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

- **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.**

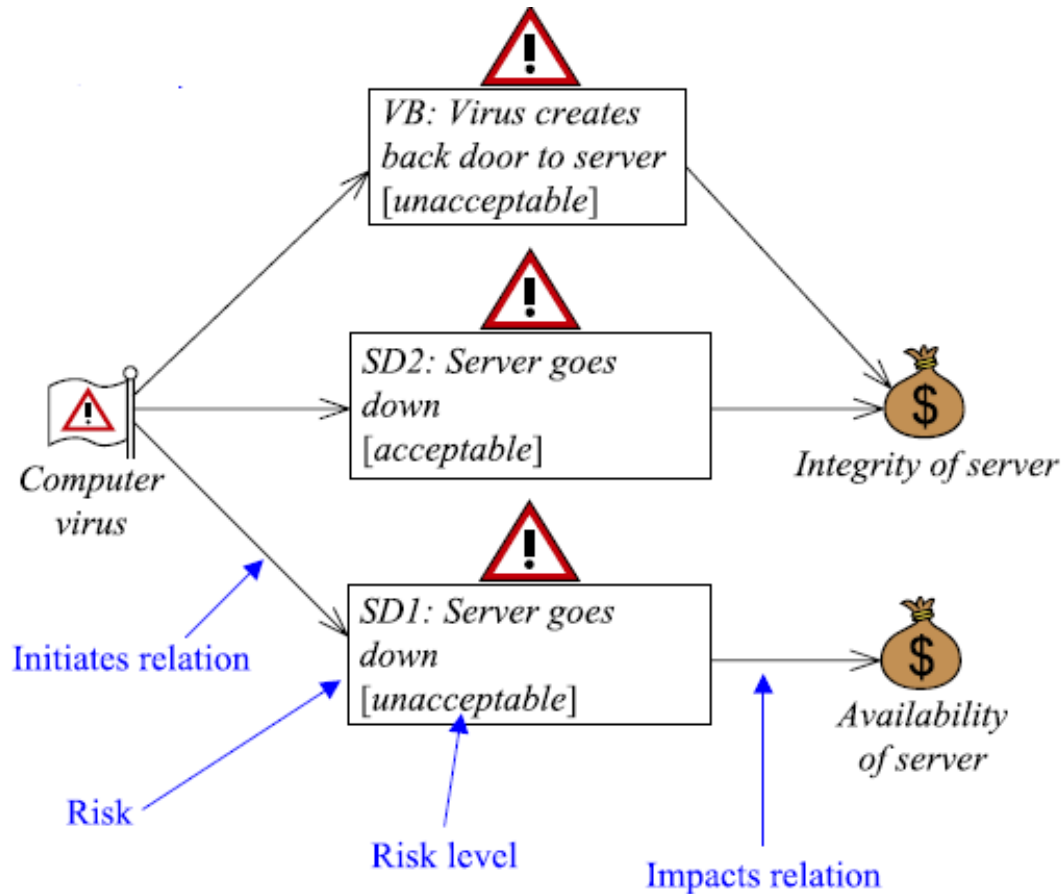
- **Asset Diagram**



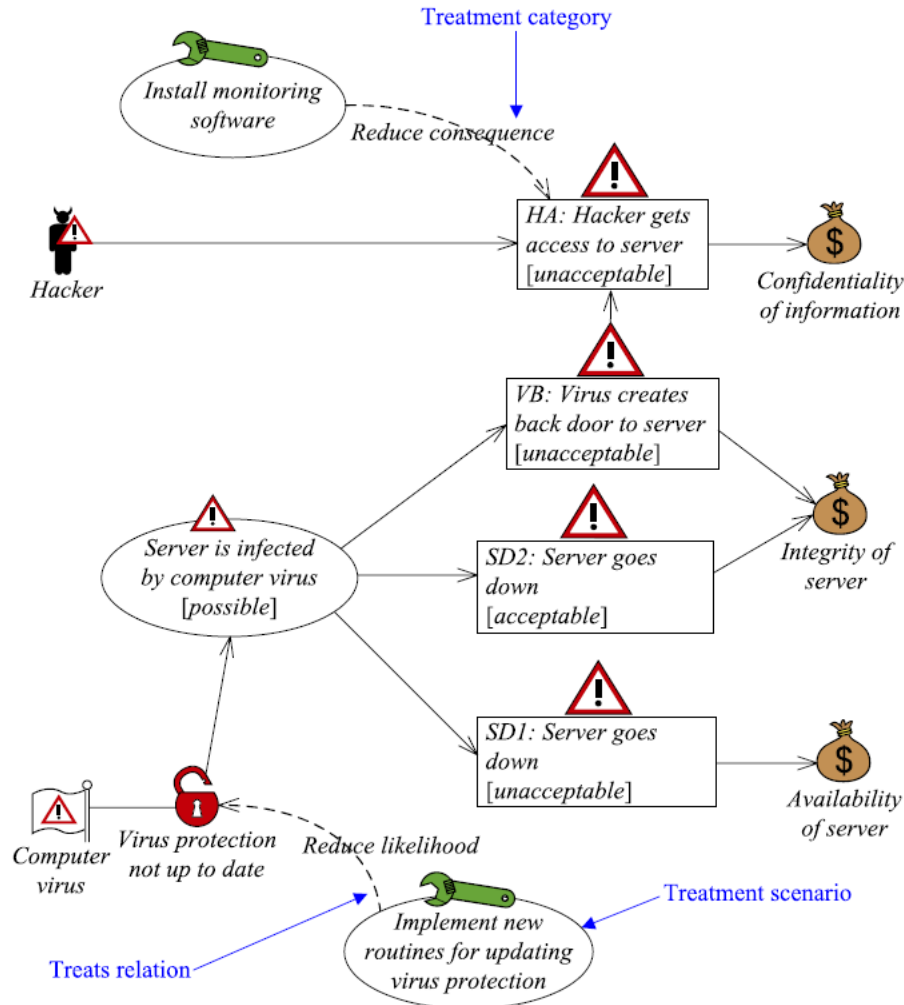
• Threat Diagram



- Risk Diagram



• Treatment Diagram



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

• Treatment Overview Diagram

