

# Security Engineering Fall 2015

*Lecture 06 – CORAS*

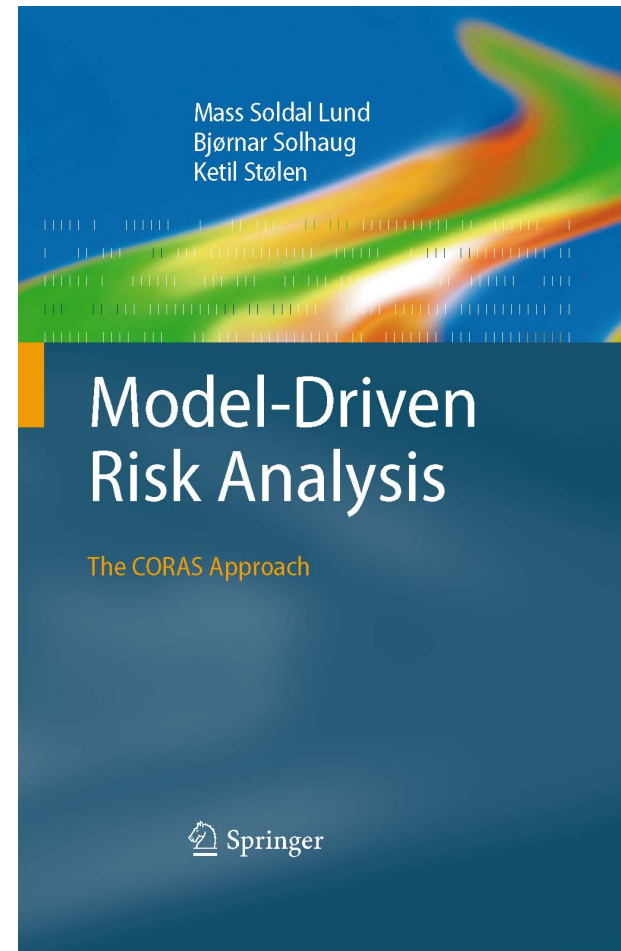
*Fabio Massacci*

# 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 (graphical) 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
  - A tool to support the risk analysis process
- **Based on standard ISO 31000**
- **Book**
  - <http://www.springer.com/computer/swe/book/978-3-642-12322-1>

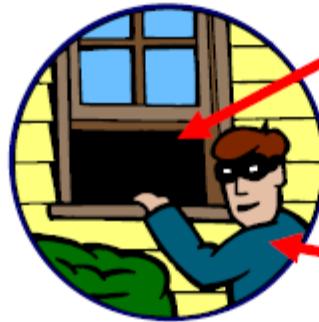


# Terms

asset, something of value



vulnerability



threat

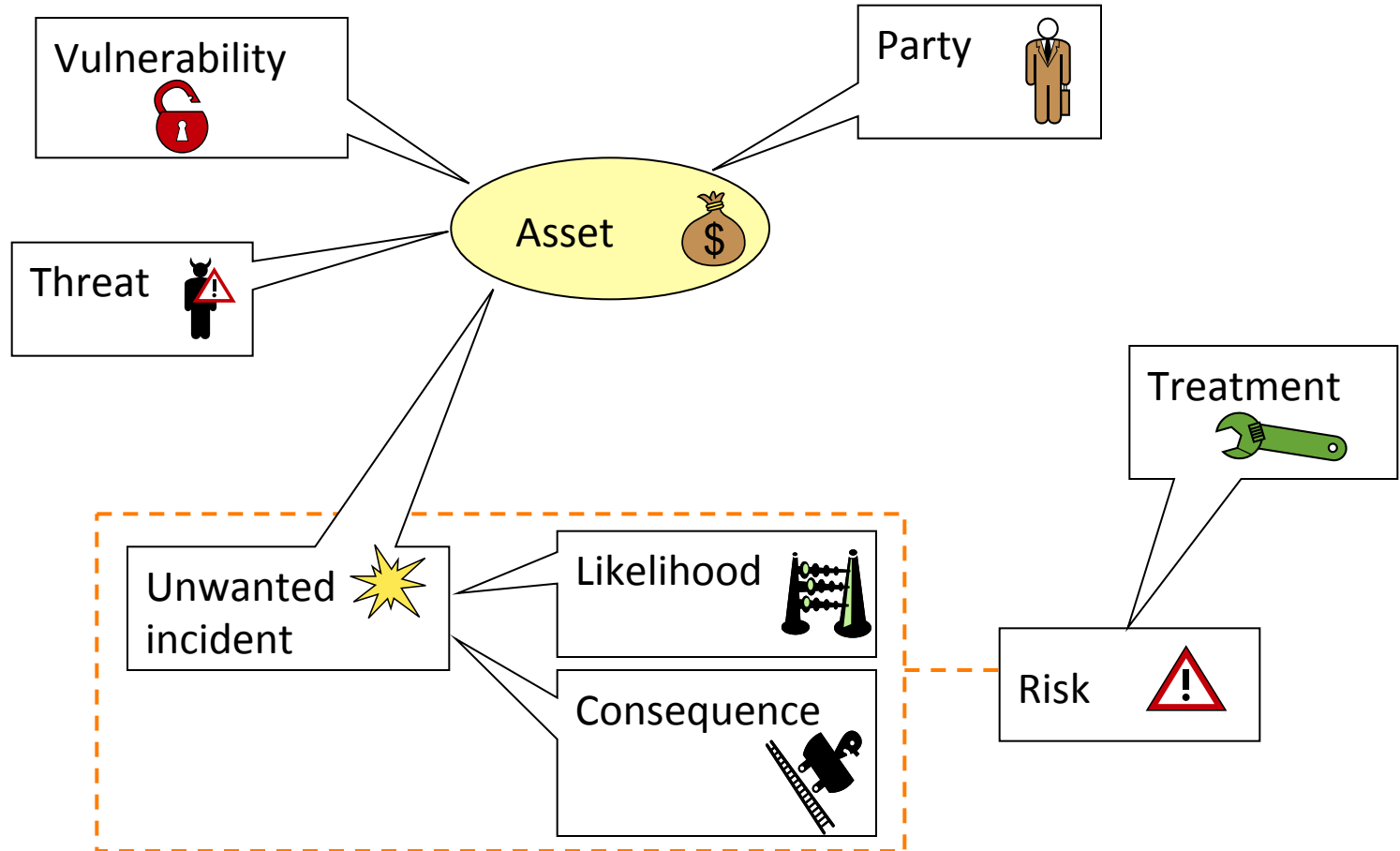
reduced risk level

constitutes a security risk

we need to introduce security mechanisms

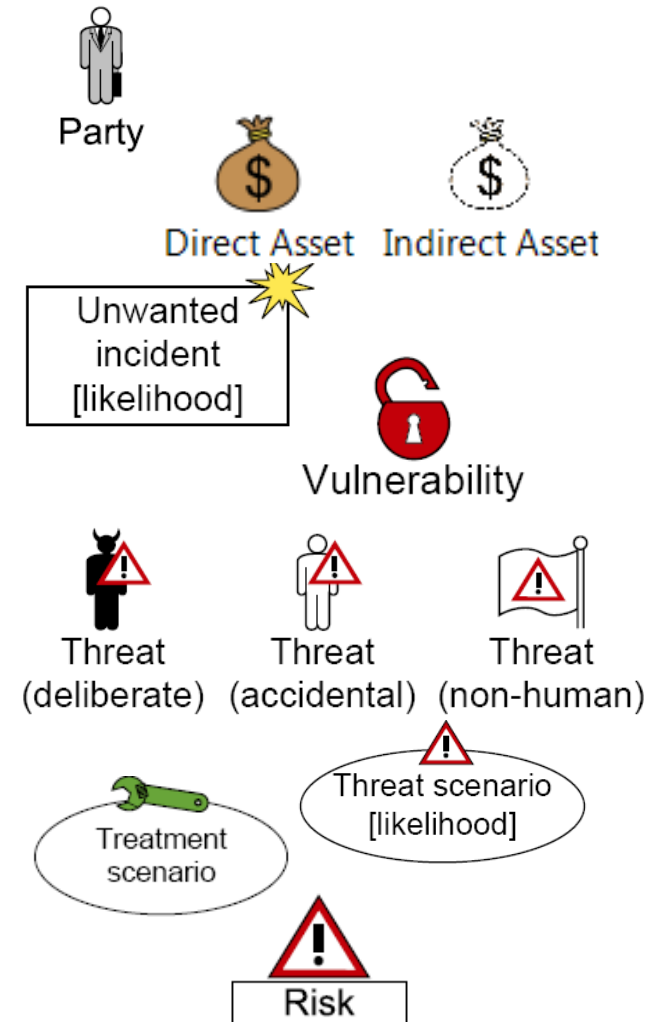


# CORAS Central Concepts



# 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

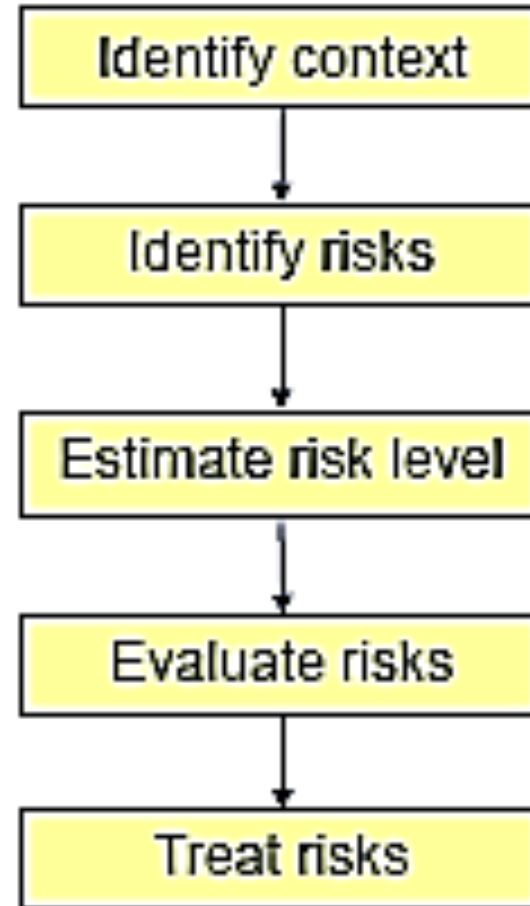


# Risk modeling

- ***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***

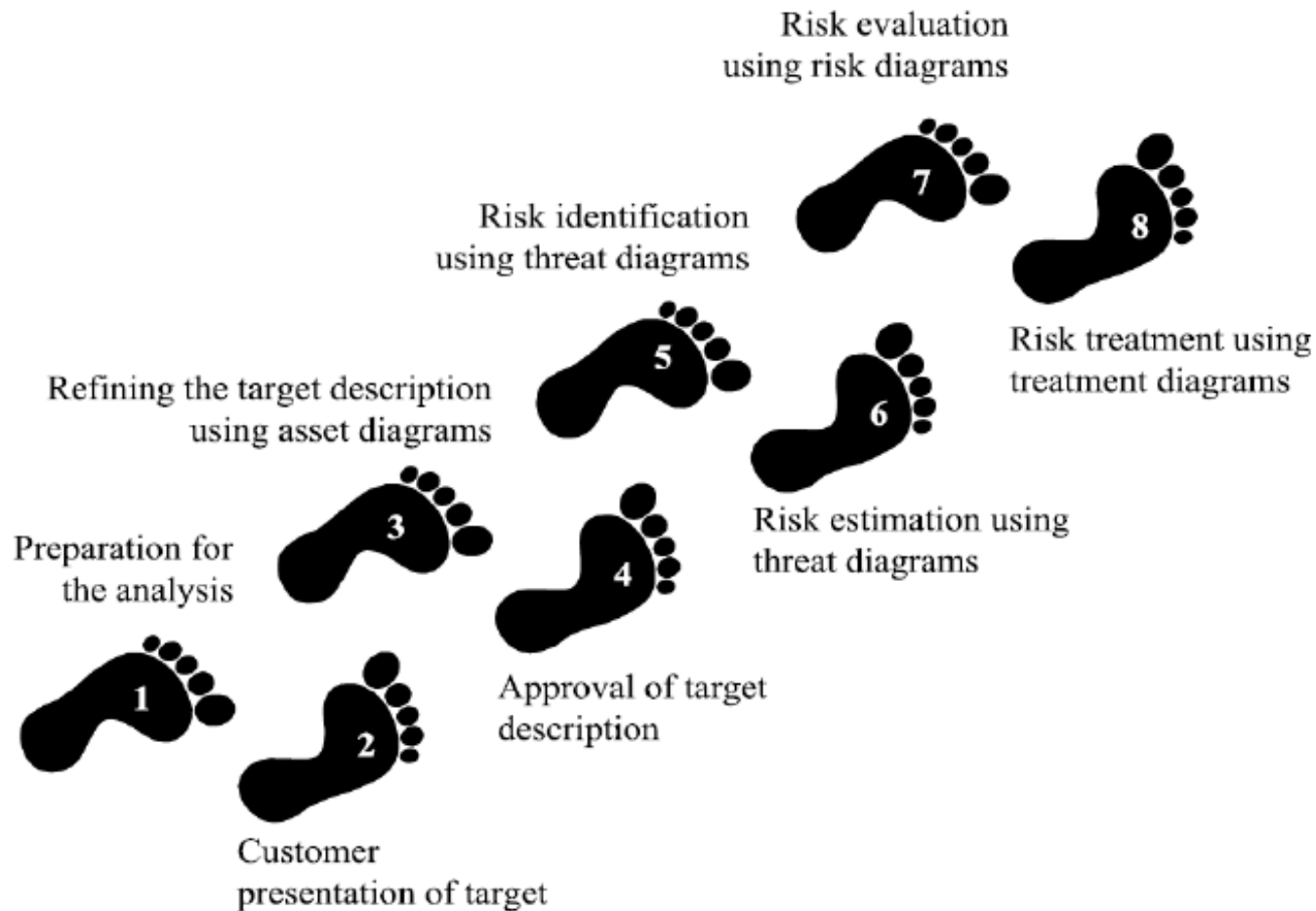
# The CORAS process

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



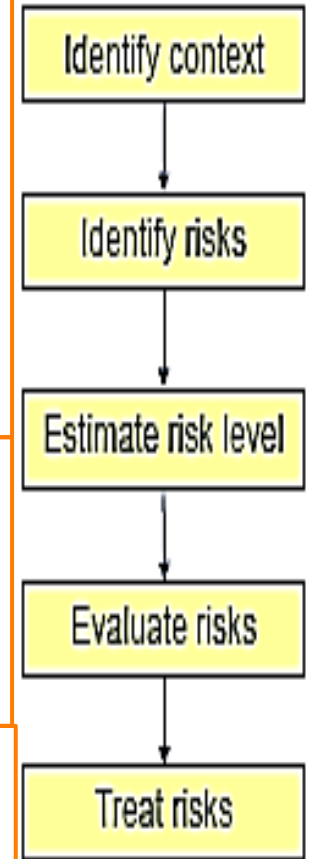


# The 8 steps of a CORAS risk analysis



# The 8 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***



# 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
    - Usually called Target of Evaluation (TOE) or Target of Assessment - TOA)

# Example: AutoParts

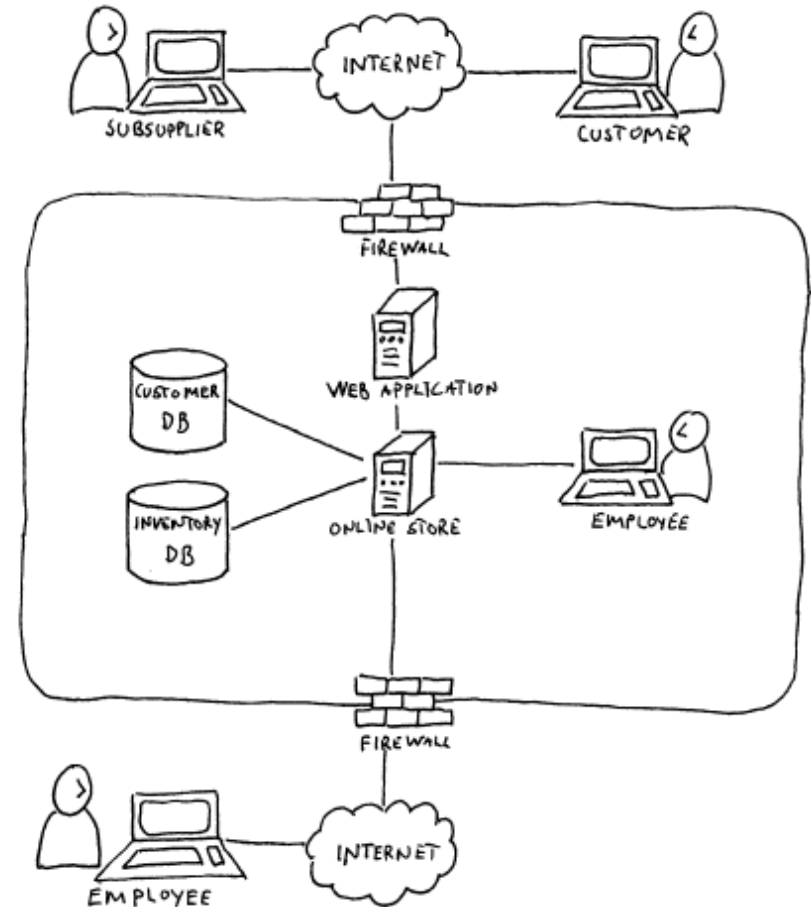
- ***AutoParts is a company.***
  - Its business is to sell spare parts and accessories for a wide range of car makes and vehicle models.
- ***AutoParts has***
  - an automated online store.
- ***AutoParts is***
  - distributing catalogues by mail that present its products and
  - usually shipping goods to customers paying 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.

## 2: Customer presentation of ToE

- **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

## 2: Customer presentation on the target (Example)

- ***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.

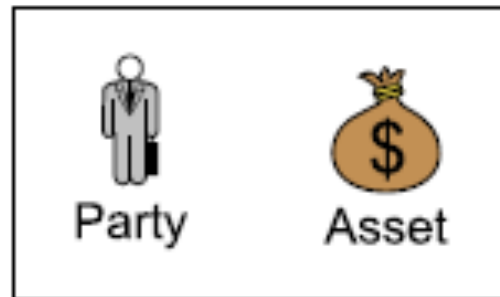


# 3: Refining target description using asset diagrams

- **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: includes relations between **Assets**, and **Parties**
  - 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***

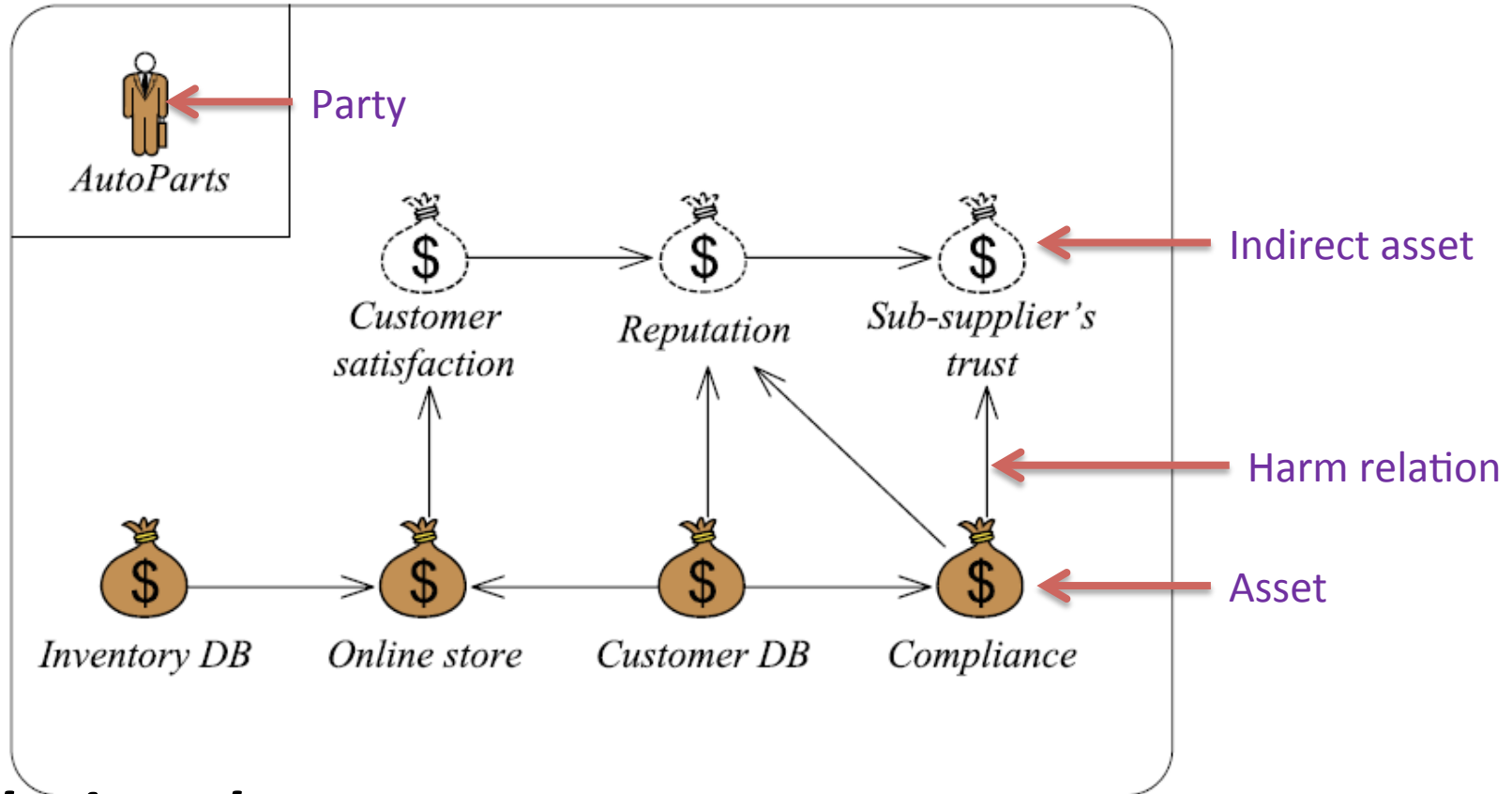




# Example: Identify Party and Asset

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

# Example: Asset diagram


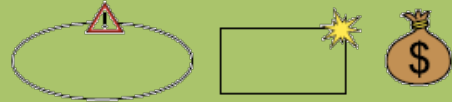



- **Relations between assets**


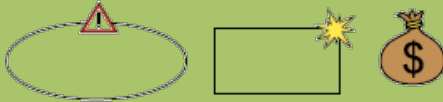

- Harm in one asset might harm also other assets

# High Level Risk Analysis


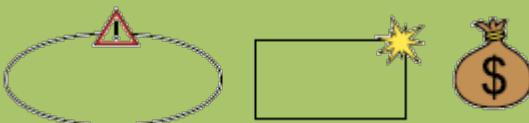

- Preliminary list of Unwanted Incidents***

 Who/ What is the cause?	 How? What may happen? What does it harm?	 What makes this possible?
hacker	Leaked customer database	A SQL injection makes something possible
hacker	altered inventory database changes in costs	Web application is vulnerable
employee	modified inventory to steal a part for his own purposes	work process (lacking separation of duties), access control, motivation(?), lack of vetting process (employee selection)

# High Level Risk Analysis (II)

 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 DBs	Insufficient virus protection
Hacker	DoS attack causes online store to go down	Use of web app; insufficient DoS attack prevention

# High Level Risk Analysis (III)

 <p>Who/ What is the cause?</p>	 <p>How? What may happen? What does it harm?</p>	 <p>What makes this possible?</p>
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

# 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 direct 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:***
  - frequency or probability of something to occur
- ***Example of Likelihood scale (App specific)***

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 (II)

- *Another example of Likelihood scale*

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



# Define Consequence scale

- ***Consequence:***
  - The impact of an unwanted incident on an asset in terms of harm or reduced asset value
- ***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
- ***Again application/domain specific***

Consequence	Description
Catastrophic	Downtime in range [1 week, $\infty$ >
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 [30%,100%] of records are affected
Serious	Range of [10%,30%] of records are affected
Moderate	Range of [1%,10%] of records are affected
Minor	Less than 1% of records are affected
Insignificant	Only few individual customers 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

# Risk Function and evaluation criteria

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

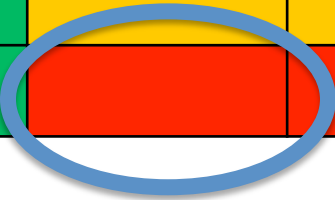
Risk Function (Inventory DB)					
Consequence/ Likelihood	Insignificant	Minor	Moderate	Serious	Catastrophic
Rare	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Unlikely	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Possible	Acceptable	Acceptable	Monitor	Need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

	Acceptable
	Monitor
	Need to be treated

# Risk Function and evaluation criteria (II)

- *May differ for different assets*

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	Need to be treated	Need to be treated	Need to be treated	Need to be treated



	Acceptable
	Monitor
	Need to be treated

# Risk Function and evaluation criteria (III)

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



# Risk Function and evaluation criteria (III)

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





# Two Alternatives

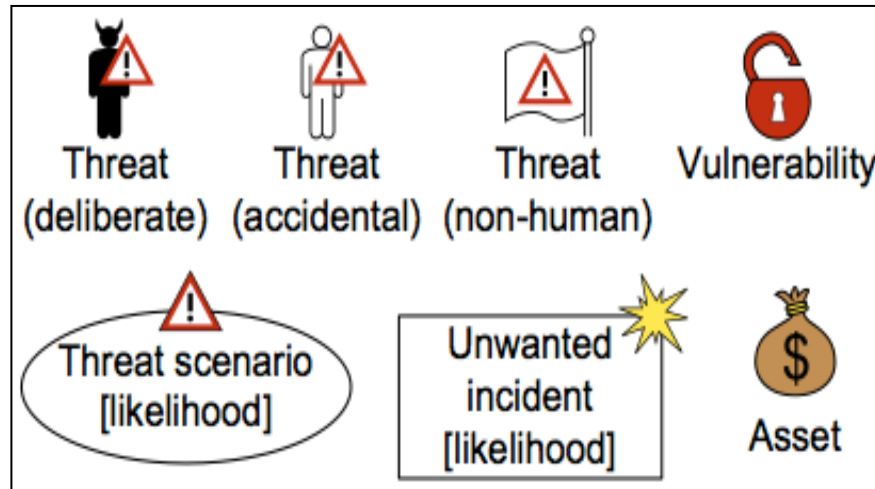
- ***Risk Functions depends on Assets***
- ***Alternative 1:***
  - Risk Function is constant across all assets
  - Likelihood and impact definition change by assets
- ***Alternative 2:***
  - Risk function changes
  - Likelyhood and impact definition are the same for each assets
- ***Both***
- ***Limitations of each approach?***
  - What is CORAS official byline?

# 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

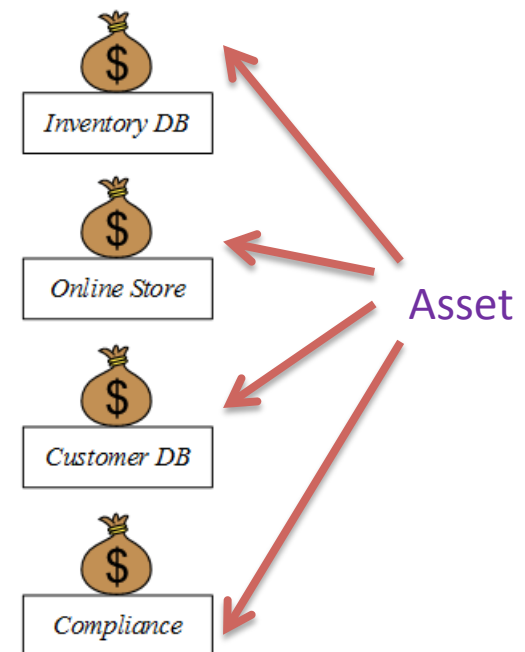
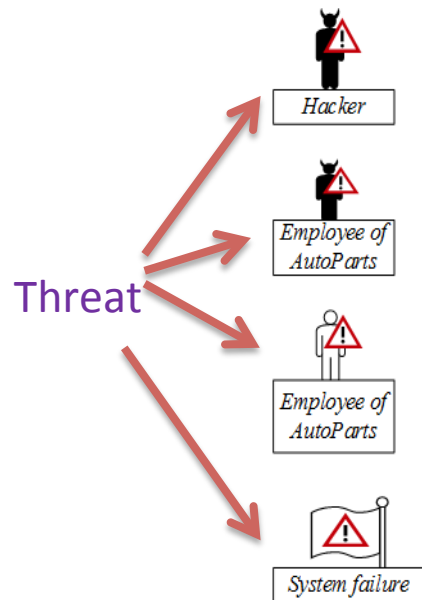
# 5: Risk Identification using Threat diagrams (II)

- *Notions to be used in Threat Diagram*



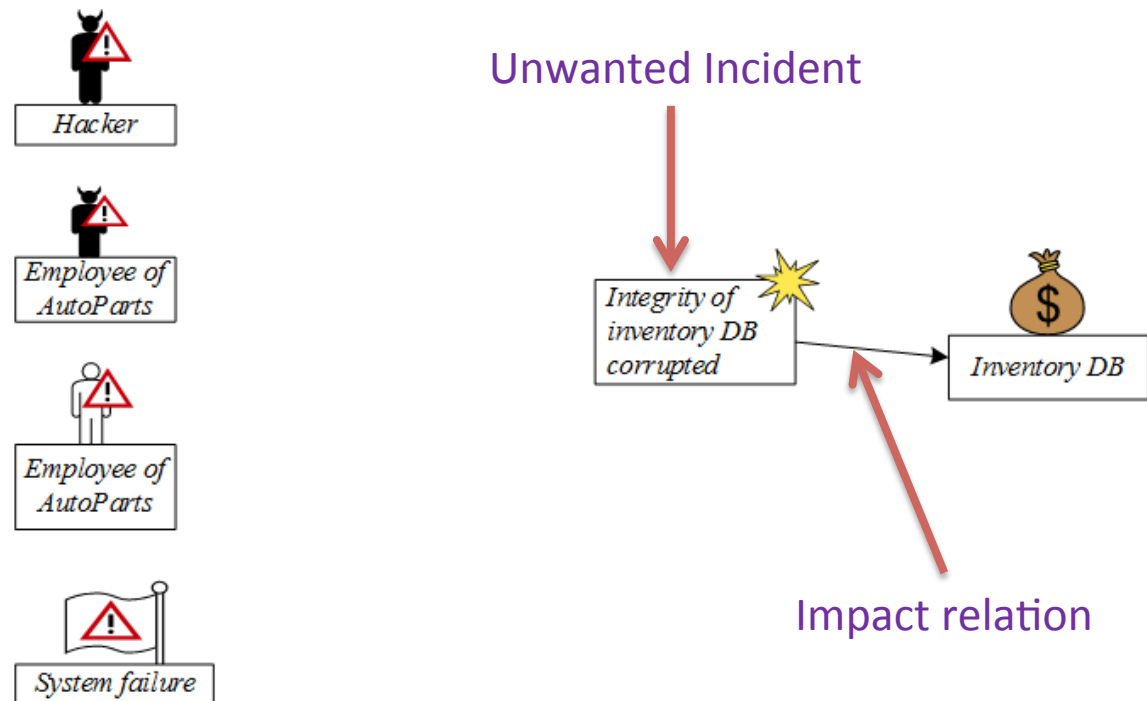
# Step 5.1: Identify Assets and Threats

- **Answer the question: “What are the threats?”**
  - Hints:
    - “Accidental threat”: e.g., users/ roles inside the system
    - “Deliberate threat”: e.g, attackers from outside



# Step 5.2: Identify Unwanted Incidents

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

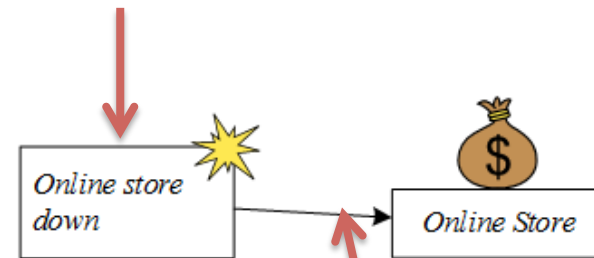


# Step 5.2: Identify Unwanted Incidents (II)

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



Unwanted Incident

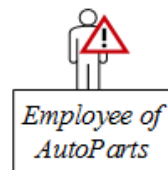


Impact relation

# Step 5.2: Identify Unwanted Incidents

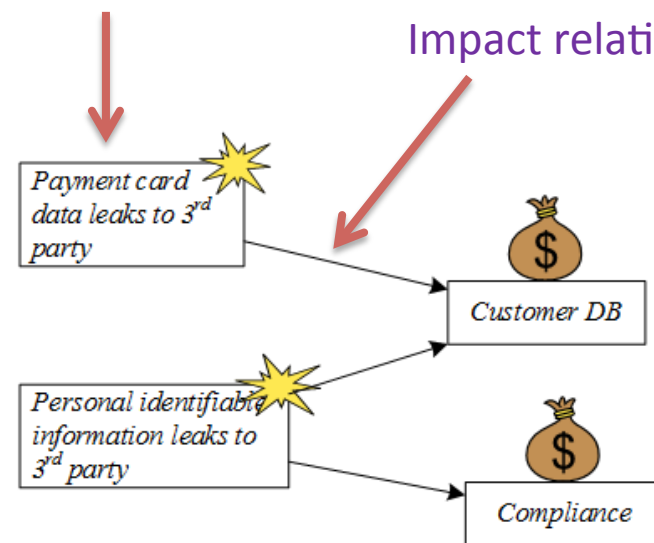
- **Answer the question:**

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



Unwanted Incident

Impact relation



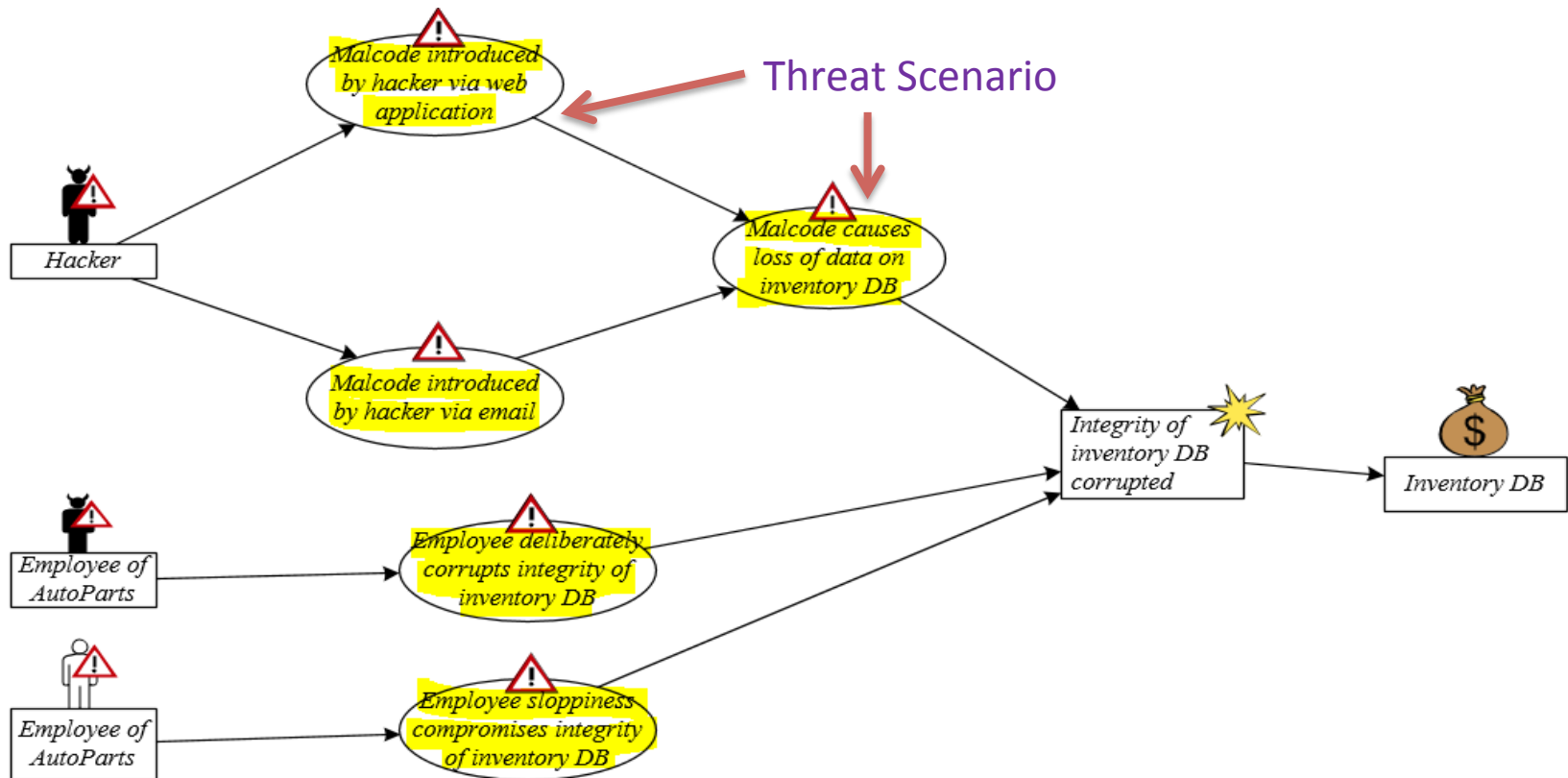
# Step 5.3: Identify Threat Scenarios

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



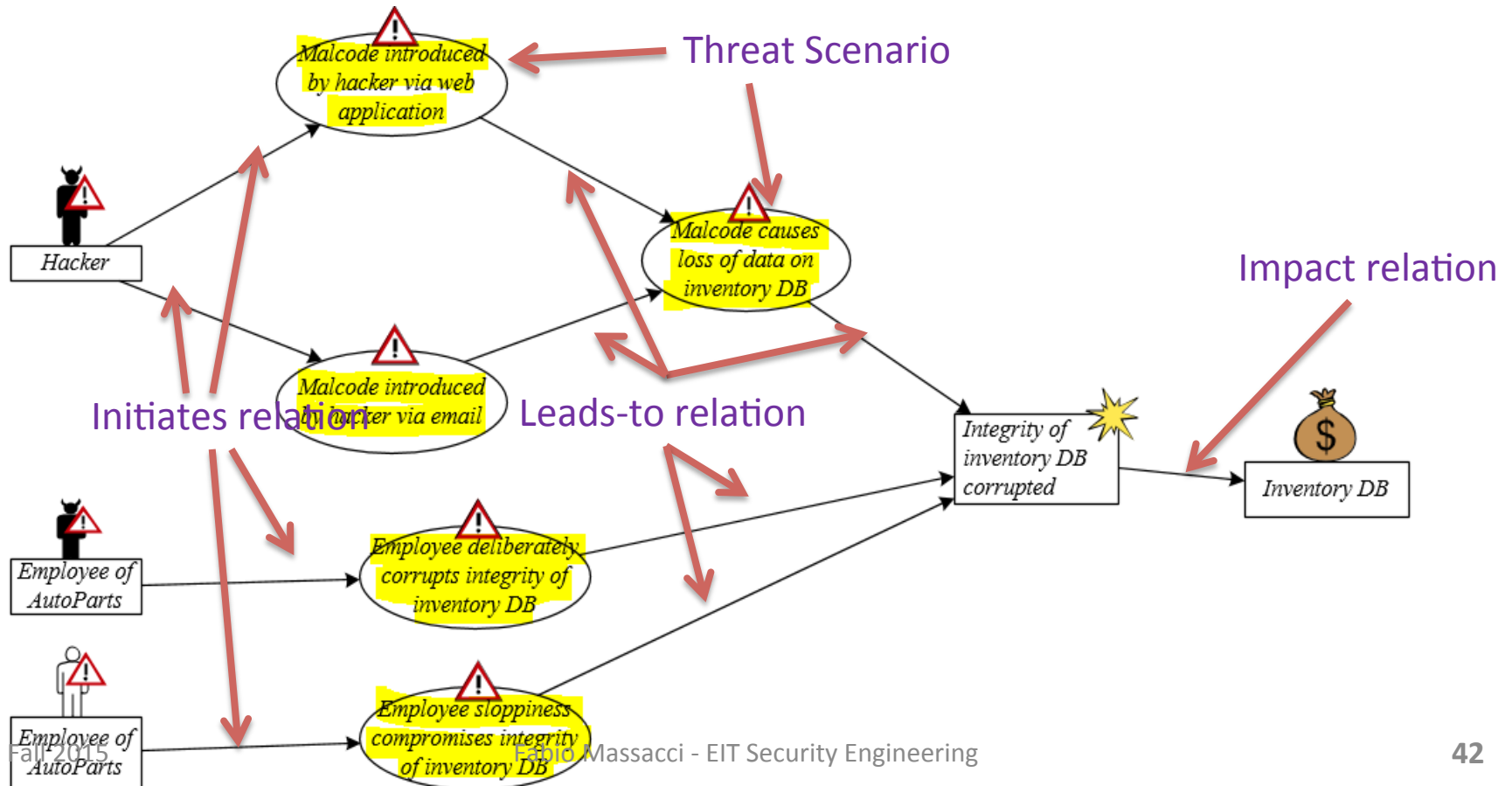
# Step 5.3: Identify Threat Scenarios

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



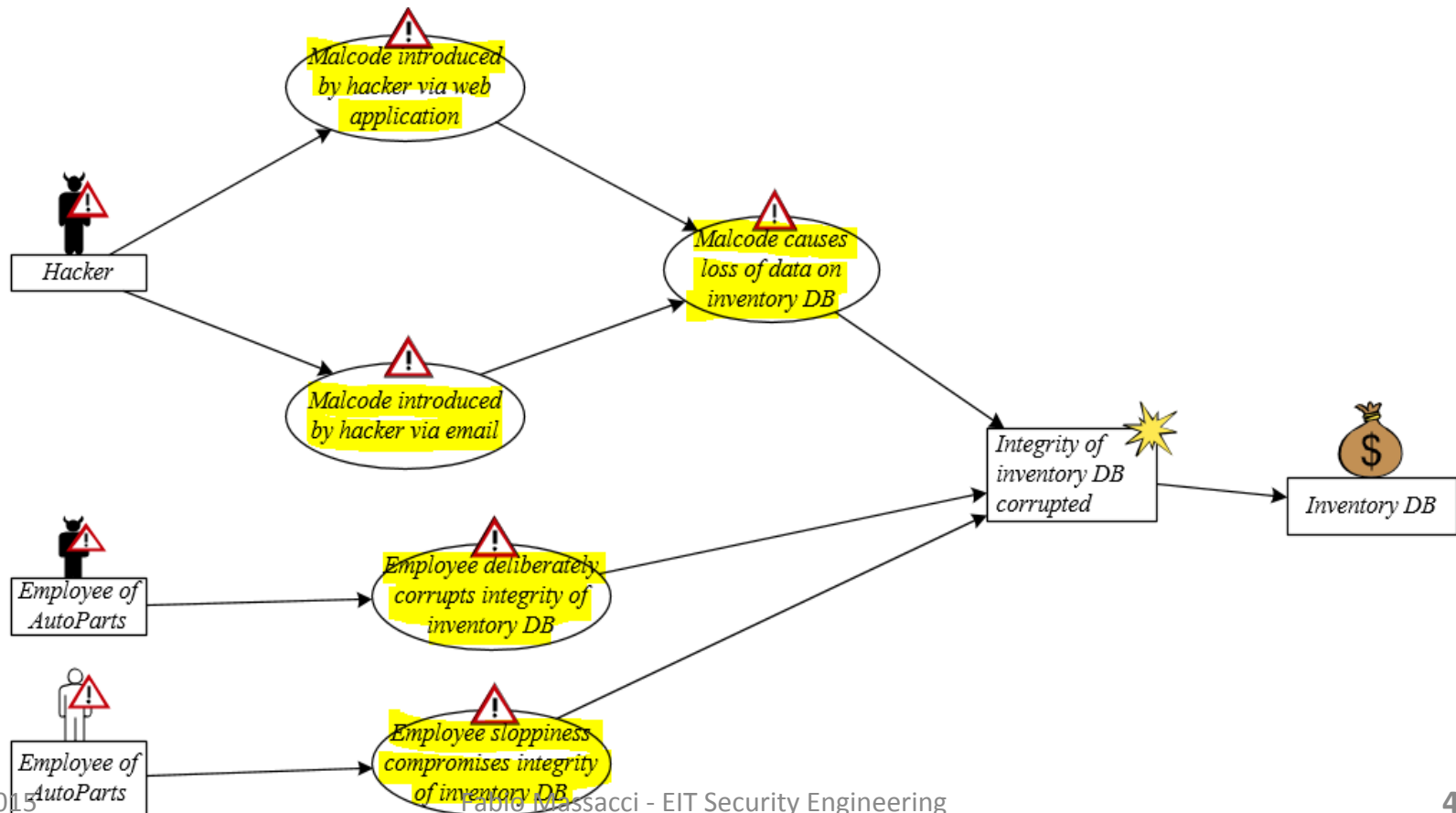
# 5.3: Identify Threat Scenarios

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

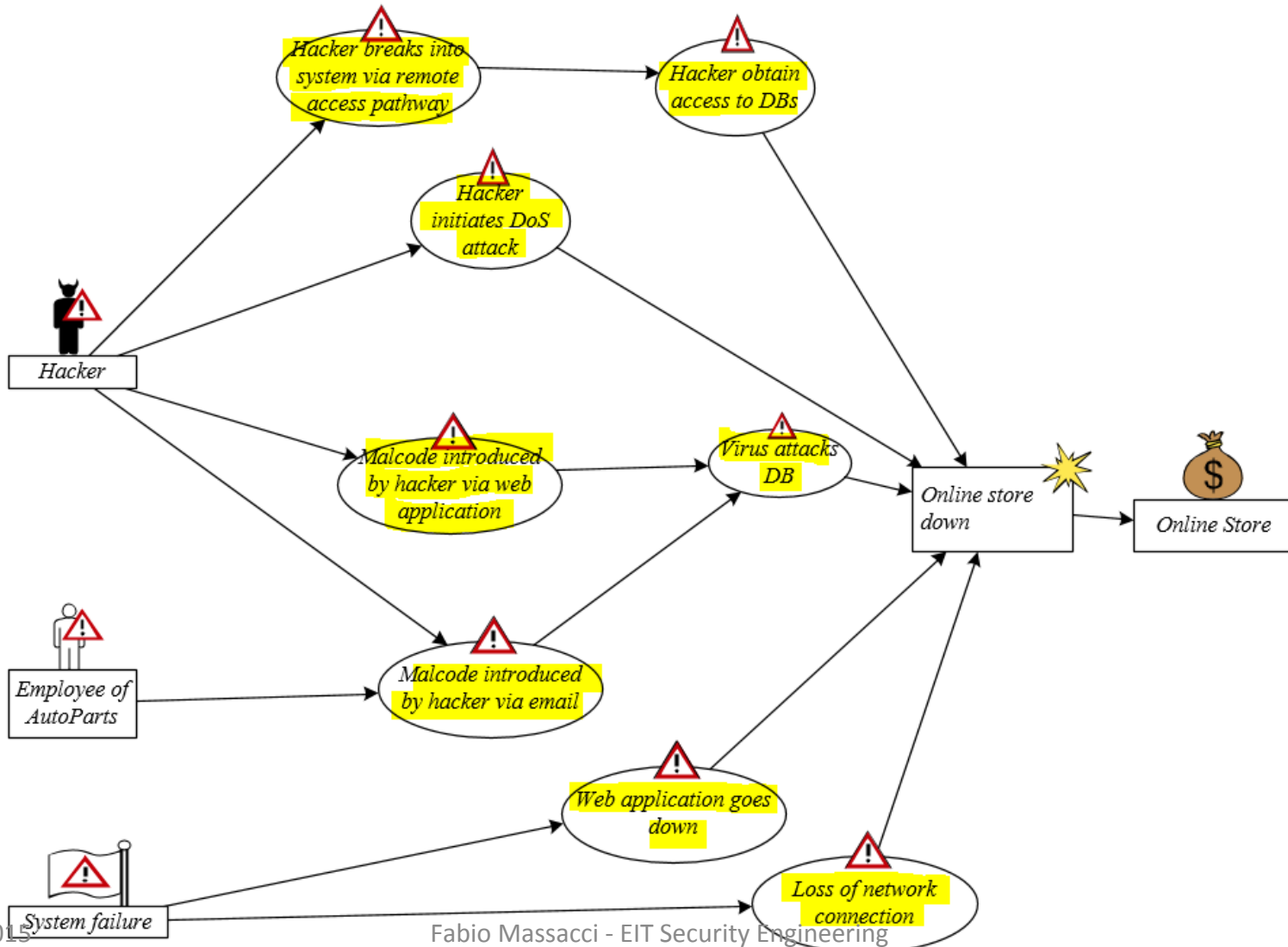


# 5.3: Identify Threat Scenarios

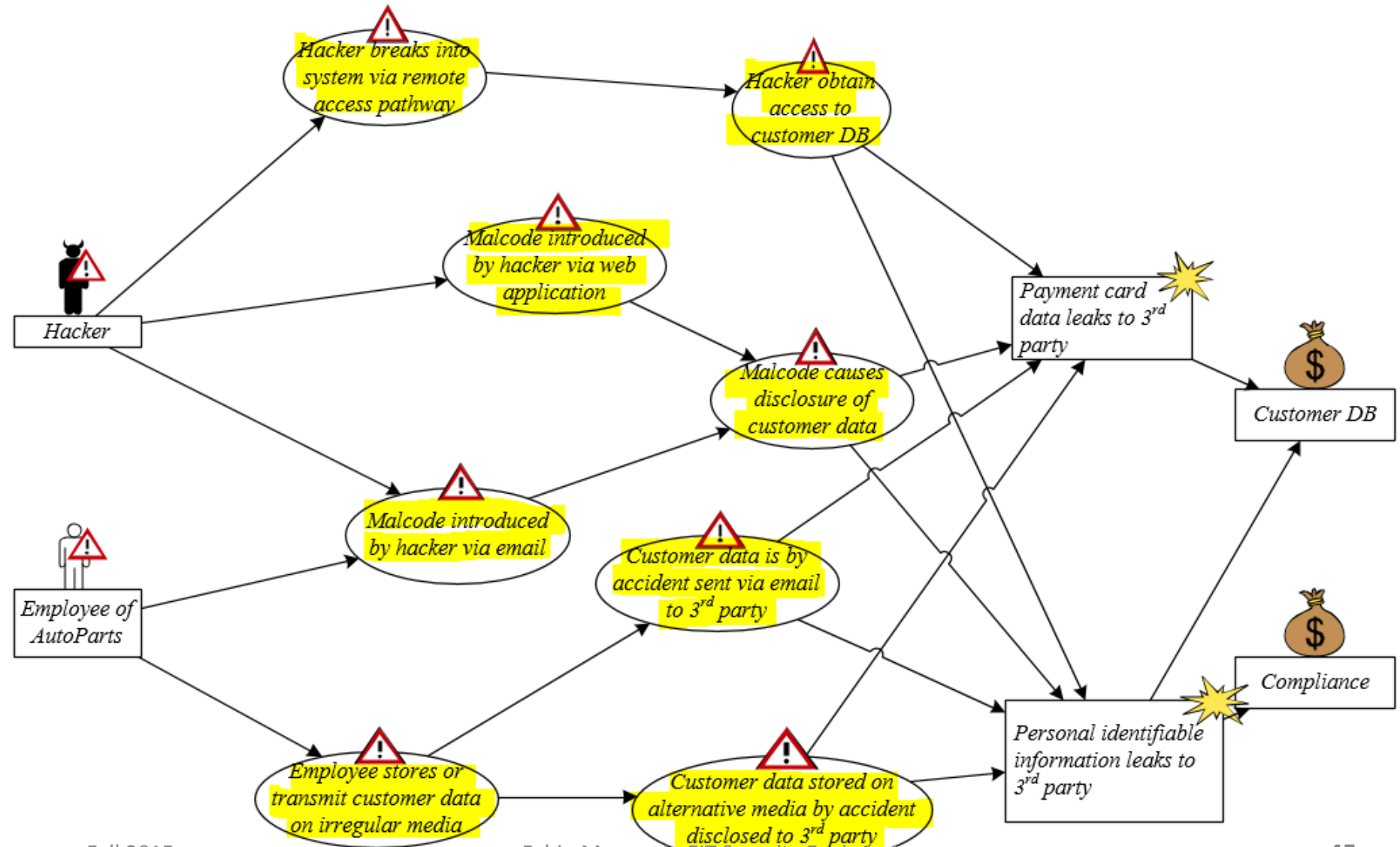
- **Answer the question:**
  - How does it happen? It happens by which threat scenarios?



# 5.3: Identify Threat Scenarios

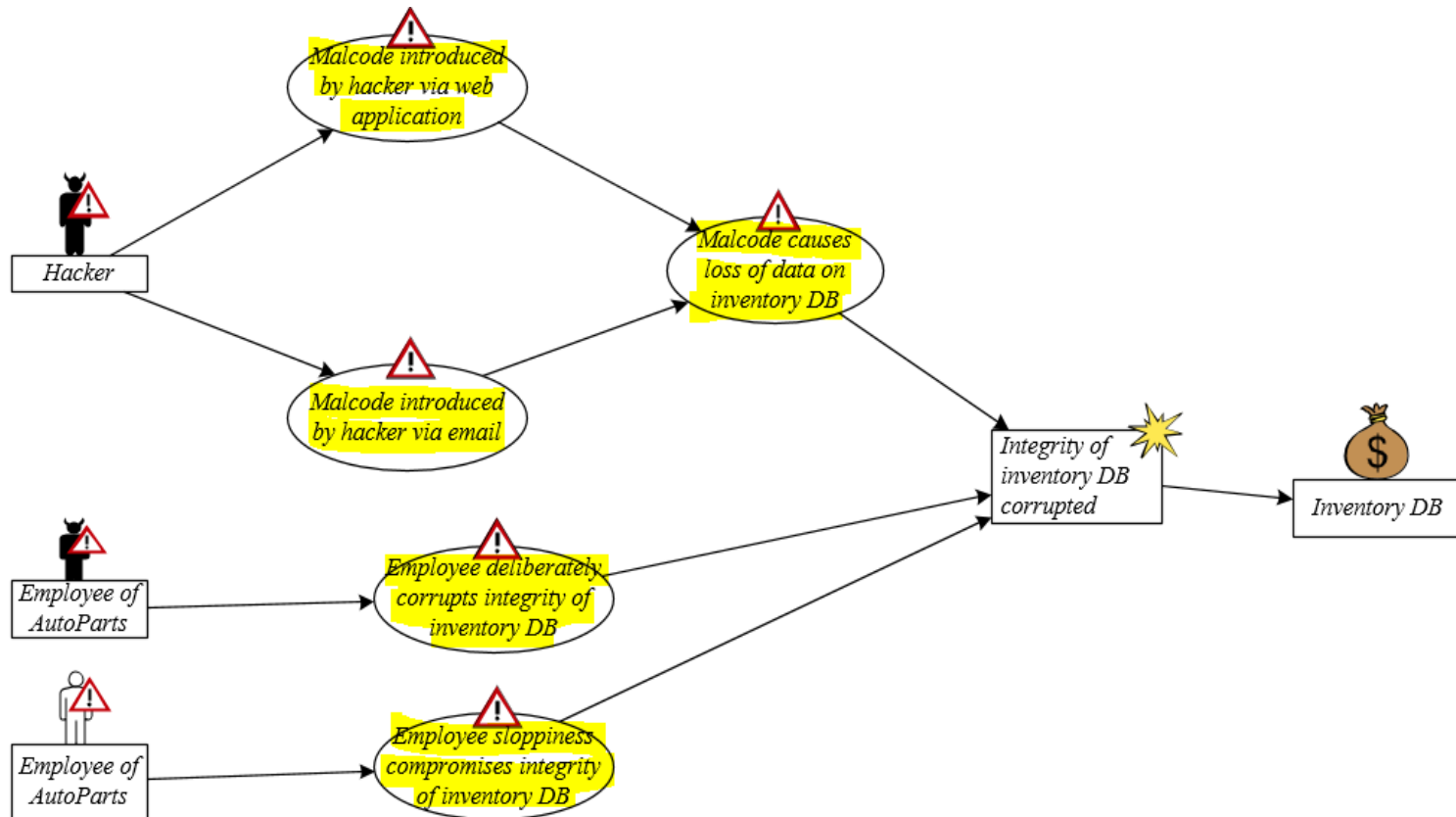


# 5.3: Identify Threat Scenarios

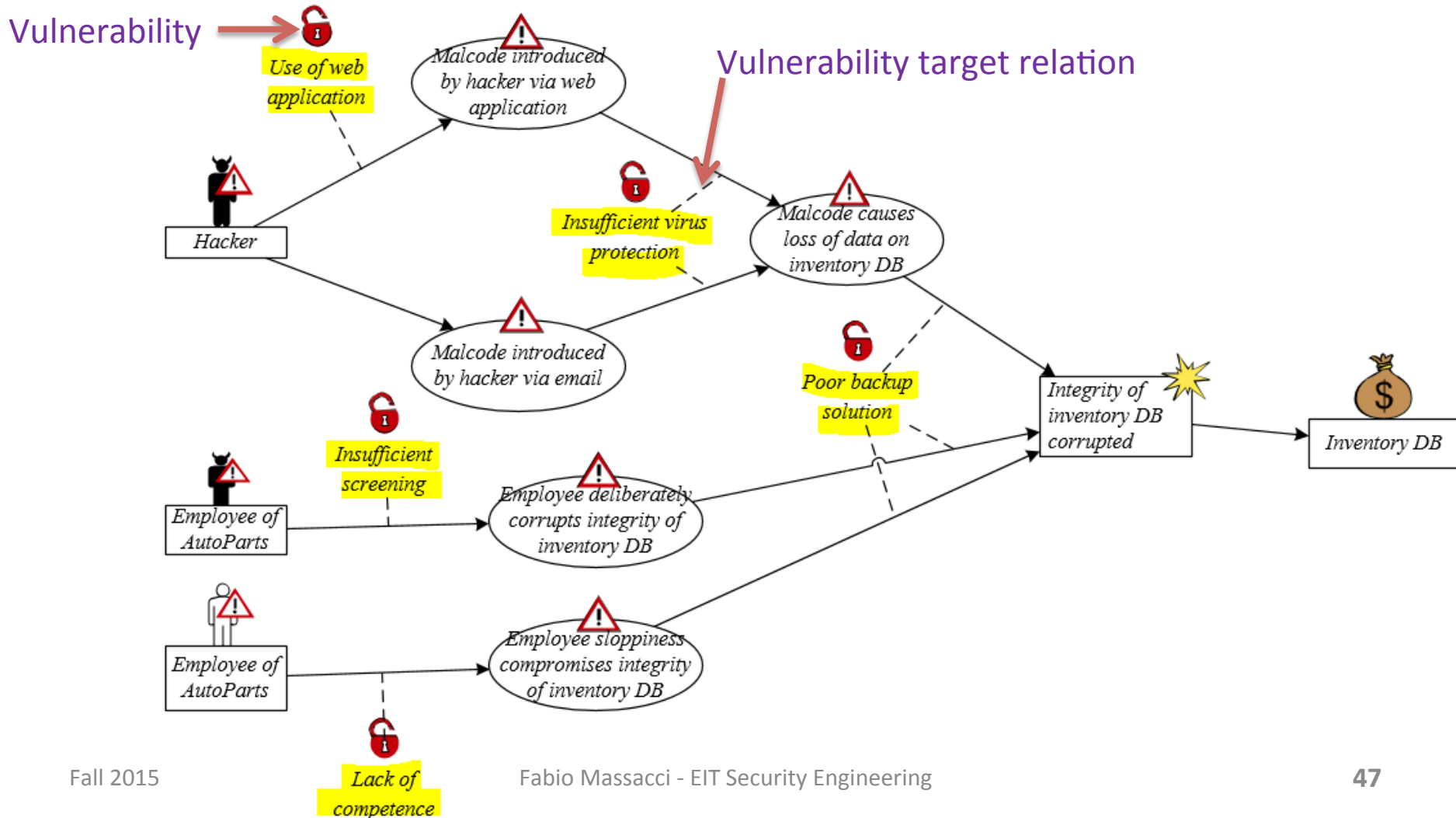


# 5.4: Identify Vulnerabilities

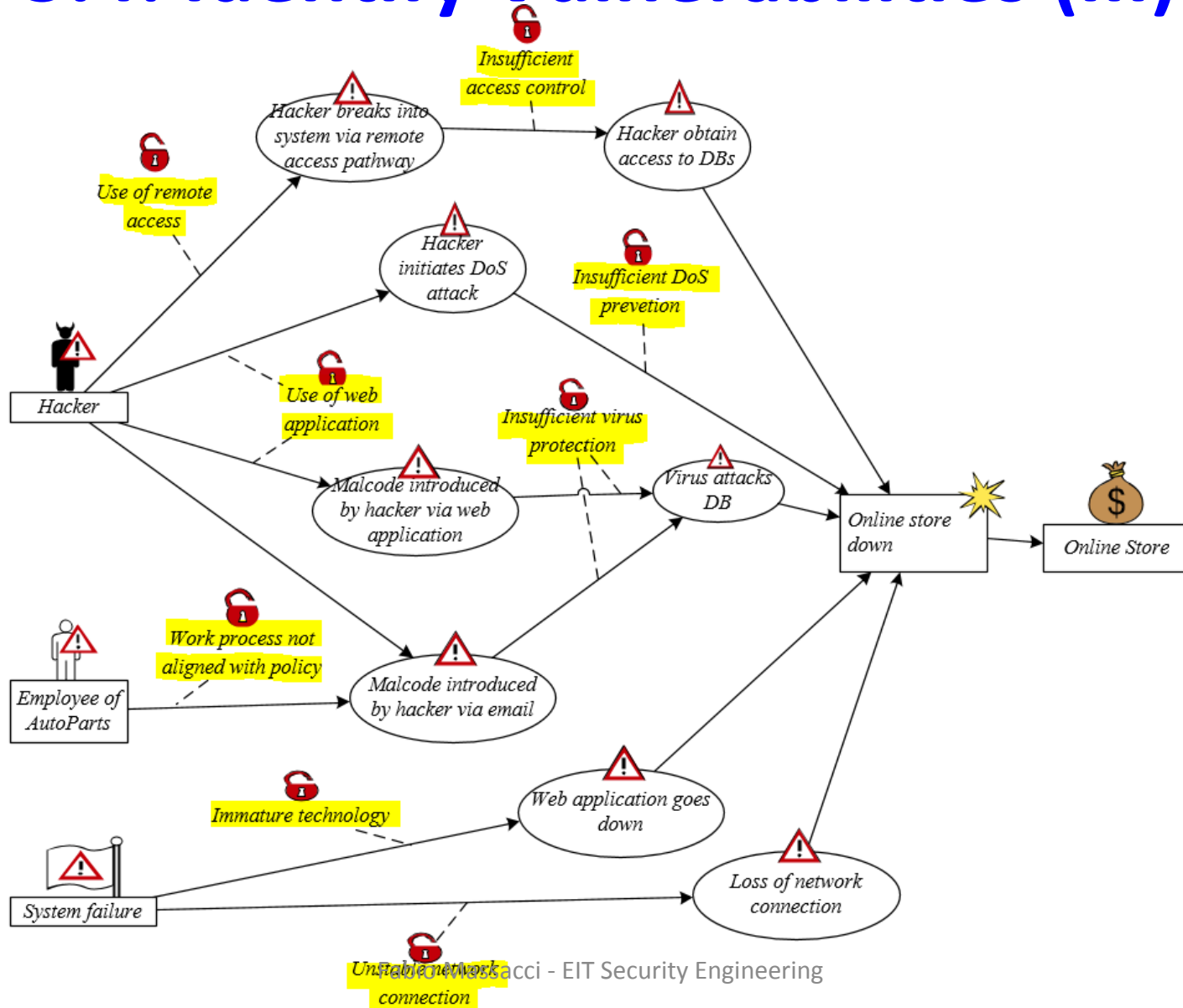
- **Answer the question:**
  - Which vulnerabilities make this possible?



# 5.4: Identify Vulnerabilities (II)

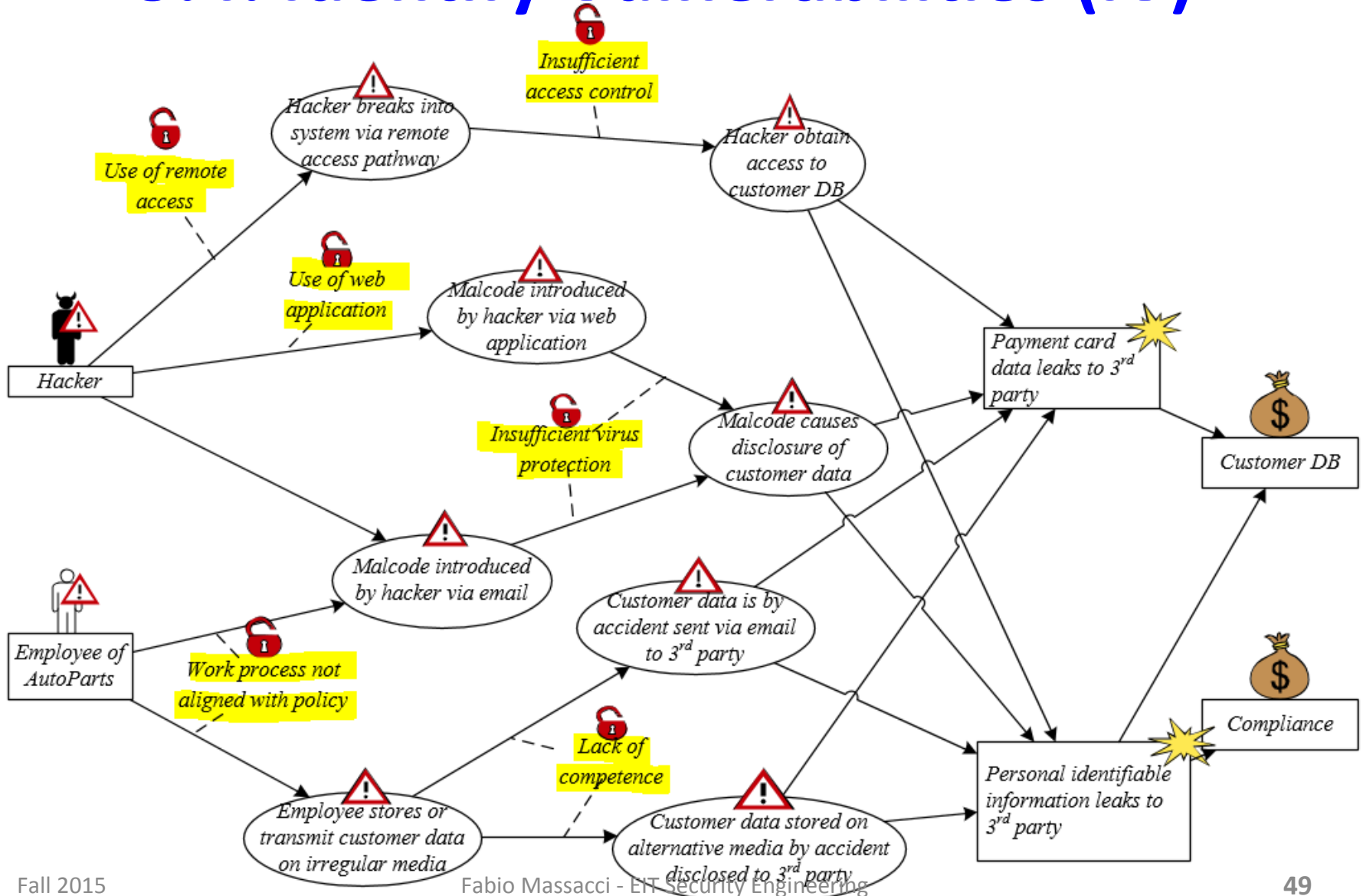


# 5.4: Identify Vulnerabilities (III)





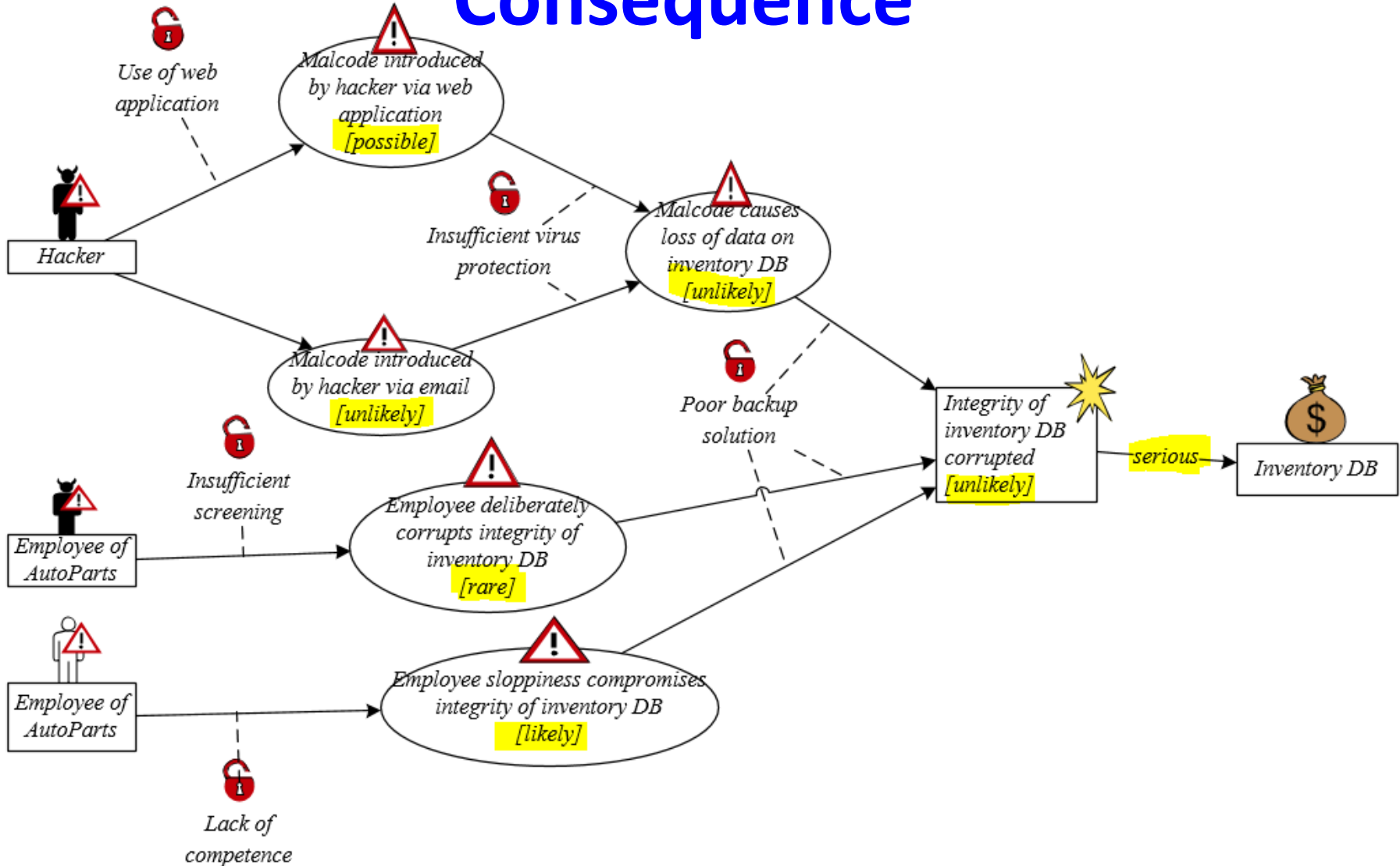
# 5.4: Identify Vulnerabilities (IV)



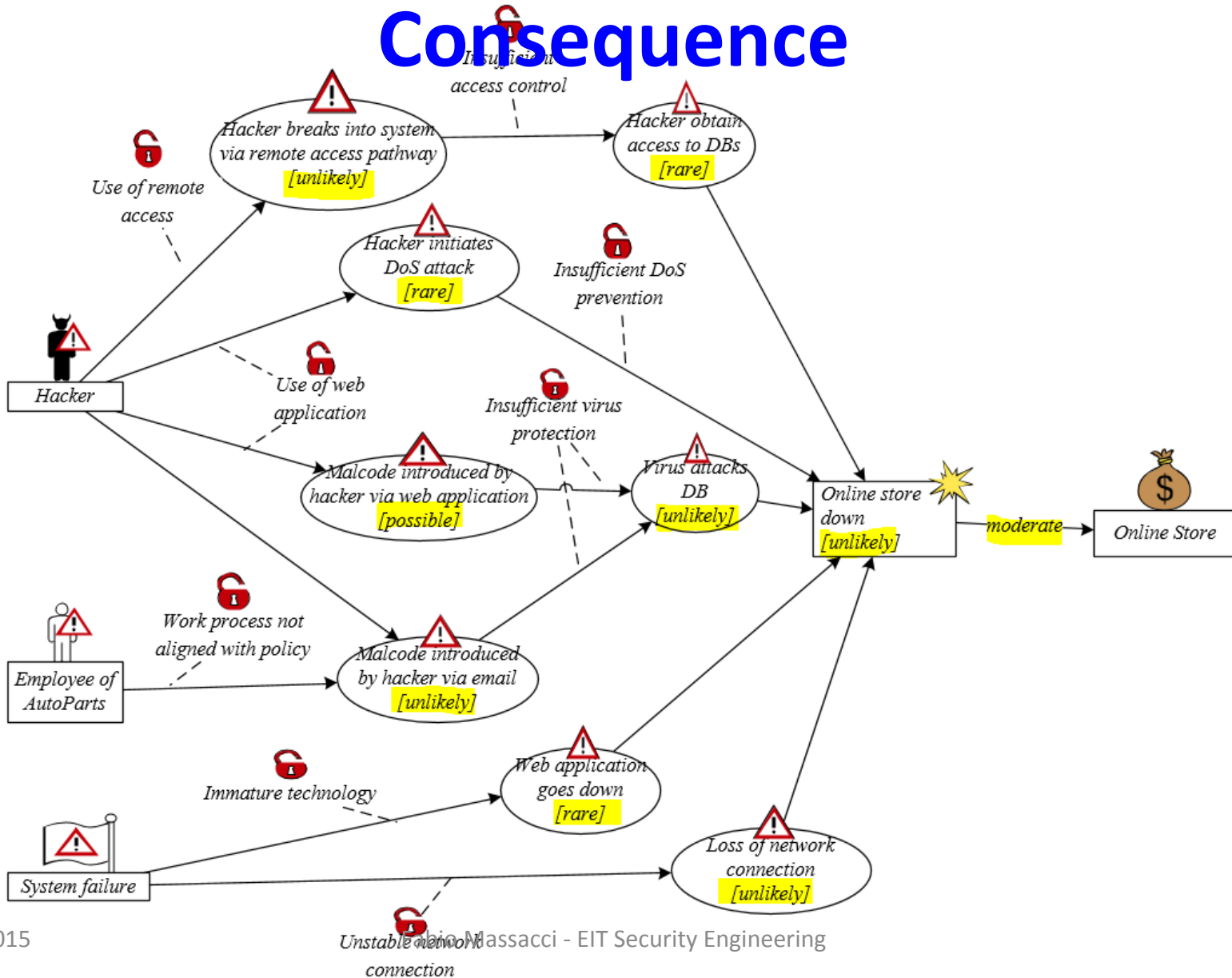
# 6: Risk estimation using threat diagrams

- ***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

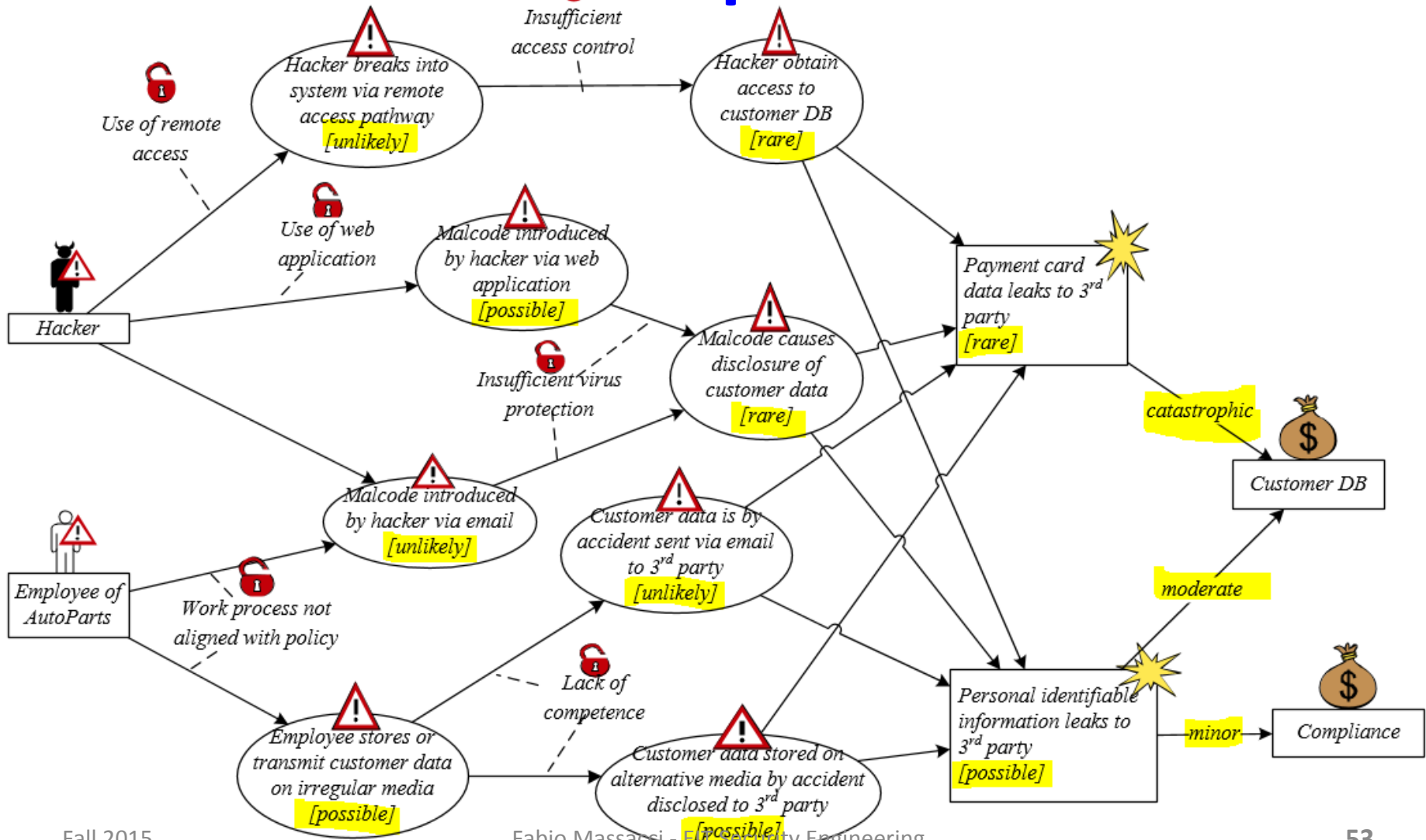
# Example: Assign Likelihood and Consequence



# Example: Assign Likelihood and Consequence



# Example: Assign Likelihood and Consequence



# 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	Acceptable	Acceptable	Monitor	Need to be treated	Need to be treated
Unlikely	Acceptable	Acceptable	Monitor	Need to be treated <i>R1: Integrity of inventory DB corrupted</i>	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	Acceptable	Acceptable	Monitor	Need to be treated	<i>R3: Payment card data leaks to 3<sup>rd</sup> party</i>
Unlikely	Acceptable	Acceptable	Monitor	Need to be treated	
Possible	Acceptable	Acceptable	<i>R4: Personal identifiable information leaks to 3<sup>rd</sup> party</i>	Need to be treated	
Likely	Acceptable	Monitor	Monitor	Need to be treated	
Certain	Need to be treated	Need to be treated	Need to be treated	Need to be treated	

	Acceptable
	Monitor
	Need to be treated

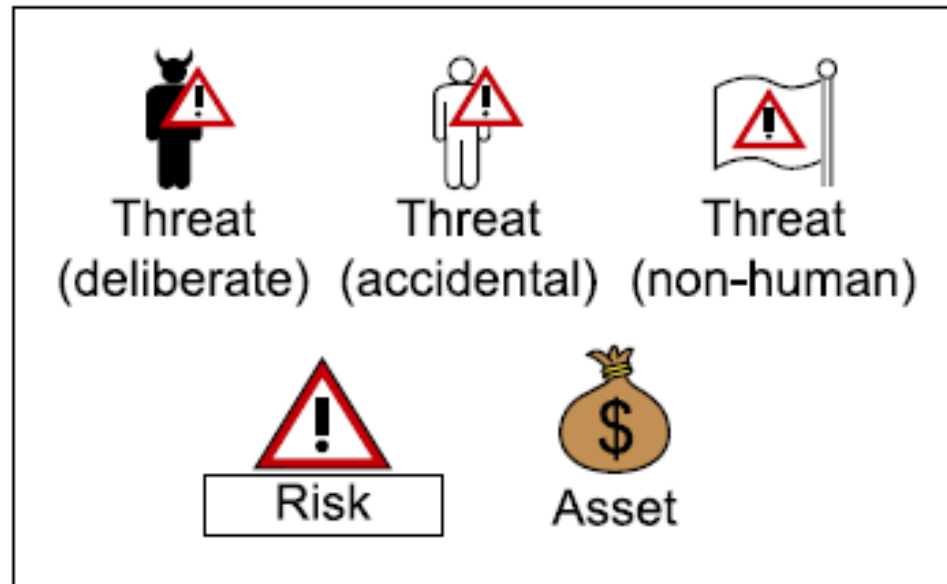
# Example: Completed Risk Function

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	Acceptable <i>R5: Personal identifiable information leaks to 3<sup>rd</sup> 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

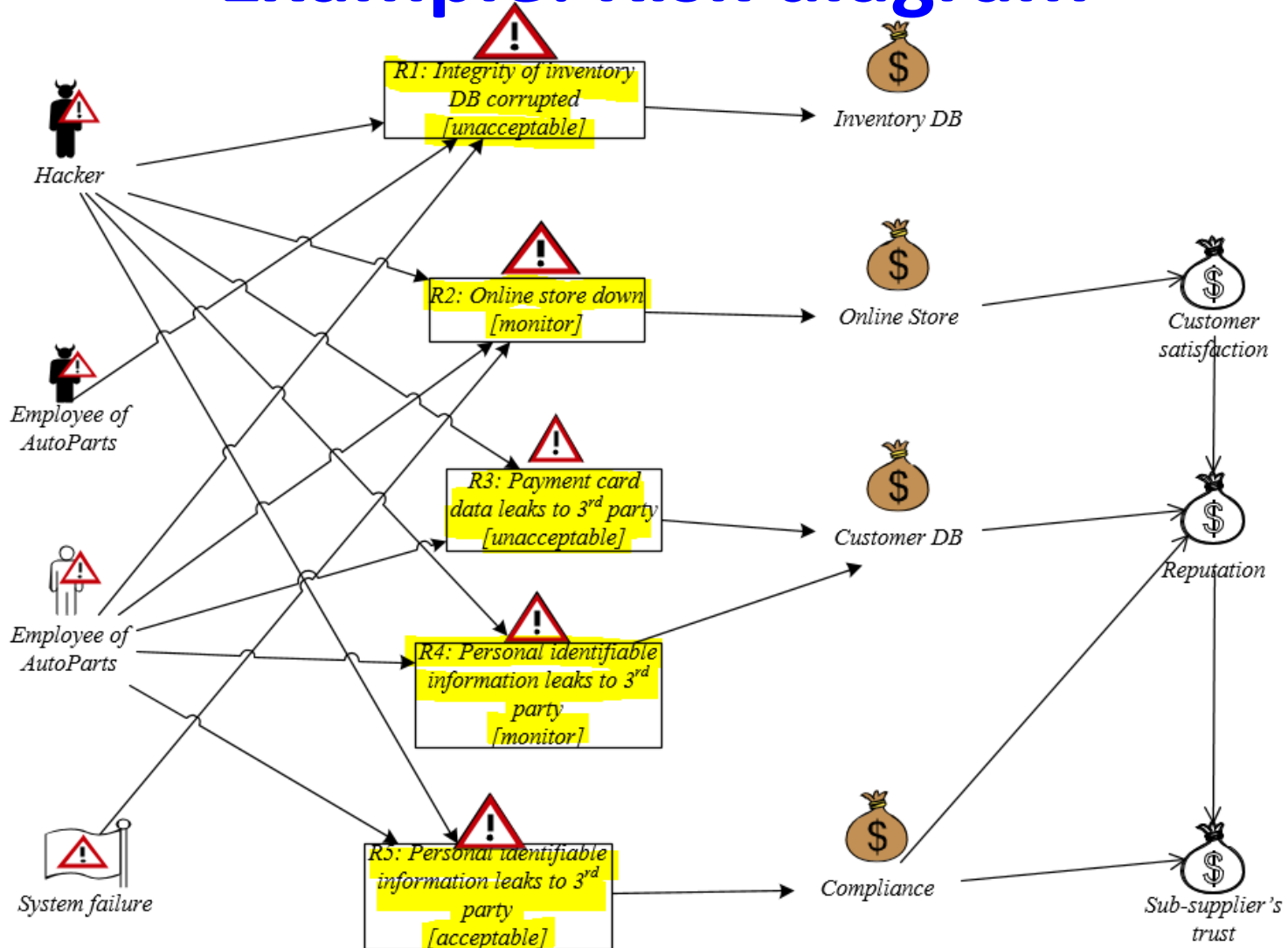


# Summarizing the Risk picture

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



# Example: Risk diagram

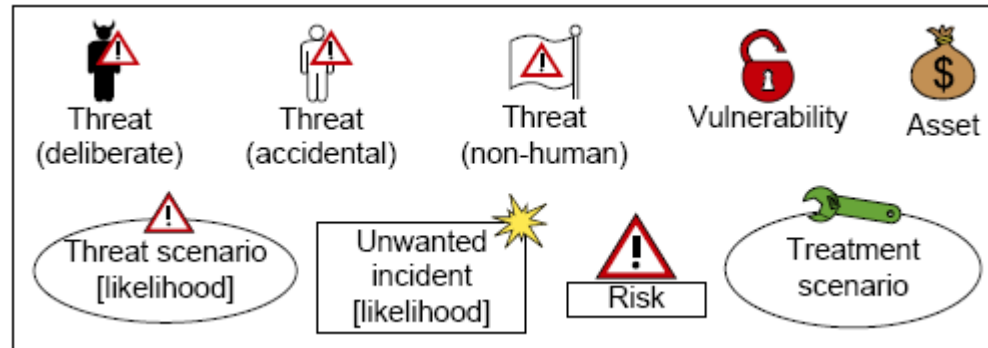


# 8: Risk treatment using Treatment diagram

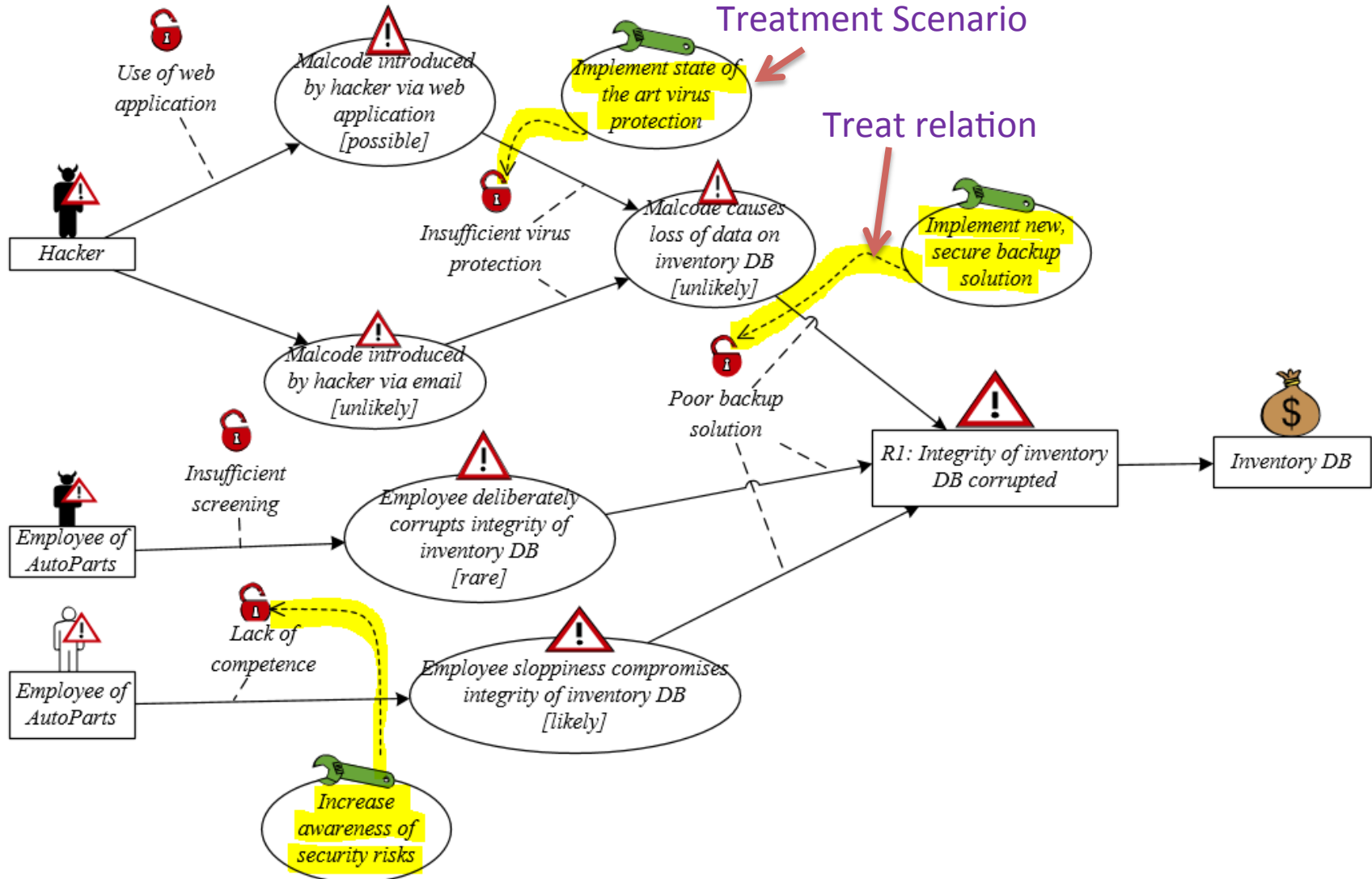
- **Objective: identify cost effective treatments for the unacceptable risks**
- **Task:**
  - Identify Treatment Scenario for unacceptable risks:
    - What can we do to reduce the risks to an acceptable (or monitor) level?
  - Create Treatment diagram
  - Summarize by Treatment Overview diagram
  -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

# 8: Risk treatment using treatment diagram

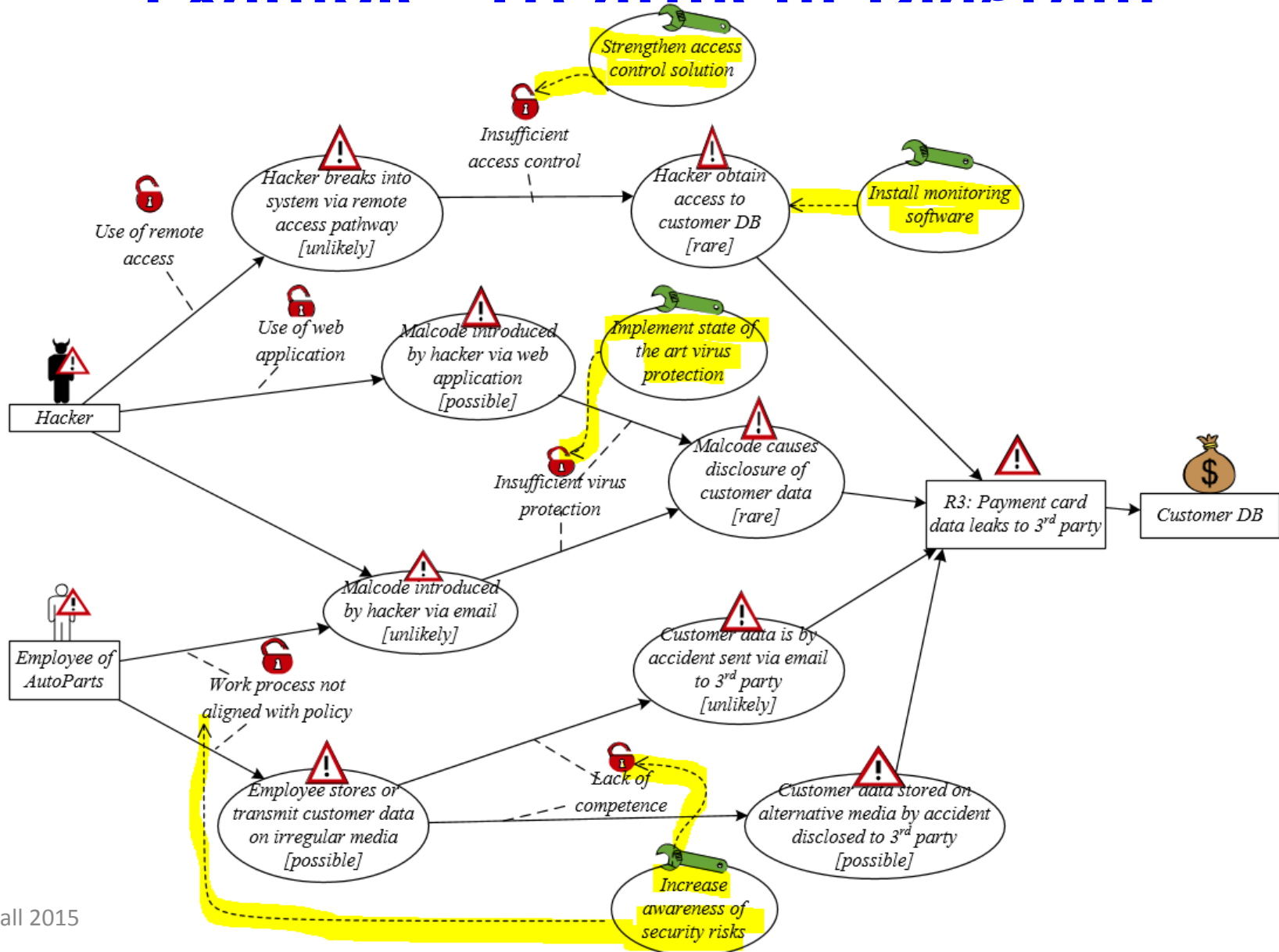
- *Notions to be used in Treatment Diagram*



# Example: Treatment Diagram

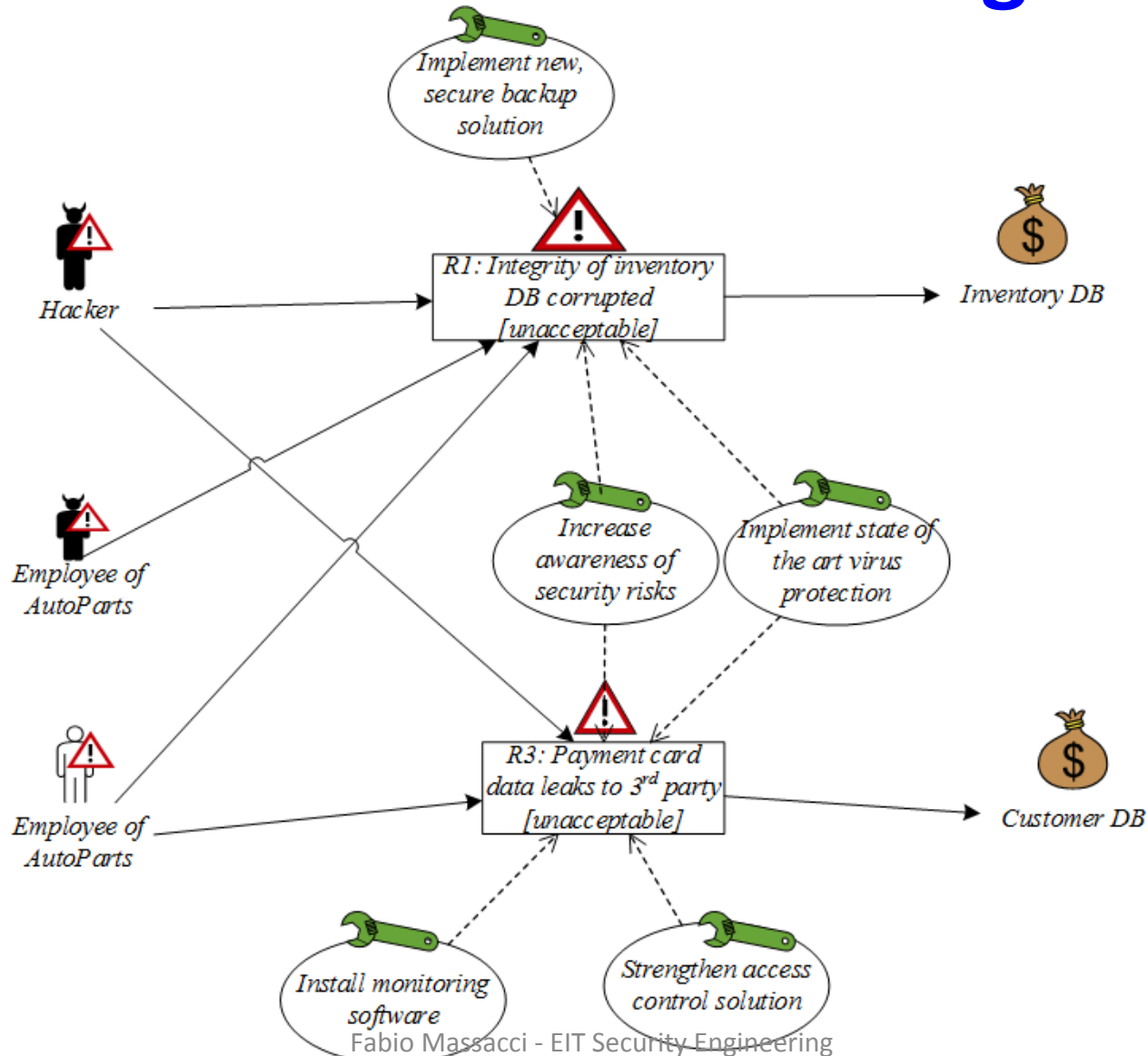


# Example Treatment Diagram





# 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

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
		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

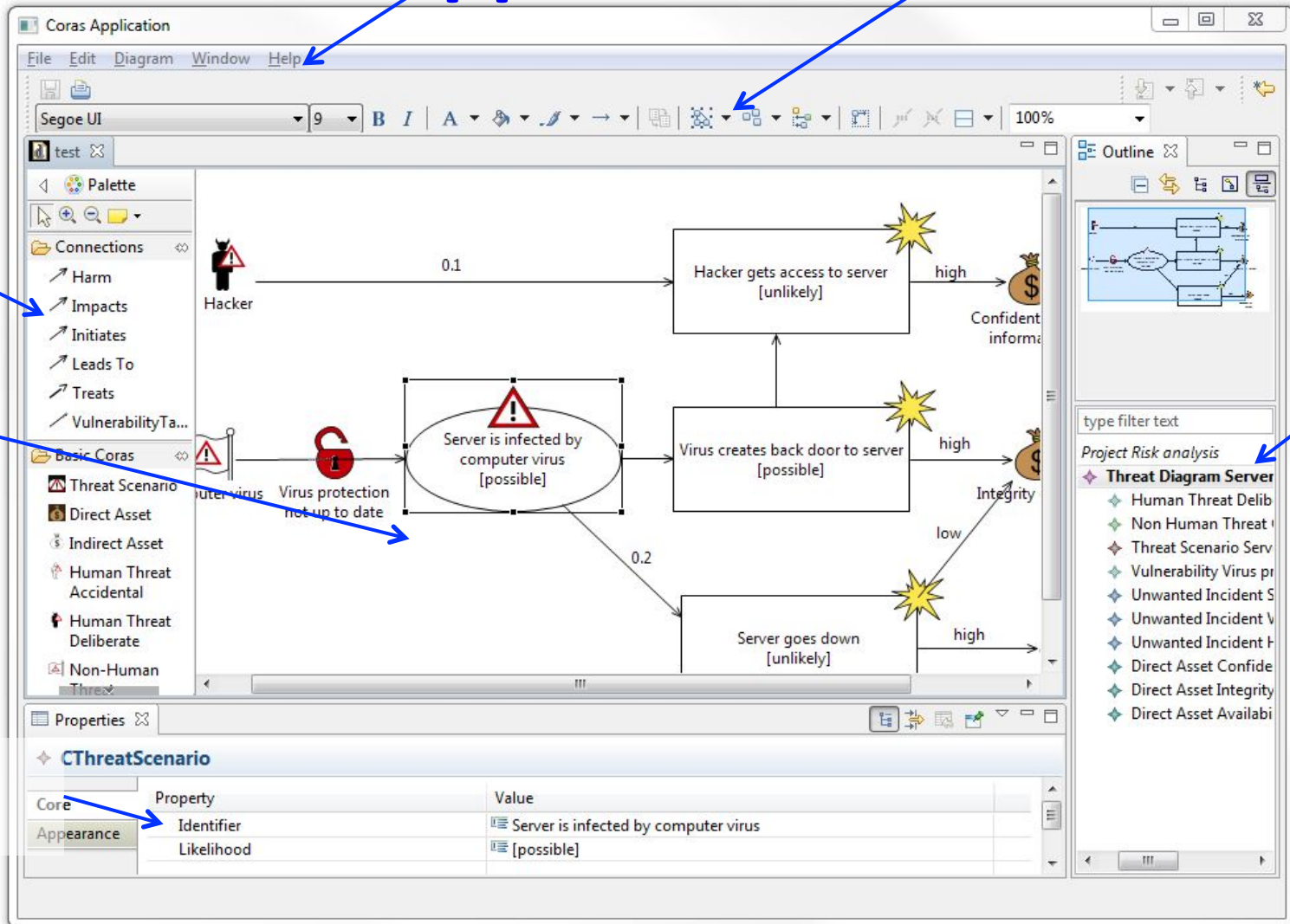
- ***The CORAS tool is a diagram editor***
- ***Support for making all kinds of CORAS diagrams***
- ***Design for on-the-fly modeling during structured brainstorming at analysis workshops***
- ***Ensures syntactically correct diagrams***
- ***Used during all steps of the risk analysis***
  - Input to 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

Palette

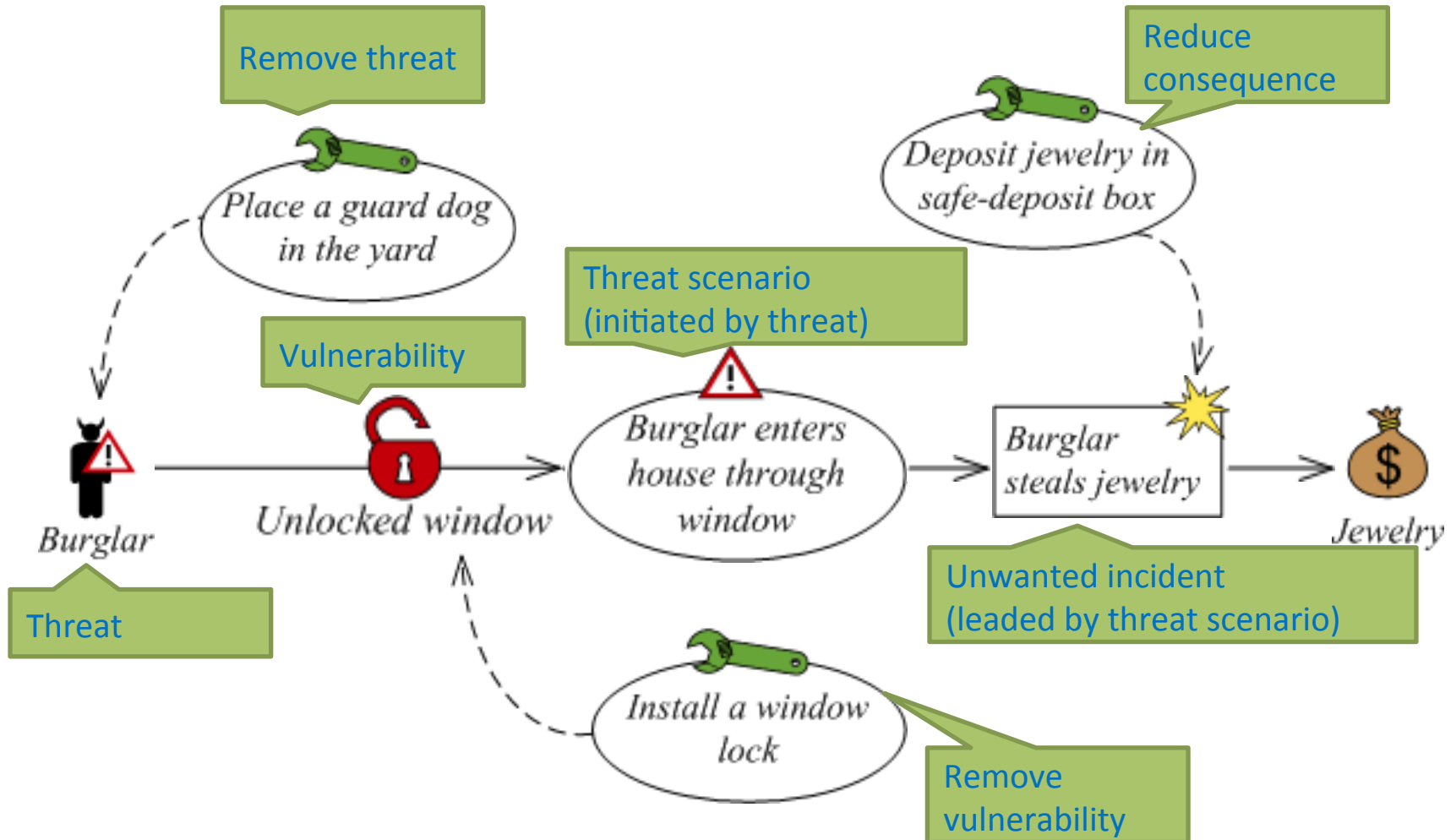
Canvas

Properties window



Outline

# Summary



# 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 ISO 31000***
  
- ***Book: <http://www.springer.com/computer/swe/book/978-3-642-12322-1>***
  - The Introduction Chapter is free!
- ***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.***