

# **CYBECO**

## **Supporting Cyber-insurance from a Behavioural Choice Perspective**

### **D4.2: Use-Case Evaluation of the Methodology and Framework**

Dissemination Level		
PU	Public	x
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

## D4.2: Use-Case Evaluation of the Methodology and Framework

### Document Status

<b>Document Title</b>	Use-Case Evaluation of the Methodology and Framework
<b>Version</b>	1.0
<b>Work Package</b>	4
<b>Deliverable #</b>	4.2
<b>Prepared by</b>	Deepak Subramanian, Mathieu Cousin (AXA)
<b>Contributors</b>	Caroline Baylon (AXA)
<b>Checked by</b>	UNN (Dawn Branley-Bell, Pam Briggs, Lynne Coventry)
<b>Approved by</b>	TREK
<b>Date</b>	30/04/2019
<b>Confidentiality</b>	PU

## D4.2: Use-Case Evaluation of the Methodology and Framework

### Document Change Log

Each change or set of changes made to this document will result in an increment to the version number of the document. This change log records the process and identifies for each version number of the document the modification(s) which caused the version number to be incremented.

Change Log	Version	Date
First draft referring only to model	0.1	Feb 7, 2019
First draft including complete structure	0.2	Mar 7, 2019
First draft content complete	0.3	Apr 5, 2019
Reviewed by UNN	0.4	Apr 16, 2019
UNN comments incorporated	0.5	Apr 20, 2019
Final check and finalization	1.0	Apr 30, 2019

## Table of Contents

### Part I: Validating the model, using the cyber-insurance scenarios

1	Introduction .....	8
1.1	Objective and Scope .....	8
1.2	Chapter Structure .....	8
1.3	Terminology .....	8
2	Approach and Analysis .....	10
2.1	Overview of the model.....	10
2.2	Analysis of Use-cases.....	10
2.2.1	Use-case 1: Cyber-insurance selection for an SME .....	10
2.2.2	Use-case 2: Loss of PII for a large company in a financial sector.....	12
2.2.3	Use-case 3: Insurance fraud for an SME in the professional services sector....	14
2.2.4	Use-case 4: Products / Services Manipulation for a large company in the manufacturing sector .....	17
2.2.5	Use-case 5: Insufficient insurance coverage for an SME operating in the IT industry sector .....	18
2.2.6	Use-case 6: Accumulation of cyber-incidents following a single large-scale attack with involvement of reinsurance in the claim process.....	21
3	Conclusion .....	23
4	Introduction .....	25
4.1	Objective and Scope .....	25
4.2	Chapter Structure .....	25
5	Cyber-insurance scenarios .....	26
5.1	Scenario 1: Loss of personally identifiable data for a large company in the financial sector	26
5.2	Scenario 2: Insurance fraud for an SME in the professional services sector .....	32
5.3	Scenario 3: Manipulation of Products / Services for a large company in the manufacturing sector.....	36
6	Approach and Analysis .....	41
6.1	Overview of the toolbox.....	41
6.2	Analysis of Use-cases.....	41

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

6.2.1	Scenario 1: Loss of personally identifiable data for a large company in the financial sector .....	41
6.2.2	Scenario 2: Insurance fraud for an SME in the professional services sector ....	42
6.2.3	Scenario 3: Manipulation of Products / Services for a large company in the manufacturing sector .....	45
7	Conclusion .....	46
8	Introduction .....	48
9	Expert review of October 2018 .....	49
9.1	Objective .....	49
9.2	Method .....	49
9.3	Feedback .....	49
10	Areas for improvement .....	50
10.1	Prioritised security controls .....	50
10.2	Threats and terminology .....	52
11	Conclusion .....	53
	Appendix: Tables referenced in the scenario descriptions .....	54

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

### List of Figures

Figure 1: Toulmin model argumentation for use-case 1 .....	12
Figure 2: Cyber-security objectives specification (ref. Figure 9 D3.1).....	13
Figure 3: Toulmin model argumentation for use-case 2 .....	14
Figure 4: Toulmin model argumentation for use-case 3 .....	16
Figure 5: Attacker model in ARA (Ref. D3.1).....	17
Figure 6: Toulmin model argumentation for use-case 4 .....	18
Figure 7: Toulmin model argumentation for use-case 5 .....	20
Figure 8: Toulmin model argumentation for use-case 6 .....	22
Figure 9: CYBECO toolbox - large companies .....	42
Figure 10: CYBECO toolbox input for scenario 2 .....	43
Figure 11: CYBECO toolbox simulation for scenario 2 .....	44

## **Part I:**

### **Validating the model using the cyber-insurance scenarios**

#### **Abstract:**

In order to assess the risk calculation methodology and toolbox, and also to make it possible to incorporate the behavioural components into this methodology, it is necessary to understand the interactions between the parties in the cyber-insurance process through a set of use cases that are sufficiently representative of the global cyber-insurance ecosystem. The use cases presented in this documented are based on the analysis of the value chain for a given company, and the associated assets, and provide the basis for more in-depth cyber-insurance scenarios in this work package.

# 1 Introduction

## 1.1 Objective and Scope

This section provides an overview of the model and provides an analysis of the model over the three use-cases that were defined in the document referenced as D4.1. The scope of the evaluation is limited to the cyber-insurance scenarios defined in D4.1 and the analysis is not exhaustive in nature. This is in-line with the key objective of the analysis, which is to check the minimum level of viability of the model, rather than its ability to handle all complex insurance requirements.

## 1.2 Chapter Structure

This section, Section 1, provides a general introduction to the evaluation of the model and the scope of the evaluation. The second section provides the details of the validation of the model and the third section provides a general conclusion to the model.

## 1.3 Terminology

The following table provides the definitions of terms and concepts used throughout the document.

Table 0-1. Terminology

Value chain	The process by which businesses receive raw materials, add value to the raw materials through various processes to create a finished product, and then sell that end product to customers. The value chain disaggregates an industry into its strategically relevant processes to understand the activities that produce goods and services <sup>1</sup> .
Threat actor	An agent which either perpetrates a cyber-attack or sponsors it by providing funding, technical support, etc.

---

<sup>1</sup> Competitive Advantage: Creating and Sustaining Superior Performance, *Michael E. Porter*, Ed. Simon and Schuster, New York, 1985



#### D4.2: Use-Case Evaluation of the Methodology and Framework

Market segment	Defined in this document by the size of the company; this should not be confused with the more general definition based on the client segmentation of the market.
Market sectors	The classification of companies according to the set of activities they are involved in; they can be grouped into distinguishable industries or groups of similar industries. Market sectors can be defined according to specific needs, and can also use standard classifications of industries such as the Global Industry Classification Standard <sup>2</sup> .

---

<sup>2</sup> Global Industry Classification Standard, Available at:  
[https://www.msci.com/documents/10199/242721/MSCI\\_Global\\_Industry\\_Classification\\_Standard.pdf/88181a98-5eff-4ac7-8409-d30474fc6429](https://www.msci.com/documents/10199/242721/MSCI_Global_Industry_Classification_Standard.pdf/88181a98-5eff-4ac7-8409-d30474fc6429)

## 2 Approach and Analysis

### 2.1 Overview of the model

The model consists of the following components:

- An adversarial threat model for risk analysis
- A risk preference framework
- A computational logic for monetary risk estimation

These three parts form the whole of the model and they will be analyzed against the various scenarios mentioned in deliverable 4.1.

### 2.2 Analysis of Use-cases

#### 2.2.1 Use-case 1: Cyber-insurance selection for an SME

*Background:*

A SME is a small entity whose arguments for a complete security solution encompassing all needs or the provision of a tailor-made insurance policy may be impractical. These factors require the presence of less stringent testing mechanisms and a more generic framework to allow a selection of cyber-insurance. This is in line with other traditional insurance product such as property insurance where risks such as theft, fire and water damage could be chosen in an insurance scheme.

*Discussion:*

In this use case, the primary objective is to check if the model allows for flexibility in identified risks. This involves two stages:

1. Identification of the risks and controls

The model emphasizes the identification of risks as a primary motivator early in its presentation. The following risks are taken into account (ref. D3.1)

- Organizations' assets at risk
- Non-targeted threats
- Targeted threats
- Other uncertainties affecting the organization / targeted threats

---

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

### 2. Presenting the options for insurance

The model also presents the following requirements that are subsequently useful in the decision making efforts for insurance providers. These are enumerated as follows:

- Controls in place for the threats
- Impact analysis over organization's interests
- Risk appetite of the target organization

The model also explains the risk appetite of the organization in general in the risk perception indication of the organization. Taking these into consideration, it can be concluded that use-case 1 could take advantage of these elements in this model to ascertain their risk exposure. Therefore, it can be concluded that the model can definitely handle the parameter requirements of use-case 1. A Toulmin model argumentation for this claim can be found in Figure 1.

*Argumentation:*

## D4.2: Use-Case Evaluation of the Methodology and Framework

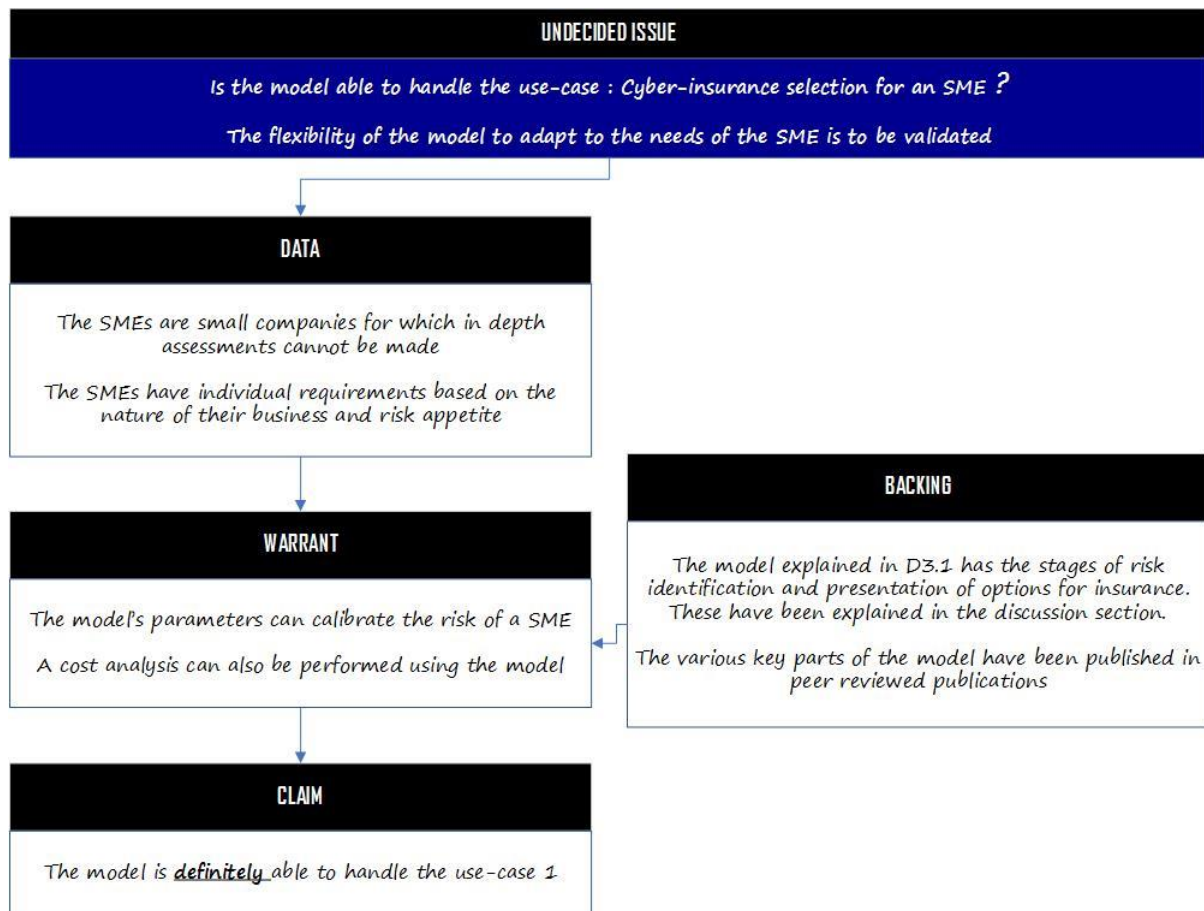


Figure 1: Toulmin model argumentation for use-case 1

### 2.2.2 Use-case 2: Loss of PII for a large company in a financial sector

#### Background:

This use-case specifically targets the large enterprises which have unique sets of requirements. In this case, the organization is also in the financial sector which typically implies a high degree of regulatory compliance requirements.

#### Discussion:

In the specification of the use-case, the attack is specifically from a non-targeted attack by random scanning with automated tools. These would be covered in “Figure 9 - Cyber-security objectives specification” in the D3.1. This is shown in Figure 2.

The probability of the attack happening is to be estimated based on the number of open ports, and the block of IPs being used. The model takes some of these factors into account

## D4.2: Use-Case Evaluation of the Methodology and Framework

and “non-targeted threats” are specifically mentioned in the model as part of the identification and controls. The adversarial threat model used in the risk analysis is able to account for such threats if performed correctly.

However, it must be mentioned that the level of detail expected in the probability estimations may require improvement. For example, the model defines that the presence of a firewall would reduce the probability of a computer virus infection to 0.005. While it is noted that it is not zero, it is our opinion that the configuration of the firewall must also be taken into account for any reduction in probability. Further, firewall is not the only control necessary from a security standpoint.

Hence, we would like to state that the model is most likely able to handle this scenario depending on the security experts’ inputs to calibrate the required parameters. An argumentation of this claim is presented using the Toulmin model in Figure 3.

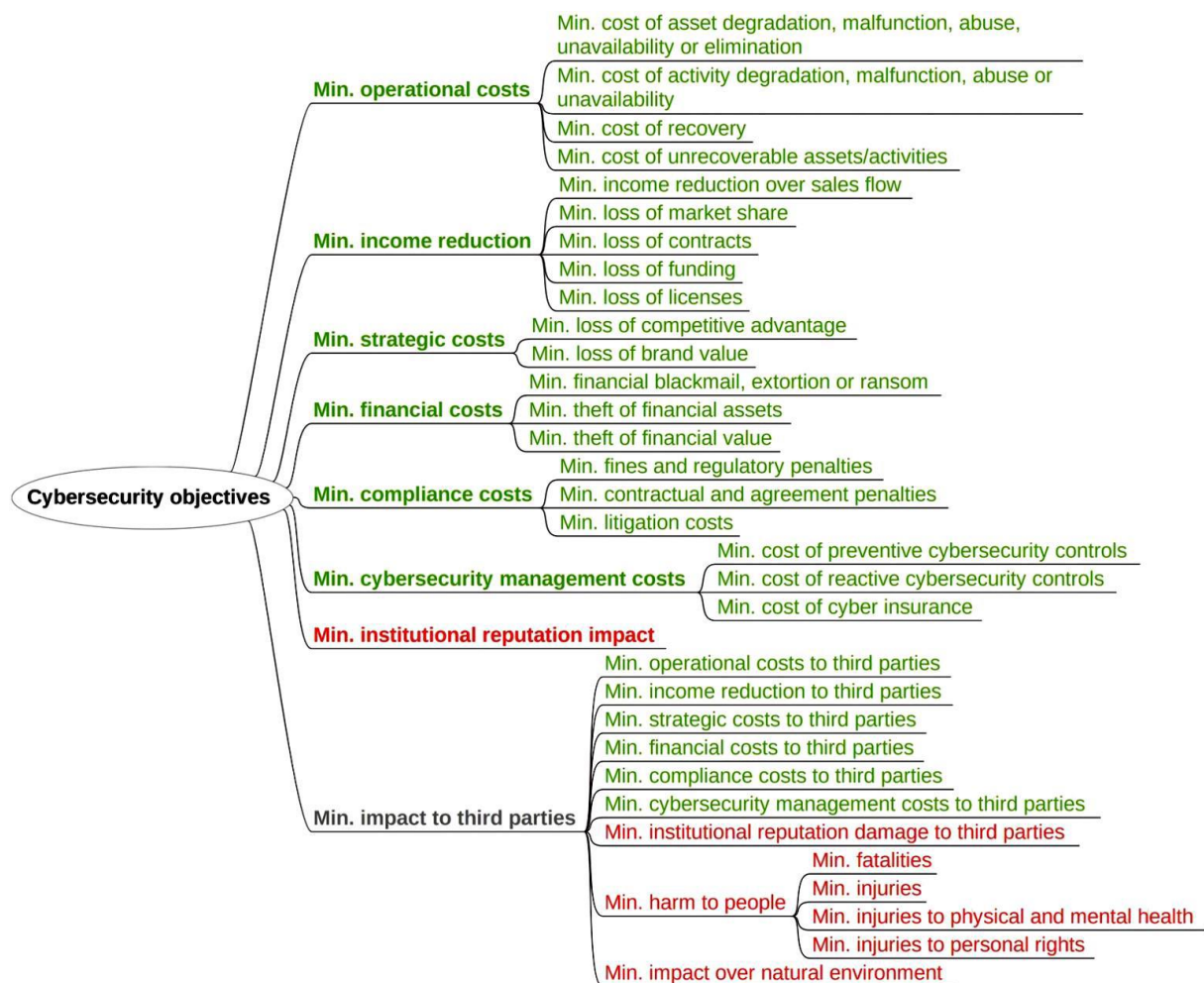


Figure 2: Cyber-security objectives specification (ref. Figure 9 D3.1)

## D4.2: Use-Case Evaluation of the Methodology and Framework

### Argumentation:

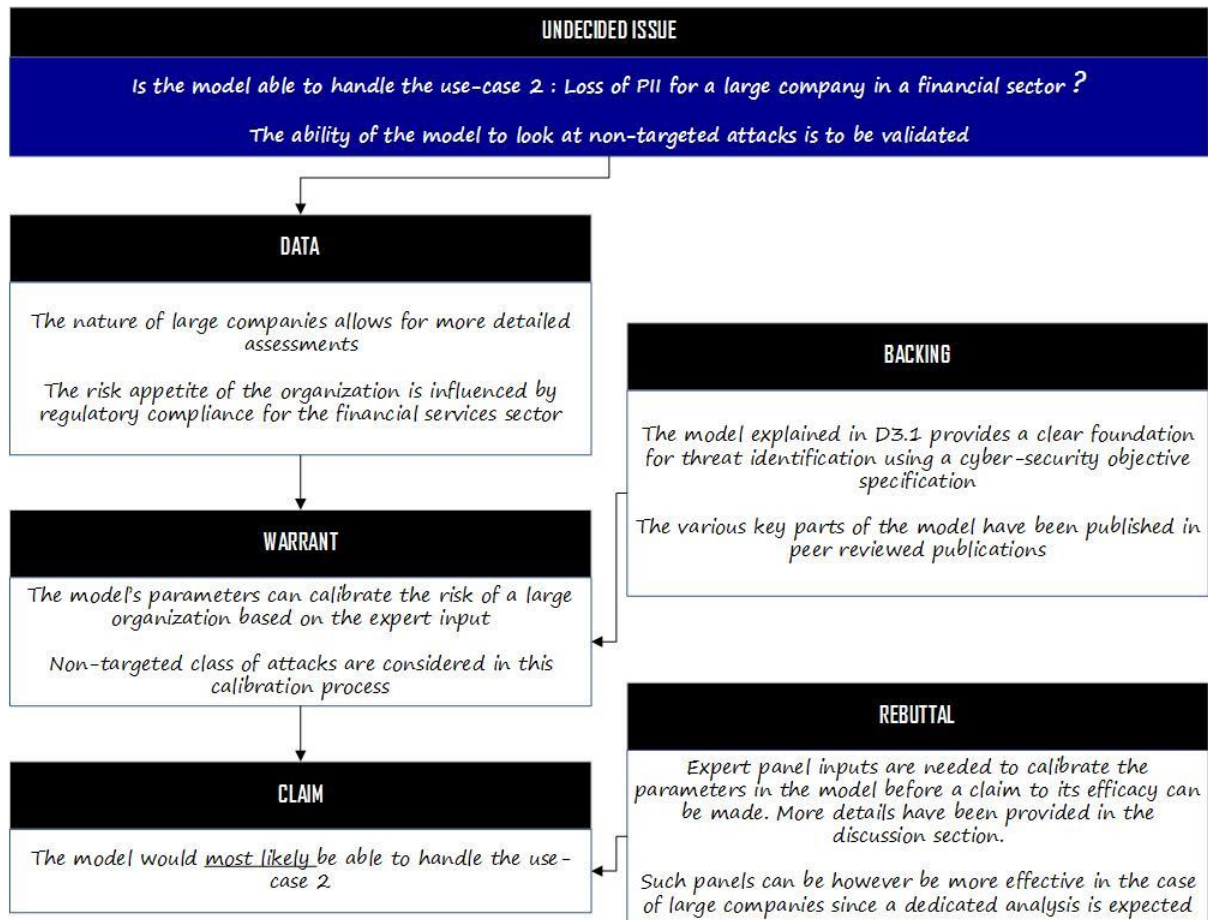


Figure 3: Toulmin model argumentation for use-case 2

### 2.2.3 Use-case 3: Insurance fraud for an SME in the professional services sector

#### Background:

This use-case is important since it deals with a primary issue in the insurance sector: insurance claim fraud. The key objectives of this use-case involves three main factors against which the model needs to be checked:

1. The claim is from an SME, i.e. the resources allocated to processing and verification the claim cannot be very high
2. The claim involves data loss which is usually covered by a typical cyber-insurance policy
3. The fraud performed is easy to implement but hard to detect - data is moved and deleted; it is temporarily unavailable till the claim is processed when it is brought back.

---

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

### *Discussion:*

The model itself provides one mechanism in this regard in the form of a defender model. The details of this model have been clearly highlighted in the paper “Cybersecurity preference models. The defender case” which was provided as part of D3.1. With an understanding of the various controls in place, the model could be used to analyse a probability of a threat. The claim by the SME typically requires justification and the threat vector identified could be evaluated against the attacker model to compute the probability of the event.

It must be noted that the model’s proposition is valid in theory and could work eventually when there is sufficient data to ascertain these probabilities. Currently the attacker model requires input from both security experts and continuous data to attain maturity. Further, this is not a “fraud detection” algorithm but one of the parameters that could be used in a more versatile fraud detection mechanism. With additional input from security experts to calibrate the probabilities, the model can provide useful inputs to “fraud detection” algorithms used by insurance provider. An argumentation for this claim has been provided using the Toulmin model in Figure 4.



## D4.2: Use-Case Evaluation of the Methodology and Framework

### Argumentation:

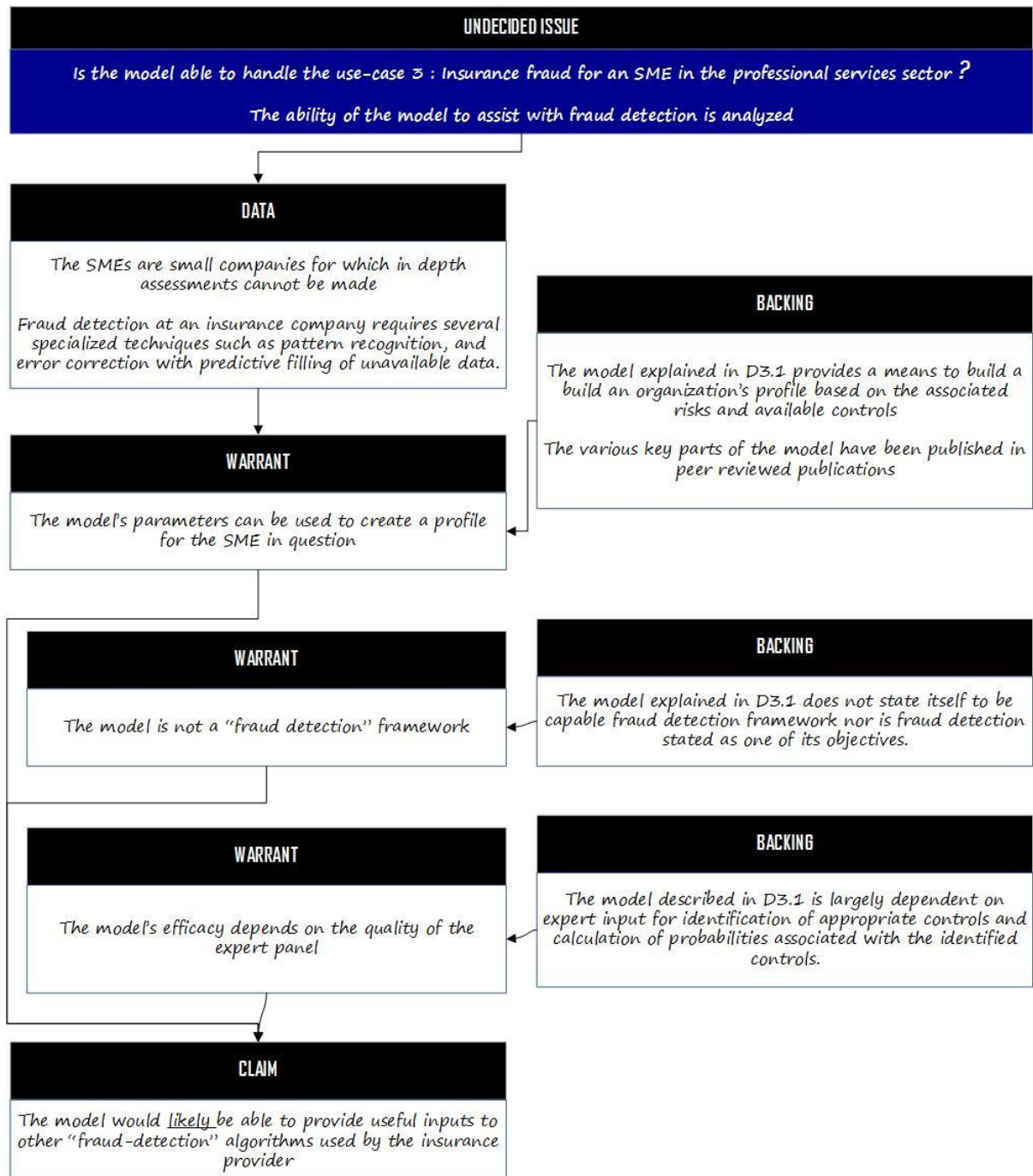


Figure 4: Toulmin model argumentation for use-case 3



## D4.2: Use-Case Evaluation of the Methodology and Framework

### 2.2.4 Use-case 4: Products / Services Manipulation for a large company in the manufacturing sector

#### Background:

This use-case primarily focuses on a large company with less cyber footprint due to the nature of its business. Further, the implications of an attack lead to a more severe attack that impacts business continuity, brand and regulatory compliance. This tests the effectiveness of the model for “Cyber-Physical Systems”.

#### Discussion:

The large company would imply the following assumptions for the insurance sector.

- A customized policy with inputs from a dedicated security professional would have been involved in the insurance conception stage
- Periodic security checks would have been involved due to the scale of the insurance
- Regulatory compliance of key assets and manufactured units would have reduced the risk of deaths due to faulty products or such more serious ramifications.
- Costs would have affected primarily the business continuity, and brand perception.

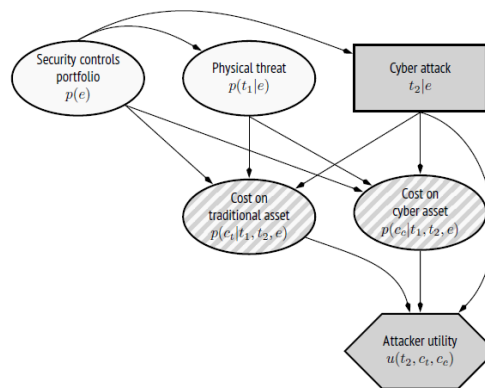


Figure 5: Attacker model in ARA (Ref. D3.1)

In the specification of the model, an adversarial risk analysis (ARA) is performed that takes both an attacker problem and a defender problem into perspective and solves them in sequence. As shown in Figure 5, the attacker model takes the cost of a cyber-attack on a traditional asset into consideration. This is in-line with expectations for identifying

## D4.2: Use-Case Evaluation of the Methodology and Framework

possible threats to assets, in this case, the production line. The model is hence most likely able to handle the requirements of use-case 4 further illustrated by the argumentation model shown in Figure 6.

### Argumentation:

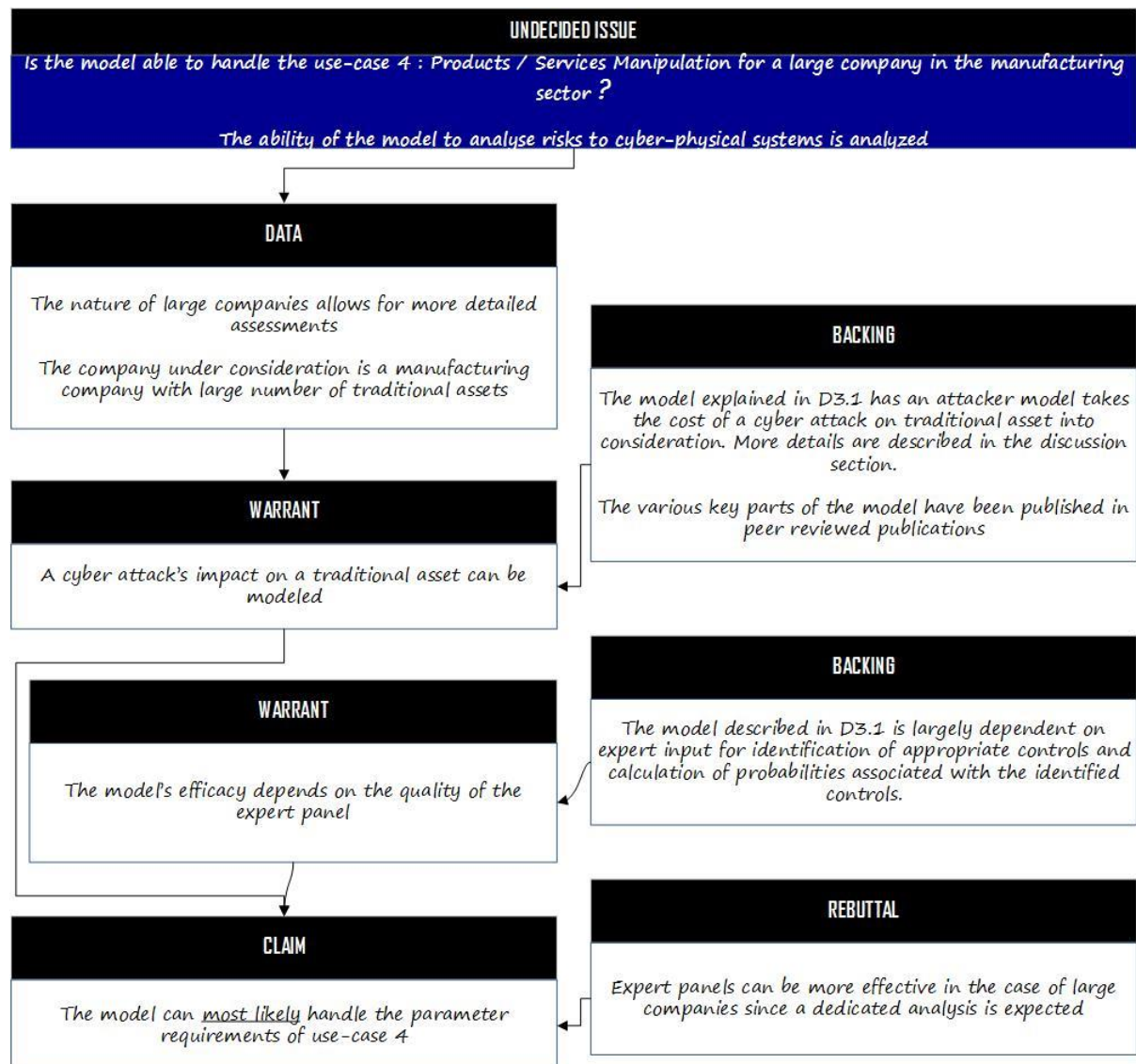


Figure 6: Toulmin model argumentation for use-case 4

### 2.2.5 Use-case 5: Insufficient insurance coverage for an SME operating in the IT industry sector

#### Background:

This use case focuses on a SME with a relatively large cyber footprint. The cyber-assets impacted directly affect its clients' business continuity as well. The implied argument is that the threat model must reflect this cost estimation error in future predictions.

---

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

### *Discussion:*

This use-case presents several legal and ethical challenges and is more under the scope of the legal domain since the financial caps of a DDoS assessment are disputed. The arguments can be summed up as follows:

- The threat is real and the insurance payout was obtained
- The cost to the SME is higher than the insurance payout
- The insurance provider is protected by the cap in the policy
- The third-parties affected need to be compensated by the SME or by their own insurance policies

In this case, the model needs to be updated to reflect the changes to the cost computation metrics. The exposure risks for the sector of the SME would have to be recomputed. This is feasible in the model with changes to likelihood metrics and recomputed impact analysis.

It can be stated that the model is most likely able to handle the parameter update requirements for the use-case 5. While the model does not handle any legal or ethical considerations, it must be noted that these are out of scope for this analysis. These claims have been presented using the Toulmin model in Figure 7.

## D4.2: Use-Case Evaluation of the Methodology and Framework

### Argumentation:

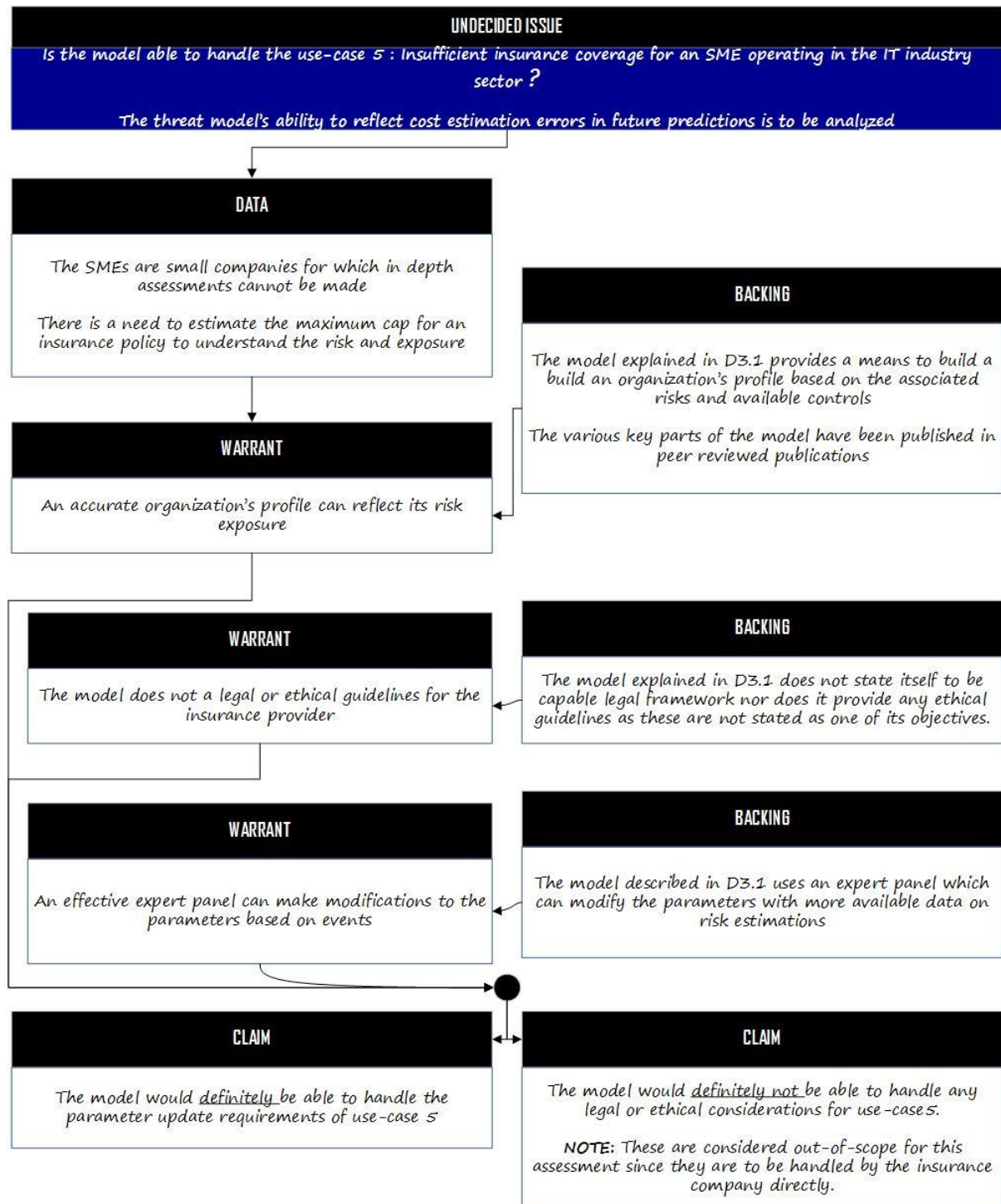


Figure 7: Toulmin model argumentation for use-case 5

### 2.2.6 Use-case 6: Accumulation of cyber-incidents following a single large-scale attack with involvement of reinsurance in the claim process

#### *Background:*

This use-case is a special case of targeted attacks where a critical asset or a series of critical assets are targeted causing a cascade effect impacting several insured entities. Such a scenario could result in simultaneous massive claims deeply undercutting the insurance sector. In this scenario, the model's ability to predict such a cascade is to be tested.

#### *Discussion:*

The APA model considers the ability to model critical infrastructure protection (CIP) problem and provides an example of how to do so in the publication "Adversarial Risk Analysis for Bi-Agent Influence Diagrams: An Algorithmic Approach" provided in D3.1. However, the paper on this problem makes a fineprint note on the requirement of several variables, and the mutual dependence between CIPs would add severe complexity. Note: The number of nodes considered would have quadratic complexity with reference to polynomial-time.

While the model is theoretically able to handle this scenario, it requires:

- Identification of dependency nodes
- Identification of critical assets
- Security expert panels required for sector specific risk mapping
- Identification of all variables involved in the risk propagation/cascade estimation
- High availability of computational resources dedicated to this analysis

Legal and ethical arguments such as government risk undertaking for use-case 6 may be out of scope for the model - however the nature of these issues fall under the purview of the insurance provider rather than the model itself. With additional input from security experts to calibrate variables and identify critical assets, the probability of a risk cascade could be estimated with significant computational resources allocated to the model for computation. An argumentation for this claim has been provided using the Toulmin model in Figure 8.



## D4.2: Use-Case Evaluation of the Methodology and Framework

### Argumentation:

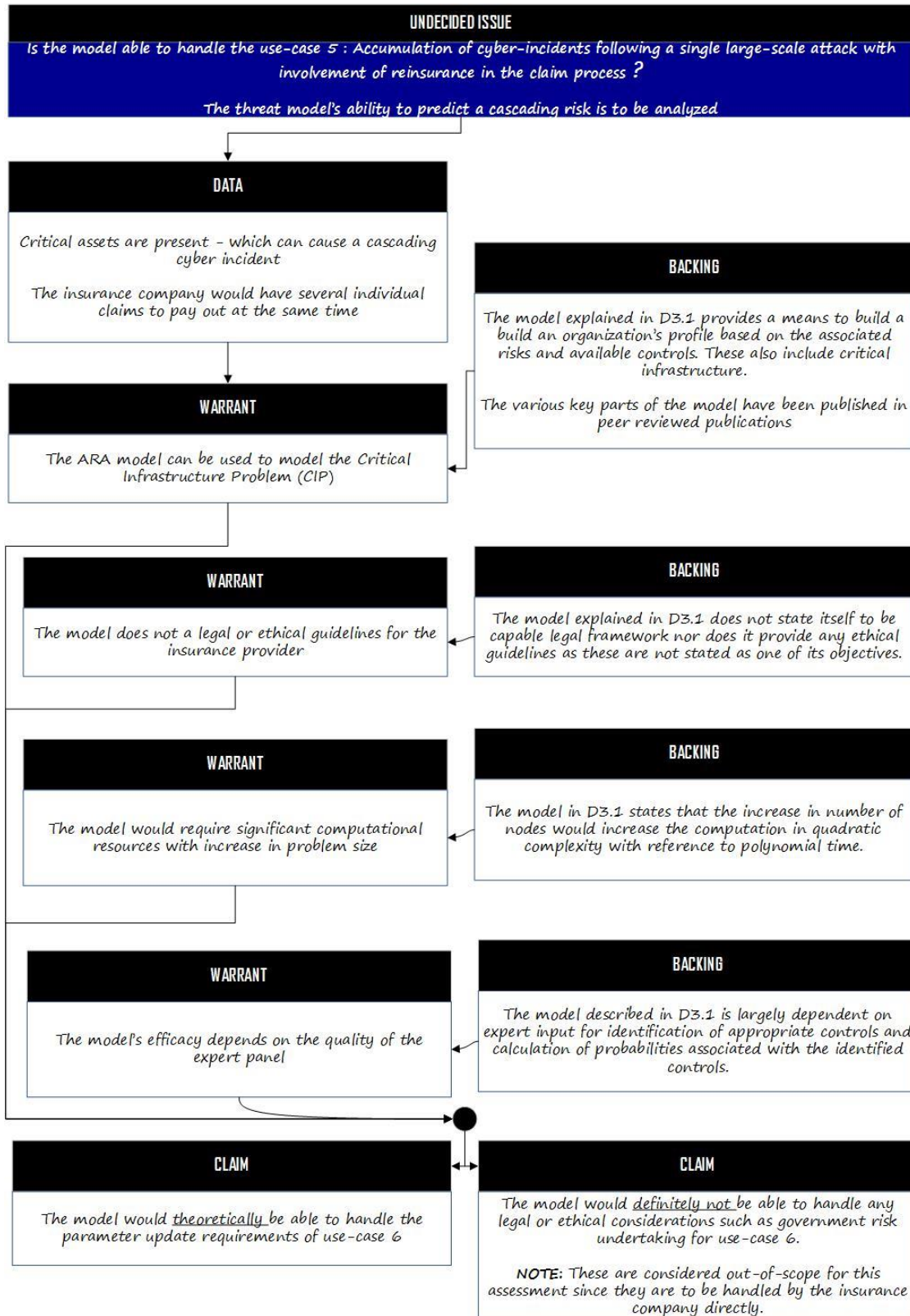


Figure 8: Toulmin model argumentation for use-case 6

### 3 Conclusion

The model was considered in full along with the fine details on its working. The scope of this analysis was limited to the technical aspects. Hence, legal and ethical considerations were considered to be out of scope as the nature of these issues fall under the purview of the insurance provider rather than the model itself. After these key considerations, the model was found to be theoretically sound in its current state. Some practical considerations on the computational resources used by the model may eventually become non-issues with the decreasing cost of computational resources. The problem of expert judgement would also be eventually solved if there is sufficient data to act as an empirical measure. With these considerations, the analysis concludes that the model provided in D3.1 is able to satisfy the requirements set by the use-cases in D4.1.

## **Part II:**

### **Validation of the toolbox using the cyber-insurance scenarios**

#### **Abstract:**

In order to assess the risk calculation methodology and toolbox, and also to make it possible to incorporate the behavioural components into this methodology, it is necessary to understand the interactions between the parties in the cyber-insurance process through a set of detailed scenarios based on previously defined use cases that are sufficiently representative of the global cyber-insurance ecosystem. The scenarios presented in this document are based on the use-cases which are derived based on the analysis of the value chain for a given company, and the associated assets.



## 4 Introduction

### 4.1 Objective and Scope

This section provides an overview of the toolbox and provides an analysis of the model over the three scenarios that were defined in D4.1. The scope of the evaluation is limited to these use-cases and the analysis is not exhaustive in nature. This is in-line with the key objective of the analysis, which is to check the minimum level of viability of the toolbox, rather than its ability to handle all complex insurance requirements.

### 4.2 Chapter Structure

This chapter provides a common structure on how each of the three scenarios were used as input into the toolbox and a rapid analysis of the output from the toolbox.

## 5 Cyber-insurance scenarios

This section provides the cyber-insurance scenarios in a common and structured view which facilitates a standardized analysis in each particular scenario, despite their respective specificities. These scenarios provide a one-to-one mapping example for each of the use-cases defined in D4.1. The results of these scenarios are defined in below.

### 5.1 Scenario 1<sup>3</sup>: Loss of personally identifiable data for a large company in the financial sector

#### 1. Background

Rocardier Finance is a large financial company with subsidiaries in over 18 countries, with its headquarter in Paris, France. The company has a strong foothold in EU countries with approximately 52% of its turnover in the European market. The US and Asia represents its second largest markets with 40 % of its turnover, the remaining 8% being distributed in the remaining regions. Rocardier Finance provides portfolio management and brokerage desks to institutional and individual investors regarding most financial instruments such as bonds, stocks, contracts for difference, and real-estate investments.

#### A. Constraints, assumptions, and preferences:

- Regulations

The French legal entities of the company must comply with the following regulations from the data and information security perspective:

- EU Directive 2016/1148 - Network and Information Security Directive
- Regulation 2016/679 -General Data Protection Regulation (GDPR)
- Act No. 78-17 of January 6 1978 on Information Technology, Data Files and Civil Liberties

- Compliance

Because of its banking activities, Rocardier Finance must ensure compliance with the following regulations:

- Bale III, which imposes a solvability ratio of at least 10.5%.
- AMF regulations: Obligation to collect information on all individual and institutional clients for transparency and tracking purpose, especially against market manipulation and insider trading. Such information can also be required by

---

<sup>3</sup> This scenario corresponds to use case 2.

---

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

TRACFIN<sup>4</sup> which conducts investigations on specifically targeted individual and institutional clients for anti-money laundering and anti-terrorist funding measures.

- Assumptions
  - Turnover of the company: € 54 billion
  - Net income: € 6.2 billion
  - Because of its size and its large potential impact on the global economic landscape, the company has interactions with the French cybersecurity regulator agency ANSSI.
- Preferences
  - The company has a strong preference for discretion and anonymity when considering cyber-attacks, regulation and compliance breaches and financial penalties or sanctions.

### B. Assets to be protected

- Customer data
- Personally Identifiable Information (PII) data
- Payment Card Information
- Marketing research and analysis
- Financial statements
- Business Intelligence
- Executive Management Information

### C. Potential threats<sup>5</sup>

- Threat actors: Organized criminal groups, Employees, Hacking groups and individual hackers
- Motivation: Espionage, Theft, Financial, Ideology
- Types of attack: All types of attacks listed in Appendix Table 2.

### D. Uncertainties

- Uncertainties of the defender
  - The repercussions of a successful attack on the market and stakeholder perception of the company
  - The legal and regulatory repercussions following potential breaches
  - The probability of successfully repelling or containing cyber-attacks, i.e. the efficiency of security safeguards and countermeasures.
- Uncertainties of the attacker

---

<sup>4</sup> TRACFIN (Traitement du Renseignement et Action contre les Circuits FINANCIERS clandestins), is a service of the French Ministry of Economy specialized in fighting money laundering and any other illegal financial activities.

<sup>5</sup> We note that in the risk scenarios presented in this document, a threat is composed by the involved threat actor, its capability, and its motivation. Capability is composed of the means to carry out an attack coupled with the required expertise and know-how.

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

- The time and effort it will take to penetrate the network of the company and its information systems
- The eventual success probability of identifying valuable assets
- Capability of avoiding detection measures
- The ability to avoid identification during the cyber-attack

### E. Safeguards and countermeasures

- All safeguards and countermeasures listed in Appendix Table 5 are implemented in the organisation, yet the effectiveness of some of these safeguards and countermeasures could be improved.

### F. Potential impact and loss

- Potential impact and loss for the attacker
  - IP ban
  - Legal suits from law enforcement agencies resulting in imprisonment or reduced freedom
  - Loss of time resulting in an unfruitful attack effort
- Potential impact and loss for the defender
  - Data loss
  - Response costs
  - Brand damage
  - Regulatory fines

### G. Initial considerations on the scenario likelihood

Organised criminal groups are known to perform numerous attack against organisations to steal their data or the information of their customers. Similarly hacking groups and individual hackers may consider Rocardier Finance as a challenge and targeting this organisation in line with their ideology. Therefore, the likelihood for Rocardier Finance to be targeted by such a group is significant due to the information it handles. On the other hand, the overall high level of cybersecurity maturity posture of large financial organisation and the regulations they need to comply with, that require information security safeguards and countermeasures, provides Rocardier Finance with a high level of readiness in identifying, responding and preventing this attack considered in this scenario.

The likelihood of this scenario is therefore estimated at a **Medium** level.

### H. Insurance perspective

- Risk assessment and recommendations
  - Cyber-risk assessment

Rocardier Finance is subject to regular and extensive cyber-assessments programs (cybersecurity maturity ratings, penetration testing campaigns). Consequently, the profile of the company appears very solid.
  - Estimated cost of potential losses

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

Given the risk scenario and the considerable domino impact of a successful cyber-attack on the financial market sector on a large financial institution, the estimated cost of potential losses<sup>6</sup> is set at High (see Appendix Table 6).

- Recommended security controls  
Rocardier Finance has already implemented all recommendable security control. No additional recommendations can be provided.
- Insurance policy 1  
The insurance policy in the scope of this risk scenario is defined by the following elements:
  - Insured legal entity: Rocardier Finance S.A, France
  - Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
  - Covered risks: Data loss, Fraud
  - Exclusions: 3<sup>rd</sup> party liability, stock market depreciation following risk occurrence
  - Endorsements: The cyber-insurance policy for Rocardier Finance S.A is conditioned upon the effective risk assessment and any additional audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy.
- Insurance policy 2  
The insurance policy in the scope of this risk scenario is defined by the following elements:
  - Insured legal entity: Rocardier Finance S.A, France/Italy
  - Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
  - Covered risks: Data loss, Fraud, Identity theft
  - Exclusions: Regulatory financial penalties
  - Endorsements: The cyber-insurance policy for Rocardier Finance S.A is conditioned upon the effective risk assessment and regular independent audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy.
- Insurance policy 3  
The insurance policy in the scope of this risk scenario is defined by the following elements:
  - Insured legal entity: Rocardier Finance Group, Europe/U.S.

---

<sup>6</sup> We recall that the potential loss includes the loss of each individual impact and loss for the defender.

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

- Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
- Covered risks: Data loss
- Exclusions: 3<sup>rd</sup> party liability, stock market depreciation following risk occurrence
- Endorsements: The cyber-insurance policy for Rocardier Finance Group is conditioned upon the effective risk assessment of individual legal entities. The underwriting pricing and contractual agreements will be fixed separately for each legal entity of Rocardier Group in Europe and U.S.

- Covered loss

- Business interruption
- Brand damage

- Premiums

The insurance company offers legal advice in case of legal suits from 3<sup>rd</sup> parties following cyber-attacks which are identified as in scope of the insurance policy contract. Also, insurance companies provide free security modules to the software and mobile apps that Rocardier Finance offers to the organization's individual and institutional users for their day-to-day operations.

- Deductibles

- The insurance company will deduct 3% of the premium for every additional year without filed claims. The deductibles will be null after each year with reported incidents followed by a filed claim.

## 2. Scenario execution

### A. Involved threats

- Actors and motivation

The risk scenario is perpetrated by an actor of the Organized crime category, and the motivations belong to the Financial and Theft types.

### B. Attack vector and execution

- Vulnerabilities and tools

- nmap
- Shodan
- CVE-2014-6271 - Shellshock
- CVE-2016-5195 - DirtyCOW

- Execution of the attack

1. The attackers follow one of the following: (i) scan the website of the company for vulnerabilities with nmap, or (ii): lookup on Shodan for vulnerable websites belonging to this company, or associated contractor websites.

2. The attack is activated through a vulnerability such as Shellshock which allows attackers to gain unauthorized access to the company server. More precisely, attackers are able to use Shellshock to execute code and add a malicious web page on the

---

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

website allowing the attacker to connect to the database, since the webserver must have access to the database in order to interact with it. After gaining access to the server, the attackers use another vulnerability exploit such as Dirty COW through a modified version of the C99 PHP script to gain administrative power on the server. Such action is useful for privilege escalation required for long-time persistence. This allows the attackers to install a command and control malware module allowing them to orchestrate the exfiltration of data from the company server.

Identification and response process

- The Identification and response process is the one described by Process ID #1 in Appendix Table 4.

### C. Impacted assets

- The impacted assets are composed of the type Information: Personally Identifiable Information (PII) data, in Appendix Table 4.

### D. Observed impact and loss

- The observed impacts include Loss of data and software, Privacy liability, Security liability, and Brand and reputation damage, as per Appendix Table 7.
- Observed losses include: (i) Customer's loss due to Brand and reputation damage category, and (ii) Recovery expenses, Analysis and audit expenses related to the Collateral expenses category, as per Appendix Table 6.

### E. Post-attack insurance overview

- Audit and forensics
- Scope analysis of incurred loss
- A priori decision on insurance coverage

## 5.2 Scenario 2<sup>7</sup>: Insurance fraud for an SME in the professional services sector

### 3. Background

Iberia Consultivo is a professional services SME with its headquarters in Madrid, Spain. It operates solely on the Spanish market. Iberia Consultivo provides advisory services to individuals, companies, and public institutions on topics including legal, regulatory, and business strategy.

#### A. Constraints, assumptions, and preferences

- Regulations
  - Regulation 2016/679 -General Data Protection Regulation (GDPR)
  - Organic Law 15/1999 of Protection of Personal Data
- Compliance

Given the activities of the company, no compliance requirements are mandatory for Iberia Consultivo.
- Assumptions
  - Turnover of the company: € 37 million
  - Net result: € 4.7 million
- Preferences
  - The company prefers internalized IT infrastructure and cybersecurity solutions. It strongly avoids outsourced services.

#### B. Assets to be protected

- Customer data
- Personally Identifiable Information (PII) data
- Financial Statements
- Executive Management Information
- Business Intelligence
- Marketing research and analysis

#### C. Potential threats

- Threat actors: Organized criminal group, Employee, Individual hackers
- Motivation: Theft, Financial, Vengeance, Technical challenge
- Types of attack: All types of attacks listed in Appendix Table 6.

#### D. Uncertainties

- Uncertainties of the defender<sup>8</sup>

---

<sup>7</sup> This scenario corresponds to use case 3.

<sup>8</sup> In this particular risk scenario, the defender is assumed to be the legal representative of the company, i.e. the CEO.



---

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

- The legal and regulatory repercussions following potential breaches
- The impact of successful cyber-attacks on the business activities
- Uncertainties of the attacker<sup>9</sup>
  - The legal repercussions in case of their identification
  - The success in perpetuating the fraud the insurance company

### E. Safeguards and countermeasures

- The safeguards and countermeasures are limited to an antivirus commercial product, a firewall for the company internet gateway, and a data backup solution deployed internally.

### F. Potential impact and loss

- Potential impact and loss for the attacker
  - Legal suits from law enforcement agencies resulting in imprisonment or reduced freedom
  - Loss of time resulting in an unfruitful attack effort
- Potential impact and loss for the defender
  - Data loss
  - Brand damage - loss of clients
  - Regulatory fines
  - Refusal from insurance company to cover the induced costs

### G. Initial considerations on the scenario likelihood

The likelihood for the scenario of insurance fraud by insider actors is estimated at a **Medium** level. While the risk of insurance fraud has a high level of frequency on a global scale, yet the relatively low implementation of cyber-insurance policies moderates this risk<sup>10</sup>.

### H. Insurance perspective

- Risk assessment and recommendations
  - Cyber-risk assessment  
Iberio Consultivo conducts occasional cyber-risk assessments in the framework of penetration testing missions by external and independent audit companies.
  - Estimated cost of potential losses penetration  
Given the risk scenario, the profile of the company, and the repercussions of cyber-attacks on the business sector of Iberia Consultivo, the estimated cost of potential losses is set at High (see Appendix Table 6).
  - Recommended security controls

---

<sup>9</sup> The attacker in this scenario is composed by a manager and a subset of the employees.

<sup>10</sup> In the future there may be an increase in the trend of this risk, due to the increasing subscription of cyber-insurance policies.

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

The insurance companies may require additional security controls consisting of Inventory of assets and a Business continuity plan as per Appendix Table 5.

- Insurance policy 1

The insurance policy in the scope of this risk scenario is defined by the following elements:

- Insured legal entity: Iberia Consultivo, Spain
- Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
- Covered risks: Data loss
- Exclusions: 3<sup>rd</sup> party liability, Incidents following acts of negligence.

Endorsements: The cyber-insurance policy for Iberia Consultivo is conditioned upon the effective risk assessment and any additional audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy.

- Insurance policy 2

The insurance policy in the scope of this risk scenario is defined by the following elements:

- Insured legal entity: Iberia Consultivo, Spain
- Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
- Covered risks: Fraud, Privacy liability
- Exclusions: 3<sup>rd</sup> party liability, media liability, extortion.

Endorsements: The cyber-insurance policy for Iberia Consultivo is conditioned upon the effective risk assessment and any additional audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy.

- Covered loss

- Business interruption
- Brand damage

- Premiums

The insurance company offers an external data backup solution hosted on a recommended and trusted Cloud operator.

- Deductibles

- The insurance company will deduct 35% of the premium for every year in which a data backup service has been subscribed by the insured company.

#### 4. Scenario execution

##### A. Involved threats

- Actors and motivation

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

The risk scenario is perpetrated by an actor of the Insider category, and the motivations is of the Financial type.

### B. Attack vector and execution

- Vulnerabilities and tools
  - Cryptowall
  - Rig
  - Nuclear
  - Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability (CVE-2012-0507)
  - Adobe Flash Player Buffer Overflow Vulnerability (CVE-2014-0515)
  - Adobe Flash Player and AIR Unspecified Heap Based Buffer Overflow Vulnerability (CVE-2014-0556)
- Execution of the attack
  1. The insider threat actor intentionally infects company servers with ransomware such as the CryptoWall ransomware, by following malware-infected adds on the Zedo ad network<sup>11</sup>. Then tools such as the Rig and Nuclear tools exploit one of the aforementioned vulnerabilities to install the CryptoWall on the servers of the company.
  2. The CryptoWall ransomware encrypts the data located in the company servers, therefore interrupting their usage for day-to-day operations of the company.

### C. Identification and response process

- The Identification and response process is the one described by Process ID #3 in Appendix Table 9.

### D. Impacted assets

- The impacted assets are composed of the type Information: Customer data, Personally Identifiable Information (PII) data, and Financial Statements data, in Appendix Table 1.

### E. Observed impact and loss

- The observed impacts include Fraud, Media liability, Management liability, and Brand and reputation damage, as per Appendix Table 7.

### F. Post-attack insurance overview

- Audit and forensics
- Scope analysis of incurred loss
- A priori decision on insurance coverage

---

<sup>11</sup> Zedo is a privately held company specialized in online advertising of products and services to Internet publishers, advertisers, and agencies.

### 5.3 Scenario 3<sup>12</sup>: Manipulation of Products / Services for a large company in the manufacturing sector

#### 5. Background

European Aerospace Company (EAC) is a large manufacturing company with subsidiaries in 7 countries, with its headquarters in Stuttgart, Germany. The company has a global foothold with approximately 48% of its turnover in the Middle East, 23% in Europe, 17% in Asia, and 12% in the US. EAC manufactures airplanes, satellites, and related technology for commercial and military clients.

#### A. Constraints, assumptions, and preferences

- Regulations
  - Regulation 2016/679 - General Data Protection Regulation (GDPR)
  - EU Directive 2016/1148 - Network and Information Security Directive
  - Federal Data Protection Act
  - IT Security Act (ITSiG)
- Compliance
  - Given the activities of the company, confidentiality compliance is required from the Department of Defense of the respective country in which the company operates for military clients.
- Assumptions
  - Turnover of the company: € 69 billion
  - Net result: € 1.4 billion
  - Given the size and the sensitive domain of activity, the company has tight links with governmental cybersecurity and defense agencies.
- Preferences
  - EAC has a strong preference for locally deployed cybersecurity protective measures, and prefers specifically-tailored services and products developed by external providers.

#### B. Assets to be protected

- IT Infrastructures
- Production lines
- Intellectual Property / Patents
- Customer data
- Personally Identifiable Information (PII) data
- Financial statements
- Business Intelligence
- Executive Management Information

#### C. Potential threats

---

<sup>12</sup> This scenario corresponds to use case 4.

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

- Non-intentional threats
  - Natural disasters
  - Production line failures and accidents
  - Fire
- Intentional threats
  - Threat actors: Hacktivists, Competitors, State Actors, Organized Crime
  - Motivation: Espionage, Financial, Ideology
  - Types of attack: All types of attacks listed in Appendix Table 2.

### D. Uncertainties

- Uncertainties of the defender
  - The repercussions of a successful attack on the market and stakeholder perception of the company
  - The legal and regulatory repercussions following potential breaches
  - The probability of successfully repelling or containing cyber-attacks, i.e. the efficiency of security safeguards and countermeasures.
- Uncertainties of the attacker
  - Ability to penetrate the IT infrastructure
  - Ability to manipulate the product manufacturing designs
  - Ability to avoid detection measures
  - Ability to avoid identification

### E. Safeguards and countermeasures

- All safeguards and countermeasures listed in Appendix Table 5

### F. Potential impact and loss

- Potential impact and loss for the attacker
  - Reinforced protective measures leading to excessive loss of time and effort.
  - Increased risk of traceability and identification leading to increased legal and penal risk, especially for competitor companies.
  - Political and economic implications in case of identification, including commercial bans in case of international retaliation.
- Potential impact and loss for the defender
  - Loss or damage to physical properties
  - Product recall
  - Brand and reputational damage
  - Non-compliance with regulation
  - Business interruption

### G. Initial considerations on the scenario likelihood

Product/Services manipulation attacks by malicious actors happen on a regular basis. While competitors may not conduct such an attack themselves, due to the potential trackability of such actions and the potential backlash on reputation from customers, the industry and regulators, organisations may profit from a nation-state sponsored campaign from their government in an attempt to give an edge to their local economy.

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

Such campaigns though are only conducted when a sector's contribution to the country's economy is significant and the potential gain outweigh the potential sanctions, official or not, the country may face, such as on its import of other goods.

Therefore, the likelihood of this scenario is **Medium** given the increasing frequency with which state actors are waging attacks.

### H. Insurance perspective

- Risk assessment and recommendations

- Cyber-risk assessment

- EAC undergoes regular internal and external cyber-assessments programs. Given the confidential nature of some of the activities of the company, the insurance companies will have access to assessment reports of non-confidential entities in Germany.

- Estimated cost of potential losses

- Given the risk scenario, and the large repercussion from a contractual perspective in the aeronautics domain, the estimated cost of potential losses is set at **Very high** (see Appendix Table 6).

- Recommended security controls

- EAC has already implemented all recommendable security control. No additional recommendations can be provided.

- Insurance policy 1

The insurance policy in the scope of this risk scenario is defined by the following elements:

- Insured legal entity: European Aerospace Company, Germany.

- Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.

- Covered risks: Data loss, Product recall

- Exclusions: 3rd party liability, and any other liability not specifically mentioned in the covered risks.

- Endorsements: The cyber-insurance policy for European Aerospace Company is conditioned upon yearly risk assessments and any additional audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy.

- Insurance policy 2

The insurance policy in the scope of this risk scenario is defined by the following elements:

- Insured legal entity: European Aerospace Company, Europe/Asia/U.S.

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

- Customer declaration elements: The customer has declared the value of the covered assets and, as well as the security measures taken as precautionary measures in the event of incidents impacting such assets.
- Covered risks: Data loss, Property damage and personal injury, Media liability, Theft of money and securities.
- Exclusions: Risks related to military, spatial, and/or government-related activities and any other liability not specifically mentioned in the covered risks.
- Endorsements: The cyber-insurance policy for European Aerospace Company is conditioned upon yearly risk assessments and external independent audits required by the insurance company prior to, and after the occurrence of, the risk events covered in the insurance policy, including the regular audit programmes initiated by EAC.

- Covered loss

- Revenue loss: Direct loss, Compensatory payments to customers and/or suppliers
- Collateral expenses: Recovery expenses, Analysis and audit

- Premiums

The insurance company offers legal advice in case of legal suits from 3<sup>rd</sup> parties following cyber-attacks which are identified as in scope of the insurance policy contract.

- Deductibles

The insurance company will provide deductions conditioned to the subscription of additional insurance policies on property damage and personal injury. Such deductions will be proportional and up to 7% of the contract size of the additional insurance policies.

### 6. Scenario execution

#### A. Involved threats

- Actors and motivation

#### B. Attack vector and execution

- Vulnerabilities and tools

- Open file-sharing folders,
- CVE-2017-0143
- CVE-2017-0144
- CVE-2017-0145
- CVE-2017-0146
- CVE-2017-0147
- CVE-2017-0148

- Execution of the attack

The first step may involve one of the following options:

- Option 1: The attacker employs a phishing campaign to obtain access in the internal network through user machine,

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

- Option 2: If an available 445 port is open, then the attacker can use it as a gateway for a foothold in the internal network.

Then the attacker proceeds with lateral movements to elevate privileges, e.g. through the Eternal family of exploits activated on unpatched internal assets, such as Windows 2003 servers, or by means of old legacy applications, default passwords, etc.

The attack follows through the targeting of e-mail servers or Active Directory to identify technical personnel and/or network administrators and thus to specifically target the production chain.

Finally, with the high-privilege role obtained, it becomes possible for the attacker to connect to the computer containing the Catia<sup>13</sup> design file, and thus alter it, resulting in final component being non-compliant with the initial specifications.

### C. Identification and response process

The Identification and response process is the one described by Process ID #1 in Appendix Table 4.

### D. Impacted assets

- The impacted assets are composed of the type Hardware: IT Infrastructures, and Production lines in Appendix Table 1.

### E. Observed impact and loss

- The observed impacts include Product recall, and Loss or damage to physical properties, as per Appendix Table 7.
- Observed losses include: (i) Contractual and Regulatory loss under the Financial penalties category, (ii) Customer's loss due to Brand and reputation damage category, (iii) Interruption of provided services/products due to the Loss of competitiveness and productivity category, and (iv) Recovery expenses, Analysis and audit expenses related to the Collateral expenses category, as per Appendix Table 6.

### F. Post-attack insurance overview

- Audit and forensics
- Scope analysis of incurred loss
- A priori decision on insurance coverage

---

<sup>13</sup> Catia is a proprietary computer-aided design software from Dassault Systemes that is commonly used to design components.



## 6 Approach and Analysis

### 6.1 Overview of the toolbox

The toolbox has been built to use the model and provide a prototype implementation to demonstrate its feasibility. It has been hosted in the site <https://toolbox.cybeco.eu/> and performs insurance simulations on the server.

### 6.2 Analysis of Use-cases

#### 6.2.1 Scenario 1: Loss of personally identifiable data for a large company in the financial sector

##### *Background:*

This scenario can be directly mapped to the use-case 2. In this use-case the major considerations are whether the non-targeted attacks are being taken into consideration when using the toolbox. Further, it is also important to note that there are several compliance requirements for this entity and controls that are needed for regulatory oversight. The toolbox's capabilities in these factors are to be analyzed.

##### *Discussion:*

The toolbox is an implementation that incorporated the previously described model for simulating the threat analysis. It also includes several components and defines the parameters to be incorporated into the model.

The parameters involved in the creation of the model for a large enterprise are varied and unique. These require several key considerations and several times involve customized considerations. The toolbox in its current state requires input on all the variables involved and is unable to satisfy these constraints for the "large enterprise" (see Figure 9).

It can hence be concluded that at the time of this review, the toolbox is still in the process of designing the components for effective use by large enterprises. It is not possible to assess this scenario at this stage since the toolbox implementation is considering the parameters for large enterprises. It must be noted that the nature of large enterprises makes such an identification complex.

## D4.2: Use-Case Evaluation of the Methodology and Framework

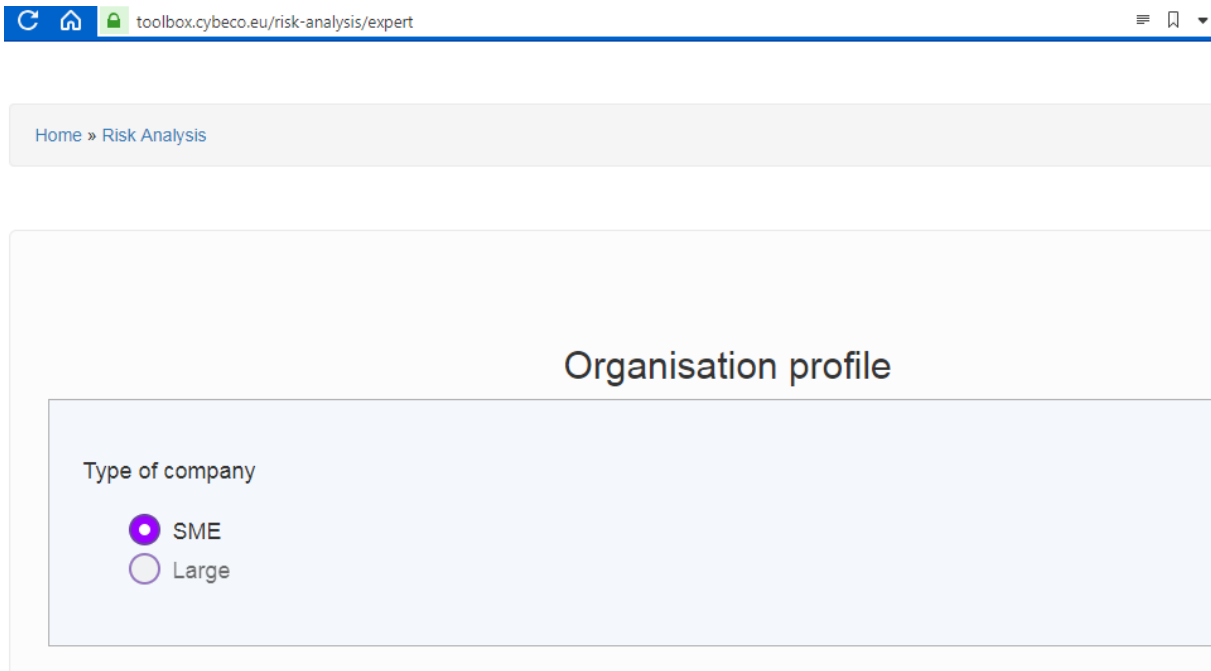


Figure 9: CYBECO toolbox - large companies

### 6.2.2 Scenario 2: Insurance fraud for an SME in the professional services sector

#### *Background:*


This scenario is important since it deals with a primary issue in the insurance sector: insurance claim fraud. The key objectives of this use-case involves three main factors against which the model needs to be checked.

1. The claim is from an SME, i.e. the resources allocated to processing and verification the claim cannot be very high
2. The claim involves data loss which is usually covered by a typical cyber-insurance policy
3. The fraud performed is easy to implement but hard to detect - data is moved and deleted; it is temporarily unavailable till the claim is processed when it is brought back.

#### *Discussion:*

The toolbox has been implemented to handle the scenario of an SME

## D4.2: Use-Case Evaluation of the Methodology and Framework


[My Account](#)
[Log Out](#)

[HOME](#)
[KNOWLEDGE BASE](#)
[RISK ANALYSIS](#)
[RESULTS](#)
[CONTACT](#)


[Home](#) > [Risk Analysis](#)

### Technical Security Controls

<input checked="" type="checkbox"/> Boundary firewalls and internet gateways <div> <input type="checkbox"/> Required for compliance           </div> <div> <input checked="" type="checkbox"/> Already implemented           </div> <div>           Capital expenditure: € <input type="text"/> <a href="#">Indicative Value</a>            Annual operational expenditure: € 500 <a href="#">Indicative Value</a> </div>	①
<input checked="" type="checkbox"/> Secure configuration <div> <input type="checkbox"/> Required for compliance           </div> <div> <input type="checkbox"/> Already implemented           </div> <div>           Capital expenditure: € 500 <a href="#">Indicative Value</a>            Annual operational expenditure: € 300 <a href="#">Indicative Value</a> </div>	①
<input checked="" type="checkbox"/> Access control <div> <input type="checkbox"/> Required for compliance           </div> <div> <input type="checkbox"/> Already implemented           </div> <div>           Capital expenditure: € 200 <a href="#">Indicative Value</a>            Annual operational expenditure: € 450 <a href="#">Indicative Value</a> </div>	①
<input checked="" type="checkbox"/> Malware protection <div> <input type="checkbox"/> Required for compliance           </div> <div> <input checked="" type="checkbox"/> Already implemented           </div> <div>           Capital expenditure: € <input type="text"/> <a href="#">Indicative Value</a>            Annual operational expenditure: € 500 <a href="#">Indicative Value</a> </div>	①
<input type="checkbox"/> Backup <div> <input type="checkbox"/> Required for compliance           </div> <div> <input type="checkbox"/> Already implemented           </div> <div>           Capital expenditure: € <input type="text"/> <a href="#">Indicative Value</a>            Annual operational expenditure: € <input type="text"/> <a href="#">Indicative Value</a> </div>	①
<input type="checkbox"/> Intrusion detection <div> <input type="checkbox"/> Required for compliance           </div> <div> <input type="checkbox"/> Already implemented           </div> <div>           Capital expenditure: € <input type="text"/> <a href="#">Indicative Value</a>            Annual operational expenditure: € <input type="text"/> <a href="#">Indicative Value</a> </div>	①
<input type="checkbox"/> DDoS protection <div> <input type="checkbox"/> Required for compliance           </div> <div> <input type="checkbox"/> Already implemented           </div> <div>           Capital expenditure: € <input type="text"/> <a href="#">Indicative Value</a>            Annual operational expenditure: € <input type="text"/> <a href="#">Indicative Value</a> </div>	①
<input type="checkbox"/> Other technical security controls <div> <input type="checkbox"/> Required for compliance           </div> <div> <input type="checkbox"/> Already implemented           </div> <div>           Capital expenditure: € <input type="text"/> <a href="#">Indicative Value</a>            Annual operational expenditure: € <input type="text"/> <a href="#">Indicative Value</a> </div>	①

[< Previous](#)
Page 9 out of 13
[Next >](#)

#### Fundings



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 742020.

The website reflects only the view of the author(s) and the Commission is not responsible for any use that may be made of the information it contains.

#### Menu

- Home
- Knowledge Base
- Risk Analysis
- Results
- Contact

#### Contact Us

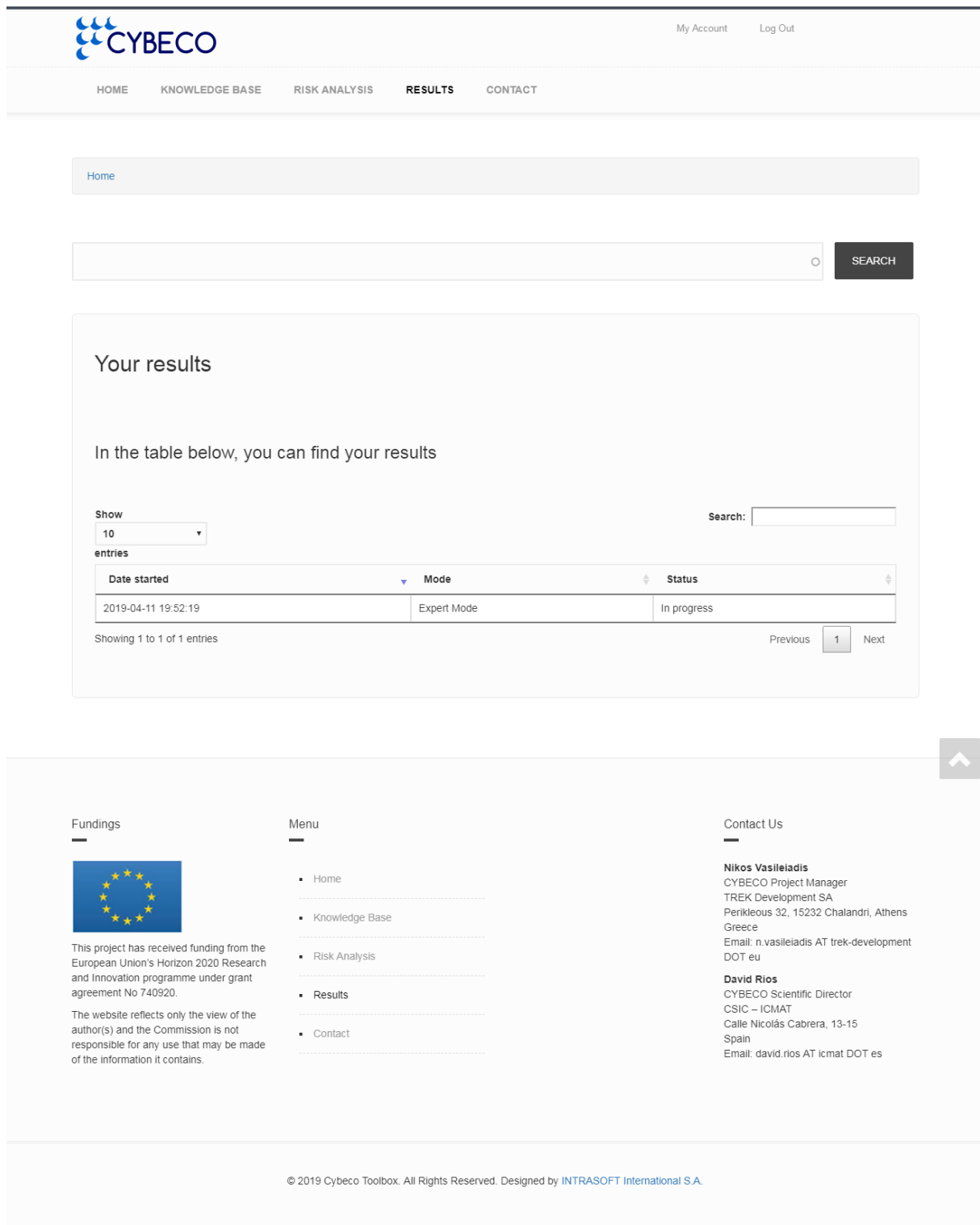
**Nikos Vasileiadis**  
CYBECO Project Manager  
TREK Development SA  
Perikleous St, 15232 Chalandri, Athens  
Greece  
Email: n.vasileiadis AT trek-development DOT eu

**David Rios**  
CYBECO Scientific Director  
CSIC - ICMAT  
Calle Nicolás Cabrera, 13-15  
Spain  
Email: david.rios AT icmat DOT es

© 2019 Cybeco Toolbox. All Rights Reserved. Designed by INTRASOFT International S.A.

Figure 10: CYBECO toolbox input for scenario 2

## D4.2: Use-Case Evaluation of the Methodology and Framework



**Header:**

- My Account
- Log Out
- HOME
- KNOWLEDGE BASE
- RISK ANALYSIS
- RESULTS**
- CONTACT

**Search Bar:**

 **SEARCH**

**Your results**

In the table below, you can find your results

Show:  entries


Search:

Date started	Mode	Status
2019-04-11 19:52:19	Expert Mode	In progress

Showing 1 to 1 of 1 entries

Previous **1** Next

**Fundings**



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 740920.

The website reflects only the view of the author(s) and the Commission is not responsible for any use that may be made of the information it contains.

**Menu**

- Home
- Knowledge Base
- Risk Analysis
- Results**
- Contact

**Contact Us**

**Nikos Vasileiadis**  
CYBECO Project Manager  
TREK Development SA  
Perikleous 32, 15232 Chalandri, Athens  
Greece  
Email: n.vasileiadis AT trek-development DOT eu

**David Rios**  
CYBECO Scientific Director  
CSIC – ICMAT  
Calle Nicolás Cabrera, 13-15  
Spain  
Email: david.rios AT icmat DOT es

© 2019 Cybeco Toolbox. All Rights Reserved. Designed by INTRASOFT International S.A.

Figure 11: CYBECO toolbox simulation for scenario 2

---

## D4.2: Use-Case Evaluation of the Methodology and Framework

---

The toolbox is able to take the various security control implementations into consideration as can be seen in Figure 10 and Figure 11. These factors also take regulatory requirements into consideration. Considering these factors, a post-event analysis can be completed, and a likelihood of fraud could be computed. It can hence be concluded that the toolbox can satisfactorily handle the identification of controls requirement for this scenario.

### 6.2.3 Scenario 3: Manipulation of Products / Services for a large company in the manufacturing sector

#### *Background:*

This scenario corresponds to the use-case 4. This use-case primarily focuses on a large company with less cyber footprint due to the nature of its business. Further, the implications of an attack lead to a more severe attack that impacts business continuity, brand and regulatory compliance. This tests the effectiveness of the toolbox for “Cyber-Physical Systems”.

#### *Discussion:*

The toolbox is an implementation that incorporated the previously described model for simulating the threat analysis. It also includes several components and defines the parameters to be incorporated into the model.

The parameters involved in the creation of the model for a large enterprise are varied and unique. These require several key considerations and several times involve customized considerations. The toolbox in its current state requires input on all the variables involved and is unable to satisfy these constraints for the “large enterprise” (see Figure 9).

It can hence be concluded that at the time of this review, the toolbox is still in the process of designing the components for effective use by large enterprises.

## 7 Conclusion

This concludes the validation of the toolbox. The toolbox is currently able to handle inputs for SME and predict the controls required as well as risk estimation. The implementation requires time for the results to be evaluated due to the time taken by the simulation. The toolbox works as expected and can be considered a successful preliminary design satisfying the original objectives. Further work needs to be done to complete the implementation of the toolbox for a large enterprise as part of future enhancements.

## **Part III: Security expert review**

### **Abstract:**

As a result of the June project review AXA conducted a security expert review of the toolbox. The feedback provided by AXA Group Security information security professionals we used to improve the toolbox's coverage of threats, risk and incidents beyond the use-cases and scenarios.

## **8 Introduction**

This section describes the feedback received following the security expert review in October 2018 of the first iteration of the toolbox and the actions taken to respond to these feedback. Section 9 provides an overview of the information security expert review conducted within AXA with a very high level summary of the comments received in regards to threats, security controls and information security terminology used throughout the toolbox.

Section 10 provides the list of improvements gathered and shared with the CYBECO partners to consider in the further development of the toolbox and that were integrated in the latest version of the risk assessment simulations (both non-expert mode and expert mode)



## 9 Expert review of October 2018

### 9.1 Objective

The objective of this review was to provide expert evaluation of the content of the first version of the Toolbox, in terms of information security and cyber security terms, concepts and information provided and used within it. The focus of the review was to gather feedback on the risk assessment tool and provide it to the project partners to consider during further work on the toolbox.

### 9.2 Method

Information security experts with AXA Group Security were given access to the CYBECO toolbox and were asked for their comments on the information security content of the toolbox. The comments were gathered and organised by the AXA Group Security Research Team.

### 9.3 Feedback

The review feedback received can be summarised as follow. The reviewers noted:

- An unrealistically limited number of threats considered to perform a risk assessment.
- A mix of confidentiality, availability and integrity consideration in the incidents.
- A significant gap between the toolbox and basic control recommendations as they are published by the UK Government - UK Cyber Essentials - or Australia - Australian Signals Directorate.
- The terminology regarding threats and controls could be improved, from an information security and cyber security perspective.

## 10 Areas for improvement

### 10.1 Prioritised security controls

The AXA Group Security Research Team provided the partners with an improved, prioritised list of security controls, using the UK Cyber Essentials standard, the Information Security Forum (ISF) Standard of Good Practices for Information Security 2018 and AXA's own Minimum Technical Security Baseline (MTSB) to consider in the next iteration of the risk assessment simulation tool.

The security controls are in the table below.

**Table 0-2. Security Controls**

## D4.2: Use-Case Evaluation of the Methodology and Framework

<b>Technical controls</b>		<b>Non-Technical controls</b>		<b>Physical controls</b>	
* Firewall & Internet Gateways	1 To prevent unauthorised network traffic from gaining access to networks, or leaving networks, network traffic are routed through a well-configured firewall prior to being allowed access to networks, or through a well-configured internet gateways before leaving the organisation's networks.	* Patch management/ Vulnerability management	1 To address technical vulnerabilities quickly and effectively, reducing the likelihood of them being exploited, which could result in serious security incidents, a process is established for the identification and remediation of technical vulnerabilities in business applications, systems, equipment and devices (e.g., patch installation and vulnerability remediation).	Physical Protection	1 To restrict physical access to authorised individuals, ensure that critical facilities are available when required and to prevent important services from being disrupted by loss of, or damage to, equipment or services, all critical facilities (including locations that house critical technical infrastructure, industrial control systems and specialised equipment) are physically protected against accident or attack and unauthorised physical access.
* Secure configuration	2 To ensure servers operate as intended and do not compromise the security of computer installations or other environments, servers are configured to function as required, and to prevent unauthorised or incorrect updates.	Security policy	2 To document the direction on and commitment to information security, and communicate it to all relevant individuals, a comprehensive, documented information security policy is produced and communicated to all individuals with access to the organisation's information and systems.	Hazard Protection	2 To prevent services being disrupted by damage to critical facilities caused by fire, flood and other types of hazard, critical facilities (including locations that house critical technical infrastructure, industrial control systems and specialised equipment) are protected against fire, flood, environmental and other natural hazards.
* Access control	3 To ensure that only authorised individuals can access business applications, information systems, networks and computing devices, access control arrangements are established to restrict access to business applications, systems, networks and computing devices to authorised users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.	User awareness	3 To ensure individuals remain aware of the importance and need for information security on an ongoing basis, and maintain a security-positive culture throughout the organisation, individuals who have access to the information and systems of the organisation receive tailored and appropriate security messages communicated to them on a regular basis.	Power Supplies	3 To prevent critical services from being disrupted by loss of power, critical facilities (including locations that house critical technical infrastructure, industrial control systems and specialised equipment) should be protected against power outages.
* Malware protection	4 To protect the organisation against malware attacks and ensure malware infections can be addressed within defined timescales, systems throughout the organisation are safeguarded against all forms of malware by maintaining up-to-date malware protection software, and effective procedures for managing malware-related security incidents.	Acceptable Use Policy	4 To prevent individuals from inadvertently increasing risk to information and systems, acceptable use policies (AUPs) are established, which define the organisation's rules on how each individual (e.g. an employee or contractor) can use information and systems, including software, computer equipment and connectivity.	Portable Storage Devices	4 To ensure that sensitive information stored on portable storage devices is protected from unauthorised disclosure, the use of portable storage devices (e.g. USB memory sticks, external hard disk drives, media players and e-book readers) is subject to approval, access to them restricted, and information stored on them protected.
Backup	5 To ensure that, in the event of an emergency, essential information or software can be restored within critical timescales, backups of essential information and software are performed on a regular basis, according to a defined cycle.	Security incident management	5 To identify and resolve information security incidents quickly and effectively, minimise their business impact and reduce the risk of similar incidents occurring, information security incidents are identified, responded to, recovered from, and followed up using an consistent and documented information security incident management process.		
Intrusion Detection	6 To identify suspected or actual malicious attacks and enable the organisation to respond before serious damage is done, intrusion detection mechanisms are applied to critical systems and networks.	Information Security Risk Assessment	6 To enable individuals who are responsible for target environments to identify key information risks, evaluate them and determine the treatment required to keep those risks within acceptable limits, information risk assessments are performed for target environments (e.g. critical business environments, processes and applications (including those under development), and supporting technical infrastructure) on a regular basis.		
Wireless network	7 To ensure that only authorised individuals and computing devices gain wireless access to networks and minimise the risk of wireless transmissions being monitored, intercepted or modified, wireless access are subject to authorisation, authentication of users and computing devices, and encryption of wireless traffic (e.g., WPA2).	Business continuity	7 To enable critical business processes to be resumed to an agreed level, within an agreed time following a disruption, using alternative processing facilities, alternative business continuity arrangements (also known as disaster recovery plans) are established for individual business environments, and made available when required.		
Mobile devices	8 To ensure mobile devices do not compromise the security of information stored on them or processed by them, and prevent unauthorised access to information in the event they are lost or stolen, mobile devices (including laptops, tablets and smartphones) are built using standard technical configurations and subject to security management practices to protect information against loss, theft and unauthorised disclosure.	Suppliers and Vendor management process	8 To protect critical and sensitive information when being handled by external suppliers (including organisations in the supply chain) or when being transmitted between the organisation and external suppliers, information risks are identified and managed throughout all stages of the relationship with external suppliers.		
* Cryptography	9 To protect the confidentiality of sensitive information, preserve the integrity of critical information and confirm the identity of the originator of transactions or communications, cryptographic solutions are subject to approval, documented and applied throughout the organisation.	Information Classification and Handling	9 To ensure that information is protected in line with its assigned level of classification, an information classification scheme is established (supported by information handling guidelines) that applies throughout the organisation, based on the confidentiality of information.		
* DDoS Protection	10 To ensure systems and information remain available, Distributed Denial of Service (DDoS) protection is implemented to protect public-facing systems.	Audit	10 To identify both non-compliances and information risks associated with target environments, security audit fieldwork are conducted for target environments and include collecting relevant background material, performing security audit tests and recording the results of the tests.		
* Other technical controls	11 To further protection the organization's assets, further technical controls are implemented, such as systems monitoring, email protection and filtering, data leak prevention (DLP), single sign-on (SSO) and biometric authentication.	* Other non-technical controls	11 To further protection the organization's assets, further non-technical controls are implemented, such as security governance, security strategy, threat intelligence, forensics investigation, secure system development methodology and information sharing.		

\*: UK Cyber Essentials  
S: Specialised controls (i.e., beyond the fundamental ones).

## 10.2 Threats and terminology

The AXA Group Security used the ISF Information Risk Assessment Methodology 2 (IRAM2) to improve the terminology regarding threat as well as reorganising the threat in three categories:

- Environmental threats (e.g., fire, flood, natural disasters)
- Accidental threats (e.g., employee error, supplier or customer error)
- Adversarial threats (e.g., data exfiltration and manipulation, denial of services and non-targeted threats such as malware)

It was agreed that for the non-expert mode of the toolbox, it was preferable to focus on the incidents that may concern the toolbox users as they may not have the knowledge to respond accurately to the threats they are concerned about. The recommendation from AXA Group Security Research Team was to replace accidental and adversarial threats with three risk and incidents entries. For each, the list of relevant threats was provided, as described below:

- Availability: shutdown of website or essential services due to hack or malware
  - All the environmental ones
  - Accidental threats (error, misconfiguration)
  - Virus and Malware
  - Unavailability of server hosted by the IT supplier (e.g., DDoS)
- Integrity: manipulation of produce, services or information
  - Accidental threats
  - Virus malware
  - Unauthorized modification of information
- Confidentiality: exfiltration of personal or confidential information
  - Accidental threats
  - Virus malware
  - Disclosure of information stored in the IT infrastructure to unauthorized parties

## 11 Conclusion

The researchers responded to the experts' comments and recommendations and made the necessary changes so that the second iteration of the risk assessment simulation uses an improved list of security controls and threats as well as an improved terminology which is better aligned to the information security expert community.

## D4.1: Cyber-Insurance Use-Cases and Scenarios

### Appendix: Tables referenced in the scenario descriptions

Table 1: Assets

This table provides a list of groups of assets and the typical assets each group include.

Group	Components
Process	R&D Sales Design Production and manufacturing Accounting Compliance
Information	Intellectual Property / Patents Customer data Personally Identifiable Information (PII) data Payment Card Information Marketing research and analysis Financial statements Business Intelligence Executive Management Information Source code
Hardware	IT infrastructure Production lines Large Infrastructure (Real-estate, etc.)
Software	Customer relationship management (CRM) Accounting IT (Active Directory) Productivity (Sharepoint, etc.)
Personnel	Executive management Finance Network administrators Security personnel Employees

## D4.1: Cyber-Insurance Use-Cases and Scenarios

Table 2: Technical types of attack

This table provides examples of technical attacks.

Label	Description
Alteration attack	This form of attack leverages unauthorized code and data alterations in order to obtain a change in the intended execution by means of code and data integrity corruption <sup>14</sup> .
Botnet	A botnet is a network of remotely controlled machines used to launch wide-scale denial of service (see DoS) attacks against specifically targeted resources <sup>15</sup> .
Brute-force attack	In this form of attack, the attacker attempts to identify a password or an encryption key through exhaustive checks until the correct string is identified.
Denial of Service (also Distributed)	A Denial of Service attack consists in an attempt to prevent users from accessing data or services provided by an information system <sup>16</sup> .
Eavesdropping/Traffic analysis	This form of attack consists in capturing and analysing network data packets in order to identify any information that may be relevant for other types of exploits.
Email spoofing	This form of attack consists in sending emails with a false sender identity, so that the receiver is misled to believe the message originates from another sender.
IRC <sup>17</sup> Flooding	This attack is a specific case of DoS attacks, and proceeds by either disconnecting users from the IRC

<sup>14</sup> <https://www.sans.edu/cyber-research/security-laboratory/article/alter-code>

<sup>15</sup> <https://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299>

<sup>16</sup> <https://www.us-cert.gov/ncas/tips/ST04-015>

<sup>17</sup> Internet relay chat is a text communication protocol.

#### D4.1: Cyber-Insurance Use-Cases and Scenarios

	servers, or by severely degrading the server's performance.
Malicious code/payload	This is a generic family of attacks all of which involve harmful code or script designed to be executed by programs, operating systems, web servers, and any other IT device, resulting in undesired effects.
Man-in-the-middle	This form of attack is a specific case in the eavesdropping type of attacks, in which a threat actor interposes between the sender and the receiver and misleading them into believing their communication line is direct and secure. This allows to either intercept confidential information, or alter it unknowingly to the legitimate communication participants <sup>18</sup> .
Masquerading	This type of attack consists in an attacker posing as a user with legitimate rights and authorizations in order to access to data or network systems.
Replay attack	A particular case of both traffic analysis and masquerade attacks, in which authentic data, collected during a previous eavesdropping session, is resent by the threat actor in order to masquerade her/his identity as a legitimate user.
Phishing	This attack type aims at obtaining confidential information by leveraging techniques such as email spoofing.
Resource enumeration and browsing	This is a type of attack through which the threat actor is able to obtain from a targeted system the list of resources that are present in the system, therefore enabling the threat actor to refine the targeting process of such resources and their consequent browsing.
Viruses, malware	Viruses and malware are types of malicious code/payload with various objectives, among which can

<sup>18</sup> F. Callegati, W. Cerroni and M. Ramilli, "Man-in-the-Middle Attack to the HTTPS Protocol," in *IEEE Security & Privacy*, vol. 7, no. 1, pp. 78-81, 2009.





Reference : CYBECO-WP4-D4.1-v1.0-AXA  
Version : 1.0  
Date : 2018.30.04

---

#### D4.1: Cyber-Insurance Use-Cases and Scenarios

---

	be mentioned replication, data manipulation or destruction, etc.
--	--

#### D4.1: Cyber-Insurance Use-Cases and Scenarios

Table 3: Impact

This table details the typical impacts an organisation may face when the target of an attack. The impact is the consequence an attack may have on an organisation's ability to conduct its operations and provide the services it delivers.

Label	Description
Loss of data and software	Information destruction and/or leakage due to data breach and consequent data exfiltration.
Loss or damage to physical properties	Product loss or undesired alteration of its specifications.
Product recall	Product retrieval following the detection of defects in said products.
Fraud	Concealment or distortion of facts leading to undue rights or compensations.
Theft of money, securities	Undue appropriation of financial means.
Extortion	The action of obtaining rights or financial means through threats or violent actions.
Privacy liability	This liability includes the claims which arise following breaches of private or sensitive data.
Identity theft	The intentional use of the identity of another physical or moral person.
Failure to render the service	The inability to provide agreed services on a contractual agreement.
Security liability	This liability includes the claims which arise following security breaches.
Property damage, personal injury	Damage and/or destruction of property, including injury to persons and casualties.
Media liability	The liability including claims of infringement of copyright, plagiarism, and defamation.

#### D4.1: Cyber-Insurance Use-Cases and Scenarios

Product liability	The act of engaging the responsibility of the provider or supplier of a product following damage caused by the product under scrutiny.
Failure to supply	Inability to provide agreed products.
Management liability	Claims and/or allegations on specific responsibilities targeting the liability of directors or officers of an organization.
Breach of duty	Failure to provide the expected functions and services associated with a certain position for an individual, or with an organization providing products or services.
Loss of competitive advantage	Strong reduction or even complete loss of knowledge providing competitive advantage such as intellectual property, commercially sensitive information, strategic information, etc.
Brand and reputational damage	Decrease in the positive perception that the general public, the market, or investors have on the brand and reputation of an organization.
Non-compliance with regulation	Lack of conformity with respect to regulations.
Business interruption	Discontinuity of business-related processes and tasks.

## D4.1: Cyber-Insurance Use-Cases and Scenarios

Table 4: Identification and response process

This table provides a list of incident identification and response processes, differentiated by the level of required information security capabilities and skills to be implemented effectively in an organisation.

Process ID	Process	Required information security capabilities and skills
1	The process starts with a set of events which are collected from several sources, including human and software. If the set of events matches with a given pre-defined use case corresponding to a specific alert, then the alert is issued. The level 1 of the Security Operations Center (SOC) oversees the validation or invalidation of the alert. In case the alert is qualified as a false positive, then it is documented as such and details are provided on the reasons behind the qualification as false positive. If the alert is qualified as true positive, then its severity is assessed. The assets that would be impacted by such an alert are evaluated. A ticket is created to what corresponds now to a confirmed incident. From this stage, the incident is handled by the incident response team. If the incident is major, then it corresponds to the qualification of crisis, and thus involving also the crisis management and business continuity team.	This process requires an internal team of experts to monitor events, triage and evaluate alerts and then respond. This type of internal capabilities and skills are typically found in large organisations
2	The process for a medium-size company is partially similar to the one for large companies. The first difference is that the collection and analysis of events is most likely to be outsourced to an external security monitoring provider. The security monitoring provider follows the same process as an internal SOC, and finally issues reports on alerts and identified incidents to the client company. Then, the respective officers in the medium-size company in charge of cybersecurity and/or asset protection follow up with identified actions addressing countermeasures, remediation, and business continuity. It should be noted that this may involve additional third-party providers, such as data backup	The process requires the same level of capabilities and skills but from a lower number of people as part of the activities are outsourced to a service provider. The is typically a process used in mid-size organisations.

#### D4.1: Cyber-Insurance Use-Cases and Scenarios

	companies, cloud service providers, public cybersecurity agencies, etc.	
3	<p>The identification and response process for an SME is significantly simpler than the previous two. For generalization purposes, it is safe to assume the implementation and deployment of minimal baseline incident detection measures, such as anti-virus software and cloud data backup solutions. Unless the SME outsources the incident detection process to a professional cybersecurity company, or even to the cloud services provider, it is very likely that the incident detection will occur when day-to-day activities are impacted by an ongoing or past attack. The response process will in many cases be undefined and will be decided on an ad-hoc basis. Provider and customer management will be the first concern when addressing a serious issue, followed by the business impact assessment and the insurance claim if relevant.</p>	<p>This process is usually applied in small organisations where resources dedicated to information security are very limited and rarely full time.</p>

#### D4.1: Cyber-Insurance Use-Cases and Scenarios

Table 5: Safeguards and countermeasures

This table provides a list of safeguards and countermeasures that can prevent or mitigate the impact of an attack on an organisation.

Type	Description
Business Continuity Plan	Set of processes which enable an organization to maintain operations during negative events or threat occurrences.
Security Policy	Formal document stating the plans of an organization for protecting its assets.
Common Technical Barriers: Antivirus/Firewall/ Intrusion Detection System/ Data Backup Solution	Technical barriers include all hardware and software solutions which either do not allow threat actors in achieving their objectives, or detect threat actors before, during and after an attack, or compensate for negative impacts in case of a successful attack.
Secure Configuration	Security measures and parameters defined and implemented in such a way as to reduce vulnerabilities.
Awareness Training	Training methods and processes which increase the education and sensitivity level of employees on matters of security.
Honeypots	Security countermeasure consisting of IT assets which appear as very appealing, but with no real value, that an organization deploys in order to deflect the attack attempts from threat actors.
Incident Response	The process, or set of processes, that defines the sequence of actions to be carried in order to detect, react, and provide response to cybersecurity incidents.
Security Personnel / Data Protection Officer	The set of employees whose functions consists in fulfilling the security day-to-day operations and activities, along with

#### D4.1: Cyber-Insurance Use-Cases and Scenarios

	officers having specific key roles in a security policy.
Information Sharing Programs	Specifically designed and implemented processes and enabling technology for sharing relevant information in a secure and instructive way.
Inventory of Assets	Exhaustive database of raw materials, hardware, software, products, services, and all other assets used in maintaining business operations and client delivery of services and goods.
Continuous Vulnerability Assessment and Remediation	The process of proactive identification and correction of vulnerabilities reported through any source, including regular scans and vendor reports.

Table 6: Levels of financial impact

Level	Threshold
Low	Impact < € 500 000
Medium	€ 500 000 < Impact < € 5 000 000
High	€ 5 000 000 < Impact < € 50 000 000
Very high	€ 50 000 000 < Impact < € 100 000 000
Critical	Impact > 100 000 000