

## D5.3: CYBECO Toolbox Prototype 1.0

---

# CYBECO

## Supporting Cyber-insurance from a Behavioural Choice Perspective

### D5.3: CYBECO Prototype 1.0

**Due date: M14**

**Abstract:**

This report describes the CYBECO Prototype version 1.0.

Dissemination Level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	x
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)	



---

**D5.3: CYBECO Toolbox Prototype 1.0**

---

**Table of Contents**

1	Introduction .....	4
2	CYBECO Toolbox v1.0 Functionality .....	5
2.1	KB Module .....	5
2.2	Risk Analysis Module .....	8
3	CYBECO Toolbox v1.0 Implementation Details .....	20

## D5.3: CYBECO Toolbox Prototype 1.0

---

### Table of Figures

Figure 1 CYBECO Toolbox Homepage .....	5
Figure 2 KB Taxonomy .....	6
Figure 3 Taxonomy subcategories .....	6
Figure 4 KB Term and related terms .....	7
Figure 5 Breadcrumb menu.....	7
Figure 6 Search with autocomplete .....	8
Figure 7 Risk Analysis cases .....	9
Figure 8 Risk case 1: Input screen.....	10
Figure 9 Insurance packet selection .....	11
Figure 10 Risk Analysis results, portfolio ranking table .....	11
Figure 11 Insurance costs diagram .....	12
Figure 12 Risk Analysis information .....	13
Figure 13 Risk Case 2 input screen .....	14
Figure 14 Risk case 2 results screen .....	15
Figure 15 Results screen: Risk Analysis information .....	16
Figure 16 R-server based input screen.....	17
Figure 17 R-server based input screen (part 2).....	18
Figure 18 CYBECO Toolbox Architecture .....	20

# 1 Introduction

The CYBECO Toolbox is a web application that comprises two main modules:

- A Knowledge Base (KB) with cybersecurity and cyber insurance related content. The KB contains hierarchical taxonomies of entities such as cyber-insurance use cases and scenarios (provided by WP4), threats and security controls. All these entities in the KB will be interconnected; for example, a cyber-insurance scenario may include several threats and security controls.
- A Risk Analysis System that provides users with the means to search and test and experiment with a set of Risk Analysis cases.

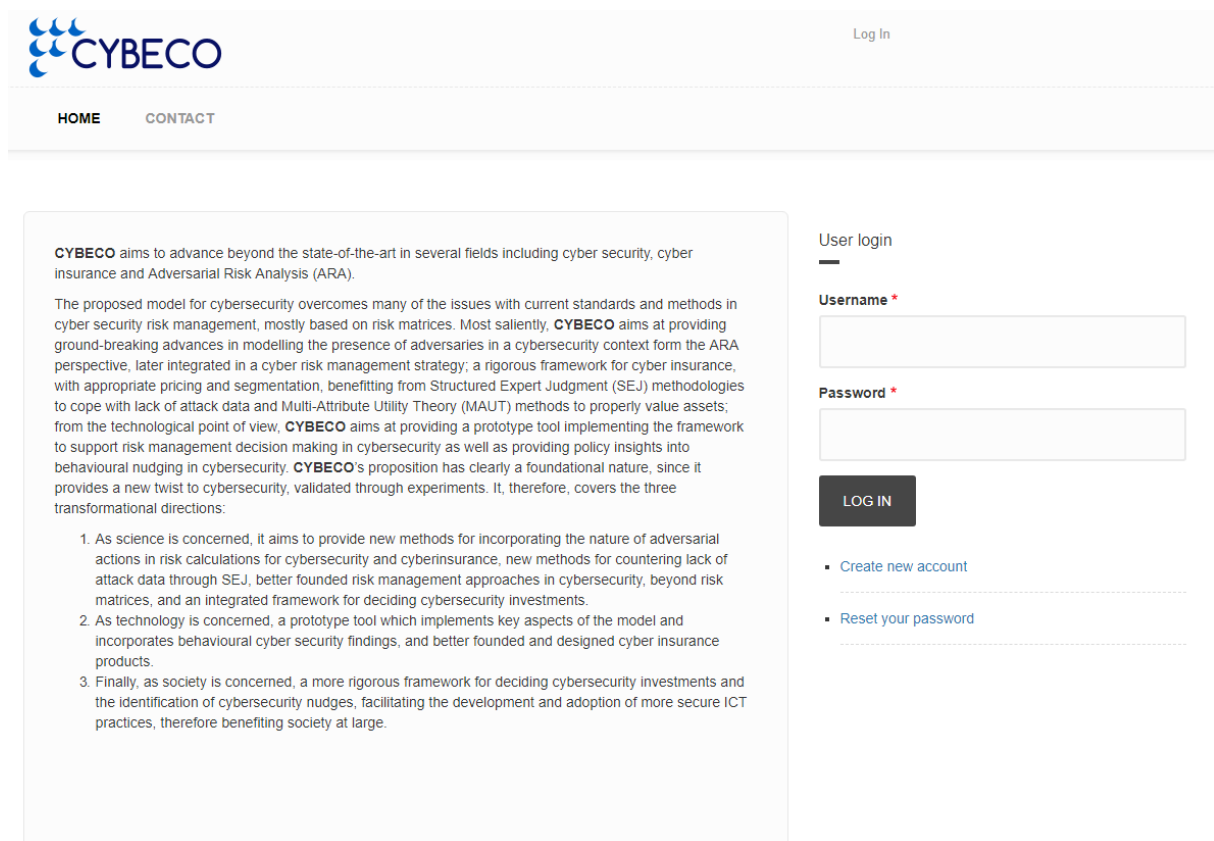
The following Risk Analysis cases are implemented CYBECO Toolbox 1.0:

- A single SME facing cybersecurity risks: This case is from the perspective of the SME decision-making aiding it to choose the optimal cyber security portfolio and cyber insurance product.
- Risk analysis an SME (insurance company perspective): it aids the decision on whether to insure a particular SME or not.

## D5.3: CYBECO Toolbox Prototype 1.0

## 2 CYBECO Toolbox v1.0 Functionality

CYBECO Toolbox is a web application that requires user registration. After registration, an authenticated user can access the KB and the risk analysis module. An unauthenticated user can only access the homepage and the contact page.



The screenshot shows the CYBECO Toolbox homepage. At the top left is the CYBECO logo, and at the top right is a 'Log In' link. Below the logo is a navigation bar with 'HOME' and 'CONTACT' links. The main content area is divided into two columns. The left column contains a paragraph about CYBECO's goals and a list of three points. The right column contains a 'User login' section with fields for 'Username' and 'Password', a 'LOG IN' button, and links for 'Create new account' and 'Reset your password'.

**CYBECO** aims to advance beyond the state-of-the-art in several fields including cyber security, cyber insurance and Adversarial Risk Analysis (ARA).

The proposed model for cybersecurity overcomes many of the issues with current standards and methods in cyber security risk management, mostly based on risk matrices. Most saliently, **CYBECO** aims at providing ground-breaking advances in modelling the presence of adversaries in a cybersecurity context from the ARA perspective, later integrated in a cyber risk management strategy; a rigorous framework for cyber insurance, with appropriate pricing and segmentation, benefitting from Structured Expert Judgment (SEJ) methodologies to cope with lack of attack data and Multi-Attribute Utility Theory (MAUT) methods to properly value assets; from the technological point of view, **CYBECO** aims at providing a prototype tool implementing the framework to support risk management decision making in cybersecurity as well as providing policy insights into behavioural nudging in cybersecurity. **CYBECO**'s proposition has clearly a foundational nature, since it provides a new twist to cybersecurity, validated through experiments. It, therefore, covers the three transformational directions:

1. As science is concerned, it aims to provide new methods for incorporating the nature of adversarial actions in risk calculations for cybersecurity and cyberinsurance, new methods for countering lack of attack data through SEJ, better founded risk management approaches in cybersecurity, beyond risk matrices, and an integrated framework for deciding cybersecurity investments.
2. As technology is concerned, a prototype tool which implements key aspects of the model and incorporates behavioural cyber security findings, and better founded and designed cyber insurance products.
3. Finally, as society is concerned, a more rigorous framework for deciding cybersecurity investments and the identification of cybersecurity nudges, facilitating the development and adoption of more secure ICT practices, therefore benefiting society at large.

User login

Username \*

Password \*

LOG IN

[Create new account](#)

[Reset your password](#)

Figure 1 CYBECO Toolbox Homepage

### 2.1 KB Module

This module is used for organizing the CYBECO knowledge base in a structured way, allowing the user to easily navigate through the entries. The KB is organized in a tree like structure, where each branch is a category, which might contain subcategories. In each subcategory the user can find the knowledge base entries that fall under it, or easily go back and choose a different subcategory.

### D5.3: CYBECO Toolbox Prototype 1.0

The CYBECO Knowledge Base contains cyber-security and cyber-insurance related content. More specifically, it contains hierarchical taxonomies of entities such as cyber-insurance use cases and scenarios, threats and security controls.

#### Subcategories

Risk	>
Threat	>
Digital System	>
Organisation	>
Security Actions	>
Impacts	>

Figure 2 KB Taxonomy

All the knowledge base entries that fall under the same subcategory are grouped together, and the user can easily access them.

#### Physical attack (deliberate/ intentional)

Threats of intentional hostage human actions

Terrorists attack	>
Damage from the warfare	>
Coercion, extortion or corruption	>
Unauthorized physical access / Unauthorised entry to premises	>
Information leakage/sharing	>

Figure 3 Taxonomy subcategories

Each entry provides a description of the term, and any related terms appear below it, allowing the user to click on them in order to see their more detailed description.

## D5.3: CYBECO Toolbox Prototype 1.0

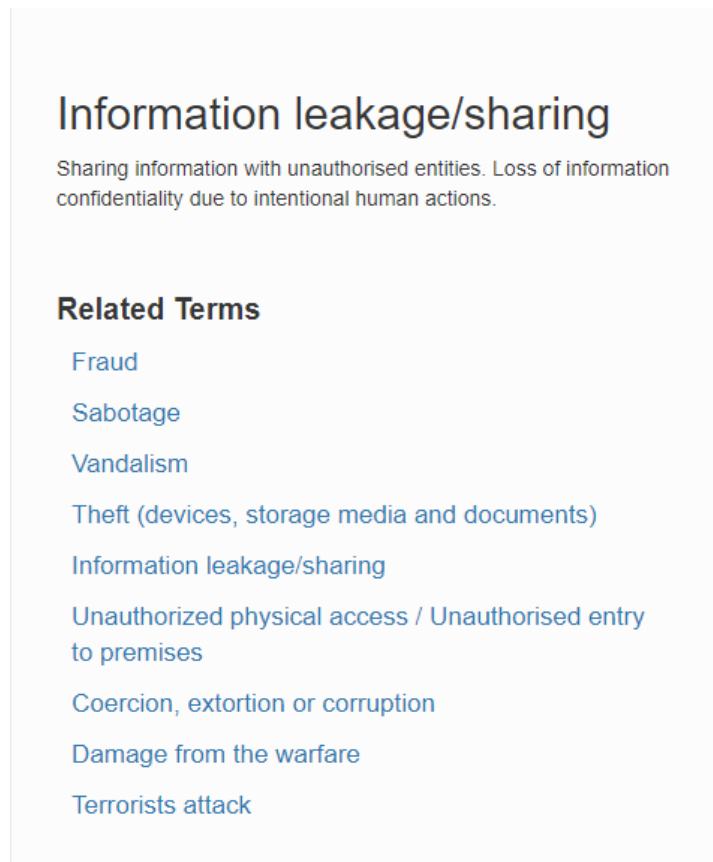


Figure 4 KB Term and related terms

The menu breadcrumb provides a path that appears on the top of the page for the logged-in users and assists with the navigation through the pages, by enabling the users to easily navigate to the parent elements.

Knowledge Base » Threat » Threat Action » Physical attack (deliberate/ intentional) » Information leakage/sharing

Figure 5 Breadcrumb menu

The KB search engine provides the search functionality with autocomplete which makes it easier for the user to search for terms.

### D5.3: CYBECO Toolbox Prototype 1.0

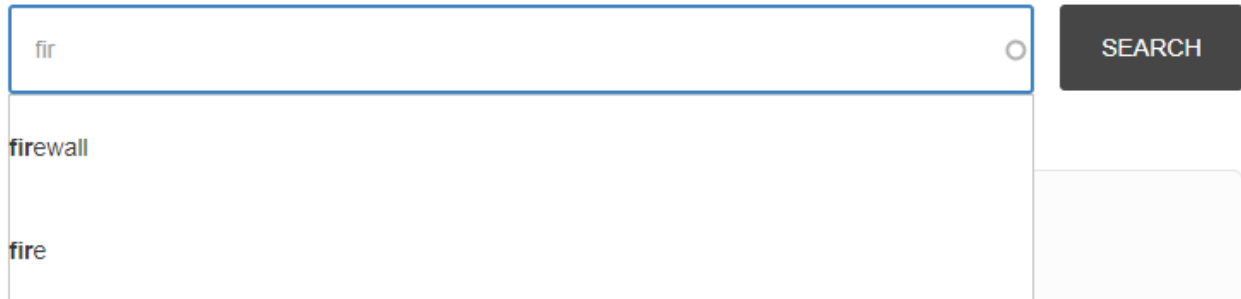


Figure 6 Search with autocomplete

## 2.2 Risk Analysis Module

The Risk Analysis module can be accessed by clicking on Risk Analysis on the main navigation bar, available only to the logged in user, providing links and short descriptions for the three risk cases.



## D5.3: CYBECO Toolbox Prototype 1.0

### Risk Cases

KB



#### Risk Analysis for an SME

This risk analysis template takes the perspective of the SME. It provides a tool for exploring the results of the risk analysis done with the CYBECO risk analysis framework.

KB



#### Risk analysis an SME (insurance company perspective)

This risk analysis template takes the perspective of the insurance company. It provides a tool for exploring the results of the risk analysis done with the CYBECO risk analysis framework.

Simulation



#### Risk Analysis for an SME

This risk analysis template takes the perspective of the SME. It provides a tool for exploring the results of the risk analysis done with the CYBECO risk analysis framework. This template is a demo version.

Figure 7 Risk Analysis cases

### D5.3: CYBECO Toolbox Prototype 1.0

By clicking on each risk case, the user is taken to an input page, specific for the selected risk case.

## Risk analysis template for an SME

This risk analysis template takes the perspective of the SME. It provides a tool for exploring the results of the risk analysis done with the CYBECO risk analysis framework.




**Overview of the use:**

1. The first screen will ask you to select the relevant security controls and insurance products that you want to consider in the risk analysis.
2. The second screen will provide an information dashboard with key risk analysis information, dynamically generated base on the elements you selected in the first screen.




**Description of the case**

The SME is dedicated to document management with 60 people and 90 computers. A cyber attack might affect, mainly, the online document management service. For confidentiality reasons, the number of relevant issues has been simplified and data conveniently masked. This simplification will allow us to better illustrate key modelling concepts and the overall scheme to follow for other case studies. Moreover, we include uncertain phenomena in which data are available and others in which it is not and, thus, we shall need to rely on expert judgement.





### Assets

Facilities	<input checked="" type="checkbox"/>	
Computer equipment	<input checked="" type="checkbox"/>	
Market share	<input checked="" type="checkbox"/>	




### Threats

Fire	<input checked="" type="checkbox"/>	
Computer virus	<input checked="" type="checkbox"/>	
Competitor attack (DDoS against website)	<input checked="" type="checkbox"/>	

### Available security control

Anti-fire system	<input checked="" type="checkbox"/>	
Firewall	<input checked="" type="checkbox"/>	
Risk mitigation procedures	<input checked="" type="checkbox"/>	
Cloud-based DDoS protection	<input checked="" type="checkbox"/>	

### Available insurance products

Traditional insurance	<input checked="" type="checkbox"/>	
Cyber insurance	<input checked="" type="checkbox"/>	
Comprehensive insurance	<input checked="" type="checkbox"/>	

### Cybersecurity budget

Cybersecurity budget € 18000

Figure 8 Risk case 1: Input screen

### D5.3: CYBECO Toolbox Prototype 1.0

At the top of each input page, the user can read a description of the case, and then he or she can make the desired choices before proceeding to generate the risk analysis results. Hovering the over the information symbol can provide some extra information and a link to the knowledge base entry for that term.

Traditional insurance ☒ ⓘ  
Cyber insurance ☒ ⓘ  
Comprehensive insurance ☒ ⓘ

All of the above. It costs € 500 if the anti-fire is installed, € 600 if the firewall or the DDoS system are installed, € 650 if the procedures are implemented and € 700 otherwise.

[Go to Knowledge Base](#)

Cybersecurity budget

Figure 9 Insurance packet selection

Clicking on Generate Risk Analysis button will take the user to the results page.

### Risk analysis information dashboard

#### Risk evaluation of security controls and cyber insurance

Based on the simulation, we rank the different combinations of security controls and insurance based on the expected total costs. These combinations are limited to those that can be bought with the cybersecurity budget of € 18000 .

Select a row to obtain further information on the probability of the different events and the expected impacts and costs.

Show  entries

Search:

Ranking based on utility ▲	Anti-fire system ⚙	Firewall selection ⚙	Risk mitigation procedures selection ⚙	Cloud-based DdoS protection system ⚙	Insurance ⚙	Expected final costs ⚙
1	Antifire	Firewall	No Procedure	1 tbps	Comprehensive	€ 18,431.43
2	Antifire	Firewall	No Procedure	1 tbps	Traditional	€ 19,503.51
3	No Antifire	Firewall	No Procedure	1 tbps	Comprehensive	€ 20,029.95
4	No Antifire	Firewall	Procedure	1 tbps	Traditional	€ 20,601.62
5	No Antifire	Firewall	No Procedure	1 tbps	Traditional	€ 23,696.87
6	Antifire	No Firewall	Procedure	1 tbps	Comprehensive	€ 25,154.16
7	Antifire	No Firewall	No Procedure	1 tbps	Comprehensive	€ 25,442.53
8	No Antifire	No Firewall	No Procedure	1 tbps	Comprehensive	€ 26,133.3
9	No Antifire	Firewall	Procedure	1 tbps	Comprehensive	€ 28,795.17
10	Antifire	No Firewall	Procedure	1 tbps	Traditional	€ 28,502.79

Filters:

All ▼

All ▼

All ▼

All ▼

All ▼

Showing 1 to 10 of 158 entries

Previous

1

2
3
4
5
...
16
Next

Figure 10 Risk Analysis results, portfolio ranking table

### D5.3: CYBECO Toolbox Prototype 1.0

The table on the results page contains all the cases that are related to the user's input. This table can be sorted based on any of its columns and it can also be filtered in order to include specific only choices.

Following this table there is a graphical representation of some indicative results of the risk case, displaying the correlation between the ranking based utility and the expected total costs.

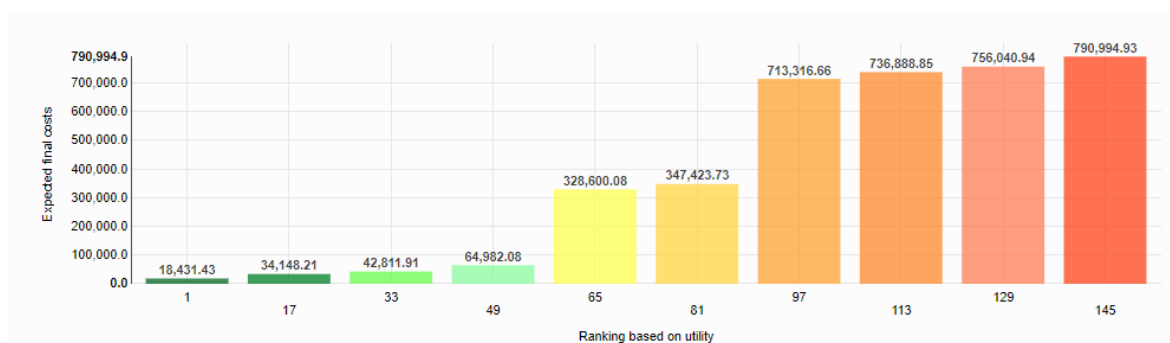


Figure 11 Insurance costs diagram

By selecting an entry on the results table, the user is navigated below the chart, where more detailed information about this specific result can be found.

### D5.3: CYBECO Toolbox Prototype 1.0



Figure 12 Risk Analysis information

All fields and charts change dynamically upon selecting a new entry on the table, allowing a more detailed view of each result. The user can return to the input page by clicking on the Return to input page button, where the previously made selections are still there, making small input changes possible without much effort.

The Insurance Perspective Risk Case provides a different input page.

### D5.3: CYBECO Toolbox Prototype 1.0

## Risk analysis template for an SME (insurance company perspective)

This template is a demo version. It describes a limited case of risk analysis with the purpose of demonstrating the risk analysis functionalities of the CYBECO Toolbox Prototype. It is an interactive and synthetic version of a cybersecurity risk analysis case based on the complete risk analysis described in the paper An Adversarial Risk Analysis Framework for Cybersecurity.

This risk analysis template takes the perspective of the insurance company. It provides a tool for exploring the results of the risk analysis done with the CYBECO risk analysis framework.




### Overview of the use:

1. The first screen will ask you to configure the insurance products.
2. The second screen will provide an information dashboard with key risk analysis information, dynamically generated base on the elements you selected in the first screen.




### Description of the case

The SME is dedicated to document management with 60 people and 90 computers. A cyber attack might affect, mainly, the online document management service. For confidentiality reasons, the number of relevant issues has been simplified and data conveniently masked. This simplification will allow us to better illustrate key modelling concepts and the overall scheme to follow for other case studies. Moreover, we include uncertain phenomena in which data are available and others in which it is not and, thus, we shall need to rely on expert judgement.





### Assets

Facilities	
Computer equipment	
Market share	

### Threats

Fire	
Computer virus	
Competitor attack (DDoS against website)	

### Security controls available to the user

Anti-fire system	
Firewall	
Risk mitigation procedures	
Cloud-based DDoS protection	

### Insurance selection




Coverage in percentage		Coverage range: 80 % - 100 %
Offer traditional insurance	<input checked="" type="checkbox"/> 	Traditional ins. price: € 200 - € 800
Offer cyber insurance	<input checked="" type="checkbox"/> 	Cyber ins. price: € 200 - € 800
Offer comprehensive insurance	<input checked="" type="checkbox"/> 	Comprehensive ins. price: € 200 - € 800

Figure 13 Risk Case 2 input screen

In this case the user can select the coverage range for the insurance, what type of insurance should be included in the results along with their price range.

### D5.3: CYBECO Toolbox Prototype 1.0

The results are again presented in a table, which offers the same sorting and filtering functionality as the one of the first risk case.

#### Risk analysis template for an SME (insurance company perspective)

This template is a demo version. It describes a limited case of risk analysis with the purpose of demonstrating the risk analysis functionalities of the CYBECO Toolbox Prototype. It is an interactive and synthetic version of a cybersecurity risk analysis case based on the complete risk analysis described in the paper An Adversarial Risk Analysis Framework for Cybersecurity.

This risk analysis template takes the perspective of the insurance company. It provides a tool for exploring the results of the risk analysis done with the CYBECO risk analysis framework.

##### Overview of the use:

1. The first screen will ask you to configure the insurance products.
2. The second screen will provide an information dashboard with key risk analysis information, dynamically generated base on the elements you selected in the first screen.

##### Description of the case

The SME is dedicated to document management with 60 people and 90 computers. A cyber attack might affect, mainly, the online document management service. For confidentiality reasons, the number of relevant issues has been simplified and data conveniently masked. This simplification will allow us to better illustrate key modelling concepts and the overall scheme to follow for other case studies. Moreover, we include uncertain phenomena in which data are available and others in which it is not and, thus, we shall need to rely on expert judgement.

#### Risk analysis template for an SME (insurance company perspective)

#### Risk evaluation of security controls and cyber insurance

Based on the simulation, we rank the different combinations of security controls and cyber insurance based on the expected total costs. The security controls are those selected by the user if Select a row to obtain further information on the probability of the different events and the expected impacts and costs.

Show

10

Search:

entries

Ranking based on utility	Traditional insurance price	Cyber insurance price	Comprehensive insurance price	Coverage	Insurance product selected	Expected final costs for insurance company
1	€ 400	€ 400	€ 400	100 %	Comprehensive	€ 57,549.31
2	€ 100	€ 100	€ 100	100 %	Comprehensive	€ 12,018.95
3	€ 600	€ 100	€ 600	90 %	Cyber	€ 44.46
4	€ 400	€ 100	€ 600	90 %	Cyber	€ 45.39
5	€ 200	€ 100	€ 200	90 %	Cyber	€ 49.73
6	€ 200	€ 100	€ 400	90 %	Cyber	€ 43.53
7	€ 800	€ 100	€ 1,000	90 %	Cyber	€ 50.04
8	€ 600	€ 100	€ 1,000	80 %	Cyber	€ 42.46
9	€ 800	€ 100	€ 800	80 %	Cyber	€ 33.64
10	€ 100	€ 100	€ 400	70 %	Cyber	€ 5.85

Filters:

All

All

All

All

All

Showing 1 to 10 of 546 entries

Previous

1

2

3

4

5

...

55

Next

Figure 14 Risk case 2 results screen

### D5.3: CYBECO Toolbox Prototype 1.0

Selecting a specific result will again take the user to a more detailed analysis of that entry. That information is again updated every time the user selected a new entry from the table.

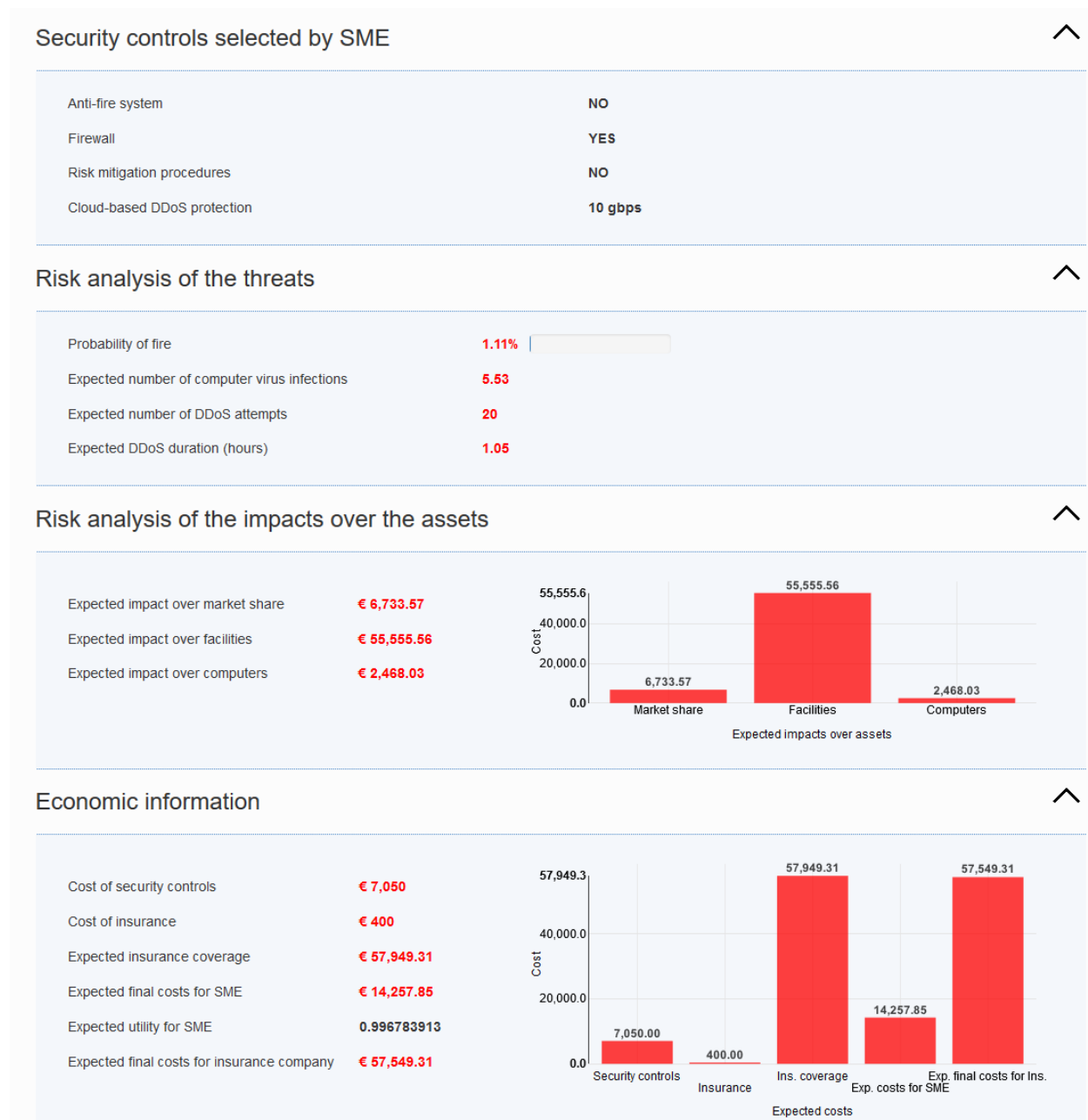


Figure 15 Results screen: Risk Analysis information

Clicking the Return to input page button, will of course again take the user to the previous page, where his or her selections are still active.



### D5.3: CYBECO Toolbox Prototype 1.0

While the previous two risk cases are Knowledge based, the third one is R Server Based, offering analysis for customizable cases. In this risk case, the user can provide a more detailed input, which will then be analyzed by the R Server, and return the results.

## Risk analysis template for an SME (R-server based)

*This template is a demo version. It describes a limited case of risk analysis with the purpose of demonstrating the risk analysis functionalities of the CYBECO Toolbox Prototype. It is an interactive and synthetic version of a cybersecurity risk analysis case based on the complete risk analysis described in the paper An Adversarial Risk Analysis Framework for Cybersecurity.*

This synthetic version provides a tool for exploring the results of the risk analysis done with the CYBECO risk analysis framework.




#### Overview of the use:

1. The first screen will ask you to configure the elements you are interested in (e.g., assets of the SME, threats, security controls and cyber insurance).
2. The second screen will provide an information dashboard with key risk analysis information, dynamically generated base on the elements you selected in the first screen.

#### Description of the case

The SME is dedicated to document management with 60 people and 90 computers. A cyber attack might affect, mainly, the online document management service. For confidentiality reasons, the number of relevant issues has been simplified and data conveniently masked. This simplification will allow us to better illustrate key modelling concepts and the overall scheme to follow for other case studies. Moreover, we include uncertain phenomena in which data are available and others in which it is not and, thus, we shall need to rely on expert judgement. Prices and rates refer to Spain, where the incumbent SME is located.

### Assets

<b>Facilities</b>	<input checked="" type="checkbox"/>	
Value of the facilities in Euros		€ 500000
<b>Computer equipment</b>	<input checked="" type="checkbox"/>	
Value of the computer equipment in Euros		€ 50000
Number of computers		100
<b>Market share</b>	<input checked="" type="checkbox"/>	
Value of the market share in Euros		€ 1550000
Number of days until the market share is lost		Min: 4 Max: 6





### Threats

<b>Fire</b>	<input checked="" type="checkbox"/>	
Probability of fire during a year		% 0.1
<b>Computer virus</b>	<input checked="" type="checkbox"/>	
Cost of repairing an infected computer in Euros		€ 60
Probability that a computer is infected during a month, without security controls		% 1
<b>Competitor attack (DDoS against website)</b>	<input checked="" type="checkbox"/>	
Attacking platform capability in gbps		6




Figure 16 R-server based input screen

### D5.3: CYBECO Toolbox Prototype 1.0

#### Available security control

<b>Anti-fire system</b>	<input checked="" type="checkbox"/>	
Cost of the anti-fire system	€ 300	
<b>Firewall</b>	<input checked="" type="checkbox"/>	
Cost of the firewall	€ 300	
<b>Risk mitigation procedures</b>	<input checked="" type="checkbox"/>	
Cost of the risk mitigation proc.	€ 300	
<b>Cloud-based DDoS protection</b>	<input checked="" type="checkbox"/>	
Cost of the DDoS protection	<div>2 gbps € 300</div> <div>5 gbps € 400</div> <div>10 gbps € 500</div> <div>1 tbps € 1000</div>	

#### Available insurance products

<b>Traditional insurance</b>	<input checked="" type="checkbox"/>	
Coverage in percentage	1 %	
Traditional ins. cost without sec. controls	€ 500	
Traditional ins. cost with anti-fire	€ 450	
Traditional ins. cost with firewall or DDoS prot.	€ 400	
Traditional ins. cost with procedure	€ 350	
<b>Cyber insurance</b>	<input checked="" type="checkbox"/>	
Coverage in percentage	1 %	
Cyber ins. cost without sec. controls	€ 500	
Cyber ins. cost with anti-fire	€ 450	
Cyber ins. cost with firewall or DDoS prot.	€ 400	
Cyber ins. cost with procedure	€ 350	
<b>Comprehensive insurance</b>	<input checked="" type="checkbox"/>	
Coverage in percentage	1 %	
Comprehensive ins. cost without sec. controls	€ 500	
Comprehensive ins. cost with anti-fire	€ 450	
Comprehensive ins. cost with firewall or DDoS prot.	€ 400	
Comprehensive ins. cost with procedure	€ 350	

#### Cybersecurity budget

Cybersecurity budget € 18000

Generate Risk Analysis

Figure 17 R-server based input screen (part 2)

---

### D5.3: CYBECO Toolbox Prototype 1.0

---

After filling these fields, the user will be taken to the results page, where the results are again organized in a table, and clicking each one will offer more information for that entry.

### D5.3: CYBECO Toolbox Prototype 1.0

## 3 CYBECO Toolbox v1.0 Implementation Details

The CYBECO Toolbox is developed in Drupal<sup>1</sup> 8, an open-source PHP software that includes a content management platform and a development framework. Drupal is modular, highly extendable and allows for the creation of custom complex document types and entities.

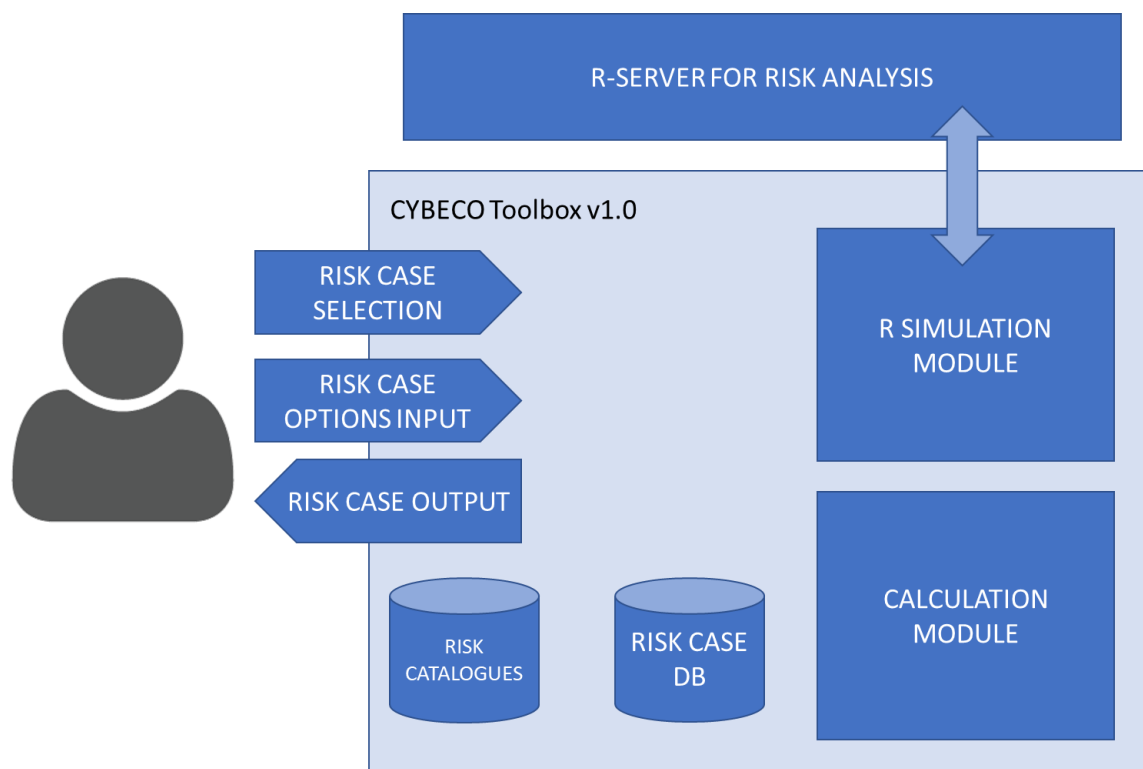


Figure 18 CYBECO Toolbox Architecture

### CYBECO Toolbox KB

The KB entities are designed as custom Drupal content types<sup>2</sup>. The content of the KB is organized using the Drupal built-in taxonomy module that can be used to connect, relate and classify the various KB entities. Moreover, extra Drupal modules have been used for the provision of the search engine.

<sup>1</sup> <https://www.drupal.org/about>

<sup>2</sup> <https://www.drupal.org/docs/7/understanding-drupal/content-types>

---

### D5.3: CYBECO Toolbox Prototype 1.0

---

#### Calculation Module

The Risk cases are implemented in the calculation module, which is designed and developed as a custom Drupal module. The module uses the Model-View-Controller (MVC) architectural pattern that separates the application into three main logical components: the model, the view, and the controller. Each of these components are built to handle specific development aspects of an application.

The implemented risk cases results are pre-simulated and stored in the Database (Risk Case DB in figure 17).

#### R-Simulation Module

The R-Simulation module will be available in the Toolbox version 2.

#### Server technologies

The software is installed in a dedicated Ubuntu Linux Server<sup>3</sup> in a Virtual machine. Apache<sup>4</sup> and Mysql<sup>5</sup> will be used for the web server and the database server, respectively.

---

<sup>3</sup> <https://www.ubuntu.com/server>

<sup>4</sup> <https://httpd.apache.org/>

<sup>5</sup> <https://www.mysql.com/>