
D6.3: Report with Findings of Experiments and Policy implications

CYBECO

Supporting Cyberinsurance from a Behavioural Choice Perspective

D6.3: Report with Findings of Experiments and Policy implications

Due date: 31/10/2018

Abstract:

This document corresponds to Deliverable 6.3 and presents the results and implications of the two online economic experiments designed and implemented within the scope of the CYBECO project. The first experiment 1, run with a sample of 4,800 subjects in four countries, analysed the ‘human actual behaviour’ when purchasing cyber protection and insurance. The second experiment was focused in testing and improving the CYBECO toolbox. Run with a sample of 2,000 potential users of the tool, this second experiment tested the usability of the toolbox and established the behavioural implications of five different designs of the interactive risk analysis dashboard of the CYBECO toolbox.

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)	

D6.3: Report with Findings of Experiments and Policy implications

Document Status

Document Title	Report with Findings of Experiments and Policy implications
Version	0.1
Work Package	6
Deliverable #	6.3
Prepared by	DevStat
Contributors	DevStat and Northumbria.
Checked by	IC-MAT and Intrasoftware
Approved by	
Date	31/10/2018
Confidentiality	PU

D6.3: Report with Findings of Experiments and Policy implications

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	0.1	October 31, 2018

D6.3: Report with Findings of Experiments and Policy implications

Table of Contents

1	Introduction	9
2	Experiment 1: Behavioural insights of CYBECO model.	10
2.1	Rationale of experiment 1	10
2.2	Methodology of experiment 1	11
2.2.1	Experimental Conditions	11
2.2.2	Behavioural measures.....	13
2.2.3	Experiment implementation	13
2.3	Selection of the cybersecurity strategy	15
2.3.1	Protection strategy.....	15
2.3.1.1	Socio-demographic profile	15
2.3.1.2	Cyber-risk attitude.....	17
2.3.1.3	Experimental factors	18
2.3.1.4	A model for protection strategy	19
2.3.2	Cyberinsurance strategy.....	21
2.3.2.1	Socio-demographic characteristics	21
2.3.2.2	Cyber-risk attitude.....	22
2.3.2.3	Experimental factors	23
2.3.2.4	A model for insurance strategy	24
2.3.3	Risk level of online behaviour	26
2.3.3.1	Socio-demographic characteristics	26
2.3.3.2	Cyber-risk attitude.....	29
2.3.3.3	Experimental factors	31
2.3.4	Complementarity of protection and insurance strategies	32
2.3.5	Moral hazard: insurance taken and online risky behaviour.	34
2.4	Learning process and updating of believes.....	36
2.4.1	Protection strategy.....	36
2.4.2	Cyberinsurance strategy.....	38
3	Experiment 2: Behavioural insights of CYBECO toolbox.	41
3.1	Rationale of experiment 2.....	41
3.2	Methodology of experiment 2	42
3.2.1	Experimental Conditions	42
3.2.2	Behavioural measures.....	48
3.2.3	Experiment implementation	48
3.2.4	Profile of the participants.....	49
3.3	Impact of the output design in the cybersecurity strategy of the SME	50
3.3.1	Protection strategy.....	50
3.3.1.1	Expertise of the potential user.....	52
3.3.2	Cyberinsurance strategy.....	53
3.3.2.1	Expertise of the potential user.....	55

D6.3: Report with Findings of Experiments and Policy implications

3.3.3	Cybersecurity strategy	57
3.3.3.1	Expertise of the potential user.....	59
3.4	Impact of the output design in the usability of CYBECO toolbox	60
3.4.1	Interaction with CYBECO toolbox	60
3.4.2	Usability of CYBECO toolbox	63
4	Conclusions and policy implications	67
4.1	Behavioural insights of cyberinsurance: implications for market development ...	67
4.2	The CYBECO model	68
4.3	Usability of the CYBECO toolbox.....	69
4.4	Optimal design of the output page.....	70

D6.3: Report with Findings of Experiments and Policy implications

List of Figures

Figure 1. C1: The attack is random	11
Figure 2. C2: The attack is intentional	12
Figure 3. Protection purchases by socio-demographic profile	16
Figure 4. Protection purchases by cyber-risk attitude.	18
Figure 5. Protection purchases by factor.	19
Figure 6. Cyberinsurance purchases by socio-demographic profile.	22
Figure 7. Cyberinsurance purchases by cyber-risk attitude.	23
Figure 8: Cyberinsurance purchases by factor.....	24
Figure 9. Risk level by socio-demographic profile.	28
Figure 10. Security behaviour by risk profile.	30
Figure 11. Risk level by factor.	31
Figure 12. Cyberinsurance purchases by protection purchases.	33
Figure 13. Cyberinsurance purchases by protection purchases and factor P.....	34
Figure 14. Risk level by protection and insurance strategies.	35
Figure 15. Transition between protection strategies (%).	37
Figure 16. Transition between protection strategies by experience of cyberattack.	38
Figure 17. Transition between cyberinsurance strategies.	39
Figure 18. Transition between cyberinsurance strategies by experience of cyberattack. ..	40
Figure 19. Treatment 1 (Expected - Losses)	43
Figure 20. Treatment 2 (Expected - Losses - Salience)	44
Figure 21. Treatment 3 (Expected - Gains)	45
Figure 22. Treatment 4 (Scenarios - Losses).....	46
Figure 23. Treatment 5 (Scenarios - Gains).....	47
Figure 24. Available protection and cybersinsurance strategies.....	48
Figure 25. Protection strategy by treatment	51
Figure 26. Protection strategy by field of expertise.....	52
Figure 27. Protection strategy by by buying expertise	53
Figure 28. Cyberinsurance strategy by treatment.	55
Figure 29. Cyberinsurance purchases by field of expertise.....	56
Figure 30. Cyberinsurance purchases by buying expertise.....	56
Figure 31. Cybersecurity strategies.	57
Figure 32. Cybersecurity strategies by treatment.	58
Figure 33. Purchases of the recommended option (%) by participants with experience	60
Figure 34. Ranking of options in the output page (Treatment 1).....	60
Figure 35. Detailed information of each option in the output page (Treatment 1).....	61
Figure 36. Number of displayed options by treatment.	62
Figure 37. Percentage of subjects displaying their purchased option.	63
Figure 38. Clarity and understandability of the output by treatment	65

D6.3: Report with Findings of Experiments and Policy implications

List of Tables

Table 1. Cyber insurance prices	12
Table 2. Breakdown of participants by country	14
Table 3. Distribution of the participants by gender, age and country.	14
Table 4. Distribution of the participants by level of education.	14
Table 5. Duration of the experimental sessions by country	15
Table 6. Protection purchases by socio-demographic profile.	16
Table 7. Protection purchases by cyber-risk attitude.	17
Table 8. Protection purchases by factor.	19
Table 9. Estimation of the model of protection purchases.	20
Table 10. Cyberinsurance purchases by socio-demographic profile.	21
Table 11. Cyberinsurance purchases by cyber-risk attitude.	23
Table 12. Cyberinsurance purchases by factor.	24
Table 13. Estimation of the model of basic insurance purchases.	25
Table 14. Estimation of the model of premium insurance purchases.	26
Table 15. Risk level by socio-demographic profile.	27
Table 16. Risk level by cyber-risk attitude.	29
Table 17. Risk level by factor.	31
Table 18. Cybersecurity strategies.	32
Table 19. Cybersecurity strategies by protection measure.	32
Table 20. Cyberinsurance purchases by protection purchases and factor.	33
Table 21. Risk level by protection and insurance strategies.	34
Table 22. Protection strategy by period.	36
Table 23. Transition between protection strategies.	36
Table 24. Transition between protection strategies by experience of cyberattack.	37
Table 25. Cyberinsurance strategies by period.	39
Table 26. Transition between cyberinsurance strategies.	39
Table 27. Transition between cyberinsurance strategies by experience of cyberattack.	40
Table 28. Breakdown of participants by country.	48
Table 29. Breakdown of participants by country.	49
Table 30. Experience of the participants (at last one year).	49
Table 31. Level of education of the participants.	50
Table 32. Protection strategy by treatment.	51
Table 33. Protection strategy by field of expertise.	52
Table 34. Protection strategy by buying expertise.	53
Table 35. Cyberinsurance strategy by treatment.	54
Table 36. Cyberinsurance strategy by field of expertise.	55
Table 37. Cyberinsurance measures purchases by buying expertise.	56
Table 38. Cybersecurity strategies.	57
Table 39. Cybersecurity strategies by treatment.	58

D6.3: Report with Findings of Experiments and Policy implications

Table 40. Differences in the purchases of the recommended option	59
Table 41. Number of options displayed by treatment.....	61
Table 42. Option displayed by treatment.	62
Table 43. Percentage of subjects displaying their purchased option.	63
Table 44. Reasons to purchase the selected cybersecurity strategy.	64
Table 45. Percentage of purchases of the first option in the ranking by treatment.....	64
Table 46. Reasons not to purchase the first option in the ranking by treatment.	65
Table 47. How confident are you in the option you have chosen? (scale 1 to 100)	66
Table 48. How much do you trust that the toolbox will suggest the best option for you? ..	66
Table 49. Intention to use the CYBECO toolbox.....	66

D6.3: Report with Findings of Experiments and Policy implications

1 Introduction

This document corresponds to Deliverable 6.3 and presents the results and implications of the two online economic experiments designed and implemented within the scope of the CYBECO project. This report completes the contents of Deliverable 6.1 (Economic experiments concept note) and Deliverable 6.2 (experimental software). Deliverable 6.1 presents the motivation, the research questions to be answered, the theoretical foundations and a draft proposal of the design (experimental tasks, behavioural measures and experimental treatments) of both experiments. Deliverable 6.2 presents the final version of the experimental design and a fully functional version of the experimental software. Finally, Deliverable 6.3 presents the details of the implementation of both experiments, the results obtained and their implications for the validation and potential improvement of CYBECO model and toolbox.

The document is structured as follows. Section 2 presents the results of Experiment 1, focused in the CYBECO model and providing behavioural insights on how subjects make the decision of which cybersecurity strategy implement. The experiment covers the purchase decision of the different components of this strategy (protection measures, cyberinsurance products and actual online behavior), as well as the process of updating of beliefs under different experimental conditions. Section 3 analyses the results of the second experiment, focused in the use of the CYBECO toolbox. Specifically, this section analyses the implications of the five alternative designs of the interactive output page of the CYBECO toolbox and how these designs affects cyberinsurance decision-making. Finally, section 4 discusses briefly the results of both experiments and their policy implication for the other work packages of CYBECO. The report includes an annex with the screenshots and questionnaires applied in the final version of the experiments, as results of the changes introduced as consequence of the pilot phase of the experimental software presented in Deliverable 6.2.

2 Experiment 1: Behavioural insights of CYBECO model.

2.1 Rationale of experiment 1

As described in the concept note (Deliverable 6.1), Experiment 1 aims to test the CYBECO model from a behavioural-experimental viewpoint. Specifically, Experiment 1 will analyse the ‘human actual behaviour’ when purchasing cyber protection and insurance. The information of this experiment will be applied to identify effective behavioural levers in the design and communication of these types of products.

The rationale of this experiment is as follows. Participants were invited to make decisions related to the purchase of cyber insurance and protection products in an online controlled economic experiment. In a role of IT heads in a SME, participants were offered the chance to buy a protection measure (to reduce the probability of suffering the attack) and/or a cyberinsurance product, that will pay back in case of cyberattack. After voluntary purchasing of these cybersecurity products (protection measures and cyberinsurance policies), participants were required to perform a simple task consisting of an online registration for an event of cybersecurity. To register the comparison website, they were required to create a password, to provide some personal information (compulsory and non-compulsory fields) and to log out after completing the registration. Before accessing the registration website, participants were informed that they may suffer a cyberattack, depending on how safely they behave when browsing.

The experiment contained two independent phases, each of them presenting the opportunity to buy cyberinsurance and protection measures and to register online. At the end of each phase, participants were informed if they have actually received the random cyberattack, and informed of their payoff for the phase, which depends on all their decisions during the experiment and the fact of suffering or not the cyberattack.

Experiment 1 was run with a total sample of 4.800 subjects from four different countries (Germany, Poland, Spain and UK). The profile of the participants were common users of internet that have purchased online products or services during the last year.

D6.3: Report with Findings of Experiments and Policy implications

2.2 Methodology of experiment 1

This section presents the main methodological features of Experiment 1, specifically it experimental conditions and behavioural measures, as well as a brief report of the implementation of the experimental sessions.

2.2.1 Experimental Conditions

Experiment 1 implements a full-factorial design with the following three factors and 2 x 2 x 3 levels, respectively:

- Context of the cyberattack (C)
 - C1: The attack is random (there is a virus in the Internet that may affect randomly to any user). Subject is informed of the average probability of suffering an attack as the percentage of similar users that have suffered the random virus attack in the last week. *“You are aware that there is a computer virus going around the Internet, that may affect your company. We can estimate the probability of this threat by measuring the percentage of similar attacks in the last week.”*



The initial probability that CYBECORP is randomly affected by the virus is 40%

Figure 1. C1: The attack is random

- C2: The attack is intentional (in an adversarial analysis framework, the attack is intentionally launch by a cyber-criminal). Subject is informed of the average likelihood of suffering an attack as the percentage of similar users that have suffered the intentional attack in the last week. *“You are aware that a cybercriminal might deliberately target your company. We can estimate the probability of this threat by measuring the percentage of similar attacks in the last week.”*

D6.3: Report with Findings of Experiments and Policy implications



The initial probability that CYBECORP is attacked intentionally by the cybercriminal is 40%

Figure 2. C2: The attack is intentional

- Relation of the protection measure and the price of the cyber insurance product (P):
 - P1: The price of the insurance does not depend on the protection level
 - P2: The price of the insurance does depend on the protection level
- Features of the cyber insurance product (I) :
 - I1: Medium price
 - I2: Asymmetric price
 - I3: High price

Notice that the cost of the insurances depends on two factors: the relation of the ASMs and the price of the cyber insurance product (P) and the features of the cyber insurance product (I). If c_{11}^i is the price of an insurance given by its expected value (i. e. the product of the initial probability of a cyberattack and the coverage of the cyber-insurance), the different insurance prices are represented in Table 1.

	P1 - Price does not depend on the purchase of the antivirus	P2 - Price does depend on the purchase of the ASMs (prices if the ASMs is purchased, if not they are the same as in P1)
I1 - Medium price	c_{11}^i	$c_{12}^i = (1 - 0.5)c_{11}^i$
I2 - Asymmetric price	c_1^1 $c_{21}^i = (1 + 0.2)c_1^1$	$c_{12}^1 = (1 - 0.5)c_{11}^1$ $c_{22}^2 = (1 - 0.7)c_{11}^2$
I3 - High price	$c_{31}^i = (1 + 0.2)c_1^i$	$c_{32}^i = (1 - 0.3)c_{11}^i$

Table 1. Cyber insurance prices

D6.3: Report with Findings of Experiments and Policy implications

2.2.2 Behavioural measures

Experiment 1 considers three behavioural measures to be analysed in terms of the different experimental conditions:

- Protection strategy.** This measure is a dichotomic variable that can take the values Basic Security Measures (BSMs) or Advance Security Measures (ASMs) according to the protection level purchased by the subjects during the experiment.
- Insurance strategy.** This measure is an ordinal variable that can take three values, according to the cyberinsurance product purchased by the subject: No insurance (none), basic insurance and premium insurance.
- Risk level of online behaviour.** Risk level of online behaviour¹ is a continuous variable between 0 and 1. The measure is equal to 0 if the online behaviour is completely safe and increases with the risk assumed by the subjects during online navigation. This measure is obtained as a combination of the proxy variables (1) security level of the password, (2) provision or not of non-compulsory private information, (3) consultation of the terms and (4) conditions and log out.

2.2.3 Experiment implementation

The fieldwork of the experiment started on 5th June 2018 in the four countries (Germany, Poland, Spain and UK). Invitations to participate to the experiment were sent constantly to the online panel during the duration of the experiment in order to reach the required quota by country and by gender and age. Once a quota was reached, the system stopped sending invitations to those profiles, and the speeders (i. e., respondents completing the experiment in less than one third of the median time allocated by participants in each country) were

¹ The risk level is computed from the following binary variables, which are equal to 1 if they verify the following statements or 0 otherwise:

- Password, x_i^{pass} : Password does not contain capital letters; Password does not contain lowercase letters; Password does not contain numbers; Password does not contain special characters ($[^\wedge \backslash \$ \% \& * () \{ \} \# - ? > < , | = _ + \cdot -]$); Password is short (less than 8 characters); Password includes the username (case-insensitive)
- Registration, x_i^{reg} : The subject has filled the “First name” field; The subject has filled the “Last name” field; The subject has filled the “Occupation” field; The subject has filled the “Phone Number” field; The subject has filled the “Address” field; The subject has filled the “City” field; The subject has filled the “Zip” field
- Privacy policy, x_i^{pp} : The subject has not opened the “Privacy Policy” window
- Log out, x_i^{log} : The subject has not logged out of the website after the registration

The security level, RL , is obtained as a weighted average of the above variables:

$$RL = w_{pass} \sum_{i=1}^6 x_i^{pass} + w_{reg} \sum_{i=1}^7 x_i^{reg} + w_{pp} x^{pp} + w_{log} x^{log}$$

where w represents the weight of each binary variable, given by $w_{pass} = 0.4 \cdot 1/6$, $w_{reg} = 0.3 \cdot 1/7$, $w_{pp} = 0.15$ and $w_{log} = 0.15$.

D6.3: Report with Findings of Experiments and Policy implications

identified in the following 24/48 hours and then removed from the quota. After that, the quota was then re-opened to complete it. On 6th August 2018, the final target was reached, and the experiment stopped. In the table below the speeders by country are presented together with the final number of respondents who successfully implemented the experiment.

	<i>Country</i>				
	Germany	Spain	Poland	UK	<i>Total</i>
<i>Total subjects click the email</i>	4156	2162	4083	2924	13325
<i>Total subjects access the experiment</i>	3944	2118	4025	2700	12787
<i>Total subjects complete the experiment</i>	1248	1226	1255	1258	4987
<i>Total 'speeders'</i>	7	5	10	1	23

Table 2. Breakdown of participants by country

A total of 13,325 participants clicked on the email that gave access to the experiment, but only 12,787 accessed the experiment, Table 2. Out of these, 4,987 completed the experiment. However, 23 of these were classified as 'speeders'. The average dropout, participants who took part but did not complete the experiment, was 62.6%, where the lowest % of dropouts is found in Spain (43.3%) and the highest % is found in Germany (70.0%). The final distribution by sex and age of the respondents is shown in Table 3. The distribution by age and gender reflects Eurostat's data from the 2017 survey on ICT that was used to create the quota. No weights needed to be applied to the quotas.

	<i>Germany</i>		<i>Spain</i>		<i>Poland</i>		<i>UK</i>	
	n	%	n	%	n	%	n	%
Male	617	51.42	600	50.00	552	46.00	595	49.58
Female	583	48.58	600	50.00	648	54.00	605	50.42
16 - 34 years	932	77.67	842	70.17	713	59.42	844	70.33
35 - 74 years	268	22.33	358	29.83	487	40.58	356	29.67
<i>Total</i>	<i>1200</i>	<i>100.00</i>	<i>1200</i>	<i>100.00</i>	<i>1200</i>	<i>100.00</i>	<i>1200</i>	<i>100.00</i>

Table 3. Distribution of the participants by gender, age and country.

Regarding the education of participants, most of them had either finished high school or had a university degree, as shown in Table 4.

Education level	n	%
0-11 years of education	403	8.40
12 years of education	1446	30.13
Some years of university (not completed)	609	12.69
University degree	1355	28.23
Post-graduate degree	987	20.56
<i>Total</i>	<i>4800</i>	<i>100.00</i>

Table 4. Distribution of the participants by level of education.

D6.3: Report with Findings of Experiments and Policy implications

Finally, with respect to the duration of the experiment (Table 5), there were no big differences among the countries: the median duration was a little more than 19 minutes, with respondents from Germany taking a little longer (20 minutes) and respondents from Spain who were faster (18,3 minutes).

	Country				
	Germany	Spain	Poland	UK	Total
Average (sec)	1715.6	1433.3	1664.3	1417.3	1557.0
Average (min)	28.6	23.8	27.8	23,6	26.0
Median (sec)	1200.0	1098.0	1200.0	1146.0	1140.0
Median (min)	20.0	18.3	20.0	19.1	19.0

Table 5. Duration of the experimental sessions by country

2.3 Selection of the cybersecurity strategy: protection, insurance and online behaviour

This section analyses the main determinants of the cybersecurity strategy defined by the user in the first round of the experiment, *before any experience of suffering or not any cyberattack in the experimental session*. Specifically, this section shown the impact of the socio-demographic profile of the subject, her or his general attitude toward cyber-risk and the experimental conditions on the purchasing decision of protection and insurance measure and the security level during online navigation. The analysis covers the analysis of the three individual measures (Protection level, insurance level and secure behaviour level), as well as their interactions.

2.3.1 Protection strategy

This section presents the results for the first behavioural measure: the protection strategy. Subjects are offered to acquire basis security measures (BSMs) which keep the initial probability to suffer the attack in 40% and are free or advance security measure (ASMs) that reduces this probability to 20% but have a cost. Subjects opted in general for a high level of protection in the experiment. Specifically, more than four-fifths of subjects, 83.4%, bought the ASMs.

2.3.1.1 Socio-demographic profile

The protection level is significantly higher for women and increases with age. This behaviour can be consequence of the higher risk-aversion shown in general by women and elder people. Table 6 and Figure 3 show how the sales of ASMs are significantly higher in females ($p\text{-value} = 0.048$) and for elder people ($p\text{-value} = 0.000$). Moreover, we found that the sales of ASMs are 6.25 percentage points lower in participants from Germany in comparison with participants from UK ($p\text{-value} = 0.000$).

D6.3: Report with Findings of Experiments and Policy implications

<i>Socio-demographic profile</i>		<i>Security Measures</i>		<i>p-value (x2 test)</i>
		<i>BSMs (%)</i>	<i>ASMs (%)</i>	
Gender	Male	17.72	82.28	0.048**
	Female	15.60	84.40	
Age	18-35	19.81	80.19	0.000***
	36-50	16.25	83.75	
	50-74	14.30	85.70	
Country	Germany	20.50	79.50	0.000***
	Spain	16.42	83.58	
	Poland	15.42	84.58	
	UK	14.25	85.75	
Studies level	0-11 years of education	17.87	82.13	0.666
	High school diploma	16.87	83.13	
	Some years of university	15.44	84.56	
	University degree	17.34	82.66	
	Post-graduate degree	15.60	84.40	
Employment status	Self-employed	26.11	73.89	0.000***
	Public/Private worker	15.67	84.33	
	Unemployed	18.03	81.97	
	Housewife/Househusband	14.67	85.33	
	Student	15.02	84.98	
	Retired	15.41	84.59	
	Other	13.75	86.25	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 6. Protection purchases by socio-demographic profile.

It is relevant to show that education seem to have no effective impact of the protection level. If we focus on employment situation, the ASMs sales are significantly lower in self-employment and unemployment participants, 73.9% and 81.2% respectively ($p\text{-value} = 0.000$).

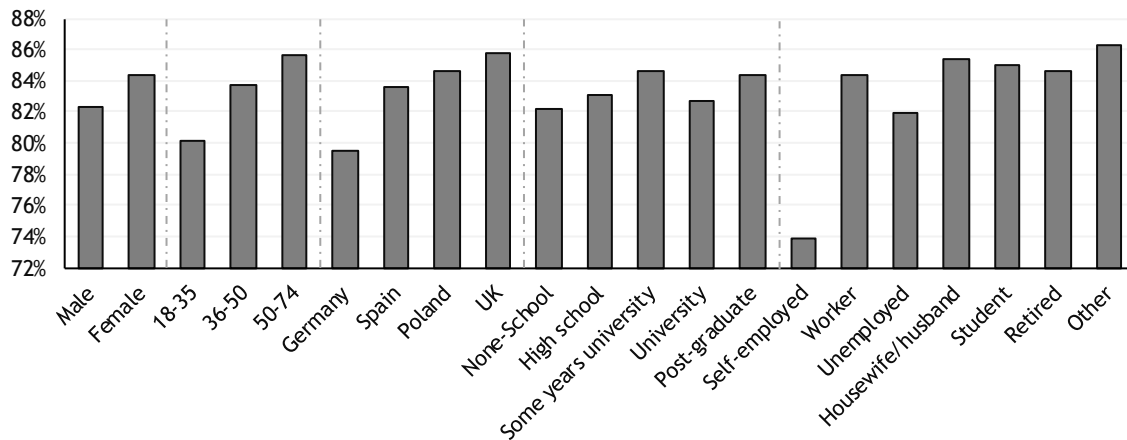


Figure 3. Protection purchases by socio-demographic profile

D6.3: Report with Findings of Experiments and Policy implications

2.3.1.2 Cyber-risk attitude

A set of questionnaires were administered that captured a range of subjective measures aligned to the constructs described in protection motivation theory. These assessed the perceived risk of an attack in terms of severity and vulnerability, the participant's response efficacy, perceived behavioural control and response cost. In addition, a set of questions addressed attitudes to cyberinsurance and also risk propensity (using the DOSPERT scale). In Table 7 and Figure 4, we observe that each of these with the exception of perceived vulnerability is predictive of security behaviour. Perceived vulnerability refers to the extent to which an individual feels that it is likely that they will be made a target of an attack. It is possible that we are not seeing an effect on this variable because participants are 'unrealistically optimistic' about the extent to which they will be targeted in an attack (see Campbell et al., 2007)². Note that those who feel that the 'response cost' of secure behaviour is high are less likely to purchase ASMs, as expected, and that those people who are risk averse are more likely to purchase ASMs, again, as predicted.

<i>Risk profile</i>		<i>Security Measures</i>		<i>p-value (x2 test)</i>
		<i>BSMs (%)</i>	<i>ASMs (%)</i>	
Perceived severity	Low	24.02	75.98	0.000***
	High	15.02	84.98	
Perceived vulnerability	Low	16.33	83.67	0.636
	High	16.85	83.15	
Response Efficacy	Low	18.73	81.27	0.002**
	High	15.34	84.66	
Perceived Behavioural Control	Low	20.43	79.57	0.000***
	High	15.51	84.49	
Response Cost	Low	13.32	86.68	0.000***
	High	20.32	79.68	
Attitudes	Low	24.93	75.07	0.000***
	High	14.44	85.56	
DOSPERT	Averse	15.11	84.89	0.000***
	Seeker	24.31	75.69	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 7. Protection purchases by cyber-risk attitude.

² Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in human behavior*, 23(3), 1273-1284.

D6.3: Report with Findings of Experiments and Policy implications

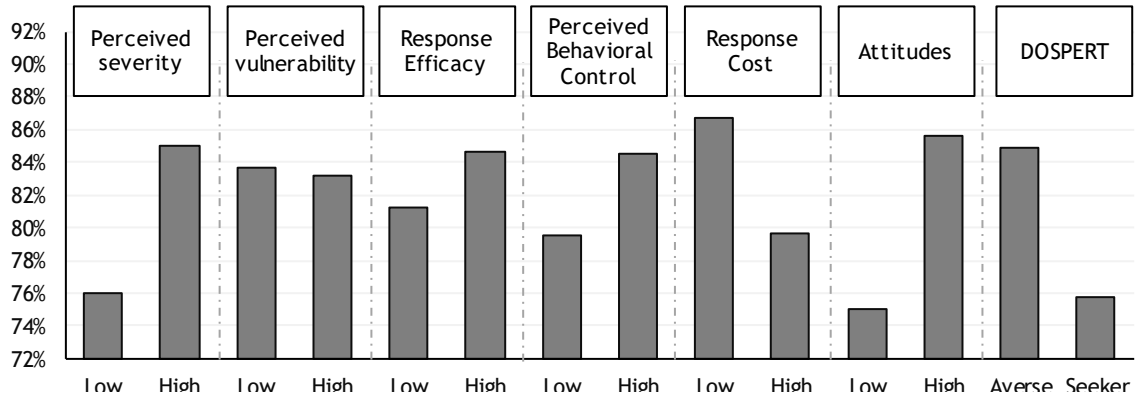


Figure 4. Protection purchases by cyber-risk attitude.

2.3.1.3 Experimental factors

The context of the attack and the price architecture of the cybersecurity products have a significant impact in the protection level selected by the subjects. Although the probability of the attack is the same in both contexts and there are no rational reasons to behave differently in each of them, subjects protect themselves more in the context of an intentional attack than in that of a random attack. The information that agents are intentionally addressing attacks to profiles similar to the subject makes, increases her or his believes on the likelihood of suffering the attack. This feature of subjects' believe formation process supports the need of considering the adversarial approach of CYBECO model, even when modelling the behaviour of the defender, who would not react in the same way than under the random approach, generally consider in risk and cyber-risk models. On the other hand, the dependence of the price of cyber-insurance products on the protection level of the subjects arises as a significant lever to promote the purchase not only of cyberinsurance but also of advance protection measures.

Specifically, Table 8 shows the percentage of purchases of the security measures and the result of testing the hypothesis by factor. As can be seen in Figure 5, the purchases of ASMs are significantly higher, when the price of the cyberinsurance products depend on the SMS purchase (p -value = 0.000).

D6.3: Report with Findings of Experiments and Policy implications

Factor		Security Measures		p-value (χ^2 test)
		BSMs (%)	ASMs (%)	
Context of the cyberattack (C)	C1: Random	17.54	82.46	0.096*
	C2: Intentional	15.75	84.25	
Price dependency (P)	P1: Independent	19.38	80.62	0.000***
	P2: Dependent	13.92	86.08	
Features of the cyberinsurance (I)	I1: Medium	16.50	83.50	0.972
	I2: Asymmetric	16.62	83.38	
	I3: High	16.81	83.19	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 8. Protection purchases by factor.

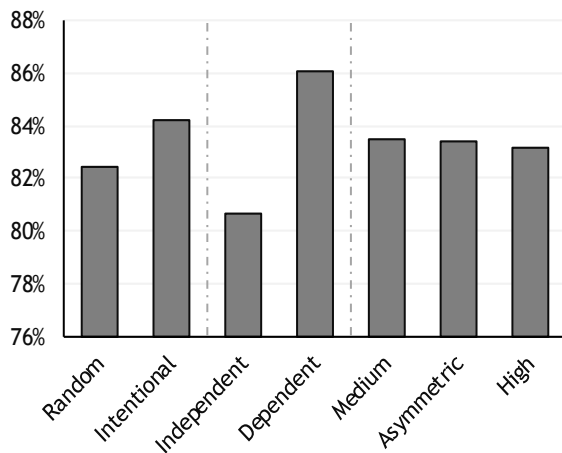


Figure 5. Protection purchases by factor.

If we compare the ASMs purchases when the context of cyberattack is random or intentional, Factor C, we notice that the purchases of ASMs are a 1.8 percentage points higher in intentional context than in the random one – although this difference is not significant (p -value = 0.096).

Finally, we can observe that the price of the cyberinsurance, Factor I, has no effect on the purchases of SMs, (p -value = 0.972).

2.3.1.4 A model for protection strategy

The election of the protection strategy depends not only of the experimental conditions, but also on the socio-demographic profile and cyber-risk attitudes of the subject. We propose a logistic model through to predict whether an individual is more likely to purchase the advanced security measures or not. In such model, we have taken into account simultaneously all the variables with a significant impact on the protection strategy: individual's age, price dependence experimental condition, country, DOSPERT, perceived severity, response efficacy, response cost and the attitudes scores of individuals. We assume that each individual has a probability of buying the advanced security measures, which depends on the last characteristics described.

D6.3: Report with Findings of Experiments and Policy implications

Mathematically, let the function f be

$$\begin{aligned} f(\text{Age, FPIndependent, Spain, Poland, UK, Dospert, Severity, Efficacy, Cost, Attitudes}) \\ = \beta_0 + \beta_1 \text{Age} + \beta_2 \text{FPIndependent} + \beta_3 \text{Spain} + \beta_4 \text{Poland} + \beta_5 \text{UK} \\ + \beta_6 \text{Dospert} + \beta_7 \text{Severity} + \beta_8 \text{Efficacy} + \beta_9 \text{Cost} + \beta_{10} \text{Attitudes} \end{aligned}$$

where each β_i coefficient has to be estimated. Then we estimate the probability of buying the advanced security measures for a certain individual as

$$p = \frac{e^{f(\text{Age, FPIndependent, Spain, Poland, UK, Dospert, Severity, Efficacy, Cost, Attitudes})}}{1 + e^{f(\text{Age, FPIndependent, Spain, Poland, UK, Dospert, Severity, Efficacy, Cost, Attitudes})}}$$

Notice that FPIndependent, Spain, Poland and UK are factors describing the characteristics of a certain individual, taking a value of 1 if they satisfy the characteristic and 0 otherwise. Table 9 shows the estimations of the coefficient of the model, as well as their standard error estimation, z-values and p-values.

	Estimate	Std. Error	z-value	p-value
Intercept	0.887	0.366	2.424	0.015**
Age	0.007	0.003	2.276	0.022**
FPIndependent	-0.386	0.080	-4.821	0.000***
Spain	0.419	0.113	3.713	0.000***
Poland	0.4557	0.114	3.993	0.000***
UK	0.6155	0.118	5.213	0.000***
Dospert	-0.184	0.037	-5.034	0.000***
Severity	0.204	0.044	4.658	0.000***
Efficacy	-0.1179	0.050	-2.346	0.019**
Cost	-0.2249	0.052	-4.316	0.000***
Attitudes	0.3271	0.058	5.647	0.000***

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 9. Estimation of the model of protection purchases.

Summarizing, the age coefficient is telling us that the older the individual, the more likely is that it purchase the advanced security measures (as it is positive). The independent factor nudges people to stop purchasing the advanced security measures. Spain, Poland and UK subjects buy more advanced measures than Germany individuals, being UK the country with more probability of buying advanced measures. The DOSPERT score tells us that the riskier an individual is, the less it is to buy the advanced measures. The perceived severity of individuals and their attitudes score tell us that the greater the score is, the more probability there is that someone purchase the advanced measure.

D6.3: Report with Findings of Experiments and Policy implications

2.3.2 Cyberinsurance strategy

This section presents the results for the second individual behavioural measure: the insurance strategy. Subjects are offered to acquire or not two different insurance products, basic and premium insurance, the second one offering a higher coverage at a higher price. It must be highlighted that almost all subjects (93.0%) decided to purchase some type of cyberinsurance. Moreover, around half of the subjects, 50.2% bought the Premium Insurance and 42.8% the Basic Insurance. Alternatively, only 7% of the subjects did not contract any cyberinsurance product. In fact, during all the analysis, we can observe the existence of a small group of subjects that are not interested in this type of products, no matter the experimental condition. As we will discuss in section 2.4, this segment does not change their behaviour no matter if they suffer an attack or not.

2.3.2.1 Socio-demographic characteristics

As for protection strategy, sex and age are correlated to the selected insurance strategy. Women and subjects over 35 years tend to purchase cybersinsurance in general, and in particular the premium insurance product, in a significantly higher proportion than men and younger subjects. Table 10 and Figure 6, we observe that the sales of ASMs are significantly higher in females ($p\text{-value} = 0.001$) and in 36-50 years old people ($p\text{-value} = 0.009$). Moreover, we found that the sales of Premium insurance are lower in Spain ($p\text{-value} = 0.000$).

Demographic characteristics		Cyberinsurance products			p-value (χ^2 test)
		None (%)	Basic (%)	Premium (%)	
Gender	Male	8.29	43.15	48.56	0.001**
	Female	5.75	42.45	51.81	
Age	18-35	11.00	44.58	44.42	0.009**
	36-50	5.33	41.42	53.25	
	50-74	5.83	43.50	50.67	
Country	Germany	5.83	41.67	52.50	0.000***
	Spain	7.69	45.61	46.70	
	Poland	6.30	43.02	50.68	
	UK	7.06	40.16	52.77	
Studies level	0-11 years of education	9.68	38.46	51.86	0.097*
	High school diploma	7.12	40.87	52.01	
	Some years of university	7.06	43.19	49.75	
	University degree	5.90	44.94	49.15	
	Post-graduate degree	7.19	44.17	48.63	
Employment situation	Self-employed	11.50	43.36	45.13	0.000***
	Public/Private worker	6.20	43.77	50.04	
	Unemployed	7.21	38.69	54.10	
	Housewife/Househusband	6.95	33.59	59.46	
	Student	9.16	49.82	41.03	
	Retired	6.26	41.09	52.65	
	Other	7.50	40.00	52.50	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 10. Cyberinsurance purchases by socio-demographic profile.

D6.3: Report with Findings of Experiments and Policy implications

If we focus on employment situation, the Premium insurance sales are significantly higher in housewives/househusbands, 59.5%, and lower in students, 41.0% ($p\text{-value} = 0.000$). This fact can be consequence of the higher presence of women among housewives/househusbands and of younger subjects among students. Finally, we found that there is no significant difference on SMs purchases between participant with different level of education ($p\text{-value} = 0.097$).

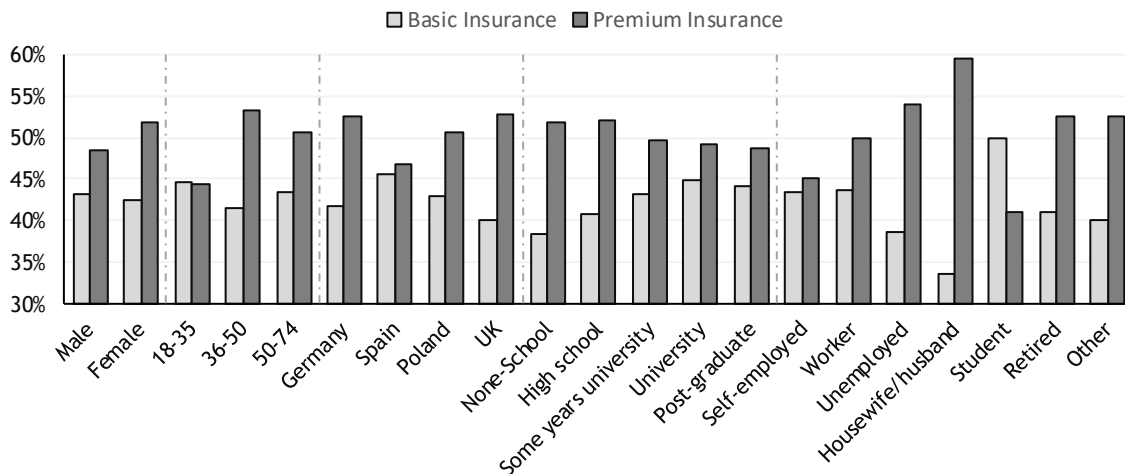


Figure 6. Cyberinsurance purchases by socio-demographic profile.

2.3.2.2 Cyber-risk attitude

Again, we were able to look at the role of threat and coping factors embedded in protection motivation theory, together with attitudes to insurance and also risk (DOSPERT Scale). These are shown in Table 12 and Figure 7. Here, we observe that all measures are predictive of behaviour (in this case the decision to purchase cyberinsurance) and that most lie in the predicted direction - i.e. that high threat or high coping ratings tend to drive the purchase of premium insurance. It is worth noting that high 'response cost' is associated with lower purchase of premium insurance - but this also makes sense. Those people who feel that taking out insurance would be burdensome are less likely to opt for premium products. In regard to the Dospert finding, this also lies in the predicted direction - those who are risk averse are more likely to take out premium insurance.

D6.3: Report with Findings of Experiments and Policy implications

Risk profile		Cyberinsurance products			p-value (χ^2 test)
		None (%)	Basic (%)	Premium (%)	
Perceived severity	Low	10.28	45.15	44.57	0.000***
	High	6.28	42.27	51.45	
Perceived vulnerability	Low	8.24	42.61	49.14	0.024**
	High	6.21	42.91	50.89	
Response Efficacy	Low	12.18	45.10	42.72	0.000**
	High	3.76	41.35	54.89	
Perceived Behavioural Control	Low	10.08	43.74	46.17	0.000***
	High	6.07	42.50	51.42	
Response Cost	Low	6.12	40.99	52.89	0.000***
	High	8.10	45.04	46.86	
Attitudes	Low	16.82	45.00	38.18	0.000***
	High	4.38	42.20	53.42	
DOSPRT	Averse	6.45	42.05	51.50	0.000***
	Seeker	9.73	46.51	43.77	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 11. Cyberinsurance purchases by cyber-risk attitude.

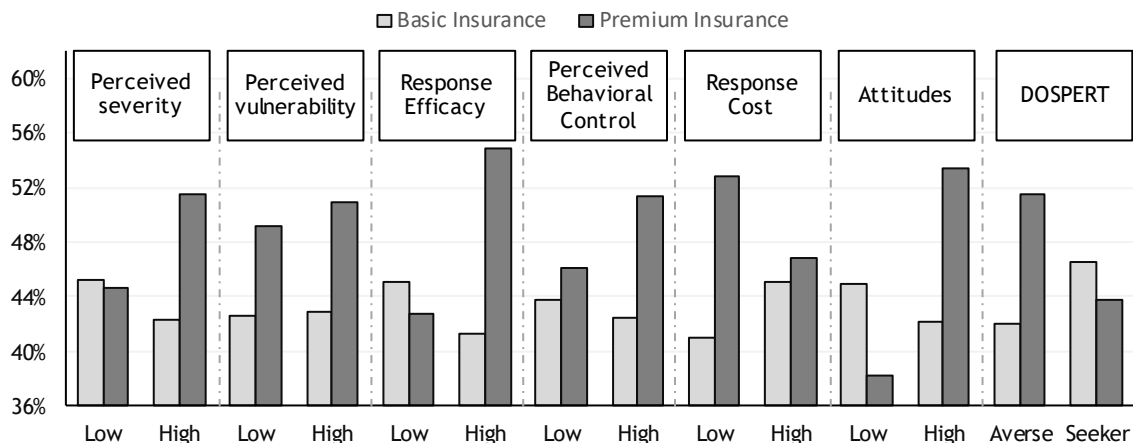


Figure 7. Cyberinsurance purchases by cyber-risk attitude.

2.3.2.3 Experimental factors

The price structure of the portfolio of protection-insurance factor is the only experimental condition with a significant impact on the insurance strategy. When the price of the insurance depends on the protection level, the purchase of the Premium insurance is significantly higher. Although no significant, and in line with the result observed for the protection strategy, the purchases of the premium insurance is slightly higher for the context of intentional attacks. Table 12 shows the percentage of purchases of the cyberinsurance and the result of testing the hypothesis by factor. As can be seen in Figure 8, the purchases

D6.3: Report with Findings of Experiments and Policy implications

of Premium Insurance are significantly higher when the price of the cyberinsurance depend on the SMs purchase, Factor P ($p\text{-value} = 0.000$).

Factor		Cyberinsurance products			$p\text{-value}$ (χ^2 test)
		None (%)	Basic (%)	Premium (%)	
Context of the cyberattack (C)	C1: Random	7.12	43.50	49.38	0.513
	C2: Intentional	6.88	42.08	51.04	
Price dependency (P)	P1: Independent	7.29	45.96	46.75	0.000***
	P2: Dependent	6.71	39.62	53.67	
Features of the cyberinsurance (I)	I1: Medium	7.25	40.81	51.94	0.337
	I2: Asymmetric	6.50	44.06	49.44	
	I3: High	7.25	43.50	49.25	

* $p\text{-value} < 0.1$; ** $p\text{-value} < 0.05$; *** $p\text{-value} < 0.001$

Table 12. Cyberinsurance purchases by factor.

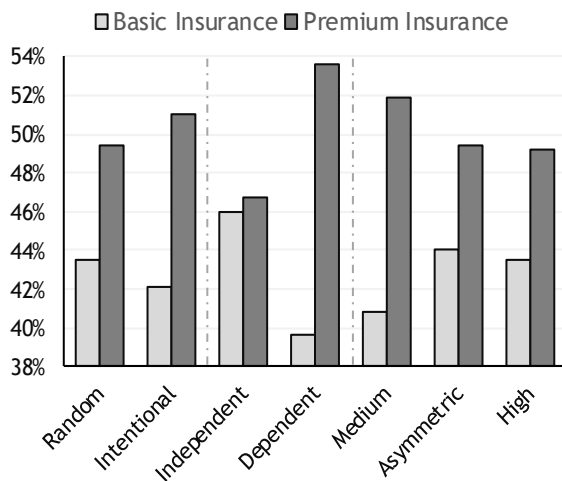


Figure 8: Cyberinsurance purchases by factor

The context of cyberattack, Factor C, have no significant effect on the cyberinsurance purchase ($p\text{-value} = 0.513$).

Finally, we can observe that the purchases of Premium insurances are a 2.7 percentage points higher when the price of both cyberinsurances, Factor I, are the medium ones (i.e. the price was calculated by the expected value) than when price of both cyberinsurance products are a 20% more expensive, although this difference is not significative, ($p\text{-value} = 0.337$).

2.3.2.4 A model for insurance strategy

As for the protection strategy, we develop a model to estimate the impact of the key socio-demographic, cyber-risk attitude variables and experimental factors on the probability to choose each type of insurance. Since the number of potential outputs is now three (none / basic / premium), we propose a multinomial logistic model. Then we estimate the probability of each individual to purchase each type of insurance protection. More specifically, we estimate the probability p_B of buying the basic protection, and the probability p_P of buying the premium protection, through which we will be capable to estimate the probability of not purchasing any kind of protection $p_N = 1 - p_B - p_P$, as there are no more choices.

D6.3: Report with Findings of Experiments and Policy implications

In this model, the gender of the individual, their country, response efficacy, attitudes and DOSPRT scores were meaningful in order to estimate these probabilities. Mathematically, the functions f_B and f_P be

$$\begin{aligned} f_B(\text{Gender, Spain, Poland, UK, Dospert, Efficacy, Attitudes}) \\ = \beta_0^B + \beta_1^B \text{Age} + \beta_2^B \text{Spain} + \beta_3^B \text{Poland} + \beta_4^B \text{UK} + \beta_5^B \text{Dospert} + \beta_6^B \text{Efficacy} \\ + \beta_7^B \text{Attitudes} \end{aligned}$$

$$\begin{aligned} f_P(\text{Gender, Spain, Poland, UK, Dospert, Efficacy, Attitudes}) \\ = \beta_0^P + \beta_1^P \text{Age} + \beta_2^P \text{Spain} + \beta_3^P \text{Poland} + \beta_4^P \text{UK} + \beta_5^P \text{Dospert} + \beta_6^P \text{Efficacy} \\ + \beta_7^P \text{Attitudes} \end{aligned}$$

Then,

$$p_B = \frac{e^{f_B(\text{Gender, Spain, Poland, UK, Dospert, Efficacy, Attitudes})}}{1 + e^{f_B(\text{Gender, Spain, Poland, UK, Dospert, Efficacy, Attitudes})}}$$

$$p_P = \frac{e^{f_P(\text{Gender, Spain, Poland, UK, Dospert, Efficacy, Attitudes})}}{1 + e^{f_P(\text{Gender, Spain, Poland, UK, Dospert, Efficacy, Attitudes})}}$$

Notice that FPIIndependent, Spain, Poland and UK are factors describing the characteristics of a certain individual, taking a value of 1 if they satisfy the characteristic and 0 otherwise. Notice that the variables 'Female' and the countries can just take the values 0 and 1, indicating if the individual we are analyzing satisfies it. Table 13 and Table 14 show the estimation of the coefficients for each equation.

	Estimate	Std. Error	z-value	p-value
Intercept	-0.844	0.342	-2.471	0.013**
Female	0.298	0.124	2.409	0.016**
Spain	0.427	0.17	2.51	0.012**
Poland	0.485	0.166	2.927	0.003**
UK	0.439	0.166	2.648	0.008**
Dospert	-0.139	0.054	-2.566	0.010**
Efficacy	0.371	0.072	5.165	0.000***
Attitudes	0.463	0.078	5.911	0.000***

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 13. Estimation of the model of basic insurance purchases.

D6.3: Report with Findings of Experiments and Policy implications

	Estimate	Std. Error	z-value	p-value
Intercept	-1.637	0.35	-4.676	0.000***
Female	0.338	0.124	2.708	0.006**
Spain	0.634	0.171	3.698	0.000***
Poland	0.613	0.168	3.649	0.000***
UK	0.662	0.167	3.96	0.000***
Dospert	-0.27	0.055	-4.92	0.000***
Efficacy	0.511	0.072	7.03	0.000***
Attitudes	0.668	0.08	8.336	0.009**

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 14. Estimation of the model of premium insurance purchases.

In this case, we see that female users are more likely to purchase both basic and premium insurance than males, being more probable that females purchase a premium insurance (as the estimate in the premium purchase is greater than the coefficient estimated in the basic insurance purchase). Again, Germany is the country with less insurance purchases as all the other country coefficients are significantly positive. Also, the DOSPERT score is significantly significant, showing a decrease on insurance purchase among the riskier subjects.

2.3.3 Risk level of online behaviour

This section presents the analysis of the risk taken by the subjects during online navigation in the first round of the experiment. Since the risk level is a continuous variable, the existence of significant differences of the risk level assumed by different groups of subjects has been done applying analysis of variance (ANOVA). As for the two previous behavioural measures, the section presents the results of the analysis by socio-demographic profile, cyber-risk attitude and factors, and concludes with a model integrating all these types of variables. As a general result, the risk level is quite constant among the different groups of subjects.

2.3.3.1 Socio-demographic characteristics

The risk level of online behaviour does not depend on the sex of the subject but is influenced by the age. A result that may be considered as surprising in a first sight is the fact that the risk taken by subjects increases with the age, in contrast to the general common finding in the literature of elders being more risk averse (Table 15). The explanation for that is that subjects do not select explicitly their level of risk they want to assume but this measure is a consequence of how safe its actual online behaviour is depending of the decisions they make in the process (for instance, how strong their password is or if the log out the website before leaving it). A possible interpretation is that elder people have more problems in understanding the security implications of their decisions and taking a risk level that they are not willing to get. This finding suggests the need to work with elder persons to help them to understand the security implication of critical online actions.

D6.3: Report with Findings of Experiments and Policy implications

The interpretation that higher risk levels could be a consequence of the lack of knowledge on security implications is supported by the fact that the risk level decreases with the education level, from the 0.57 of the participants with less than 11 years of formal education to the 0.53 of the participants with post-graduate degree, as shown in Table 15 and Figure 9. Risk level by socio-demographic profile. Figure 9.

<i>Socio-Demographic profile</i>		<i>Risk level</i>				<i>p-value (ANOVA)</i>
		<i>n</i>	<i>Mean</i>	<i>SD</i>	<i>Max-Min</i>	
Gender	Male	2364	0.555	0.151	0-0.833	0.336
	Female	2436	0.559	0.148	0-0.864	
Age	18-35	1536	0.531	0.158	0-0.864	0.000***
	36-50	1551	0.563	0.150	0-0.833	
	50-74	1713	0.574	0.138	0.036-0.833	
Country	Germany	1200	0.547	0.152	0-0.833	0.000***
	Spain	1200	0.592	0.141	0-0.833	
	Poland	1200	0.529	0.156	0-0.864	
	UK	1200	0.558	0.141	0-0.833	
Studies level	0-11 years of education	403	0.573	0.138	0.125-0.833	0.000***
	High school diploma	1446	0.576	0.140	0-0.833	
	Some years of university	609	0.558	0.153	0-0.833	
	University degree	1355	0.551	0.150	0-0.864	
	Post-graduate degree	987	0.530	0.160	0.036-0.833	
Employment situation	Self-employed	452	0.554	0.151	0.067-0.833	0.000***
	Public/Private worker	2808	0.556	0.149	0-0.864	
	Unemployed	305	0.573	0.143	0.036-0.833	
	Housewife/Househusband	259	0.581	0.133	0.125-0.833	
	Student	273	0.498	0.176	0-0.833	
	Retired	623	0.569	0.140	0.067-0.833	
	Other	80	0.572	0.141	0.067-0.767	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 15. Risk level by socio-demographic profile.

D6.3: Report with Findings of Experiments and Policy implications

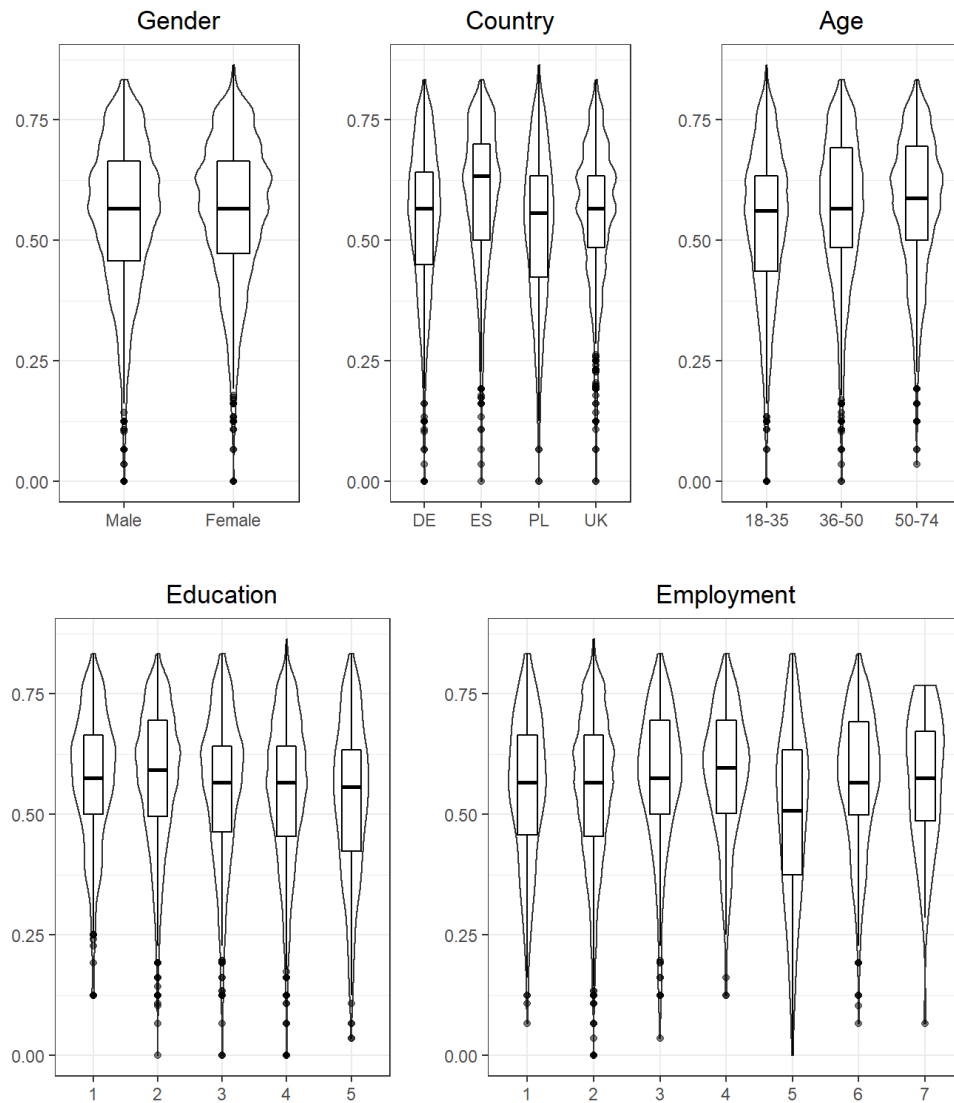


Figure 9. Risk level by socio-demographic profile.

D6.3: Report with Findings of Experiments and Policy implications

2.3.3.2 Cyber-risk attitude

Again, we were able to look at the role of threat and coping factors embedded in protection motivation theory, together with attitudes to insurance and also risk (DOSPERT Scale). These are shown in and Figure 10. Here, we see a rather different pattern emerge, where relatively few factors (response efficacy, response cost and risk aversion (DOSPERT)) are predictive of behaviour (in this case the level of risk shown in online behaviour). It seems as though the threat measures from protection motivation theory are not driving 'safe' online behaviours, but some of the coping measures are influential. Specifically those that believe that cyberinsurance and advanced security measures offer effective protection are more likely to engage in risky online behaviour. Those that believe that the cost of protection is too high are also more likely to engage in risky behaviour and those who are risk averse are more likely to navigate safely.

Risk profile		n	Security behaviour			p-value (ANOVA)
			Mean	SD	Max-Min	
Perceived severity	Low	866	0.559	0.147	0-0.833	0.575
	High	3934	0.556	0.150	0-0.864	
Perceived vulnerability	Low	1868	0.556	0.149	0-0.833	0.8
	High	2932	0.557	0.150	0-0.864	
Response Efficacy	Low	1847	0.539	0.163	0-0.833	0.000***
	High	2953	0.568	0.139	0-0.864	
Perceived Behavioral Control	Low	1111	0.560	0.153	0-0.833	0.466
	High	3689	0.556	0.148	0-0.864	
Response Cost	Low	2664	0.551	0.150	0-0.864	0.002**
	High	2136	0.564	0.148	0-0.833	
Attitudes	Low	1011	0.560	0.155	0.067-0.833	0.448
	High	3789	0.556	0.148	0-0.864	
DOSPERT	Averse	3998	0.554	0.153	0-0.864	0.003**
	Seeker	802	0.570	0.133	0.067-0.833	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 16. Risk level by cyber-risk attitude.

D6.3: Report with Findings of Experiments and Policy implications

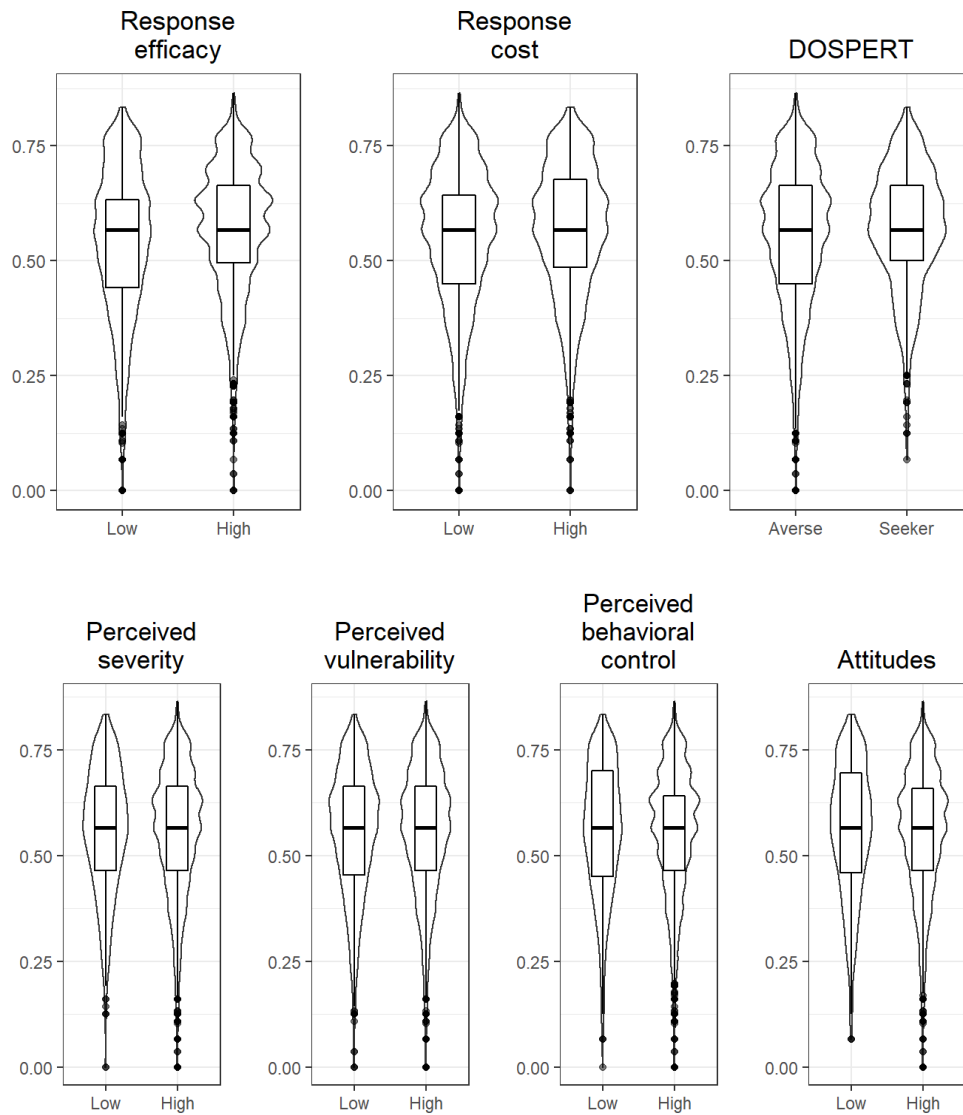


Figure 10. Security behaviour by risk profile.

D6.3: Report with Findings of Experiments and Policy implications

2.3.3.3 Experimental factors

The experimental conditions have no significant impact on the risk level of the online behaviour, the only exception being the context of the attack. As can be seen in Table 17, the risk is significantly higher, when the context is random, Factor C (*p-value* = 0.028).

Factor		n	Risk level			p-value (ANOVA)
			Mean	SD	Max-Min	
Context of the cyberattack (C)	C1: Random	2400	0.552	0.151	Table 17	0.028**
	C2: Intentional	2400	0.561	0.148	0-0.864	
Price dependency (P)	P1: Independent	2400	0.555	0.151	0-0.864	0.540
	P2: Dependent	2400	0.558	0.148	0-0.833	
Features of the cyberinsurance (I)	I1: Medium	1600	0.558	0.153	0-0.833	0.578
	I2: Asymmetric	1600	0.559	0.146	0-0.833	
	I3: High	1600	0.554	0.149	0-0.864	

* *p-value* < 0.1; ** *p-value* < 0.05; *** *p-value* < 0.001

Table 17. Risk level by factor.

Finally, we can observe that both the price dependency, Factor P and the price of the cyberinsurance, Factor I, has no effect on the security behaviour index (*p-value* = 0.972).

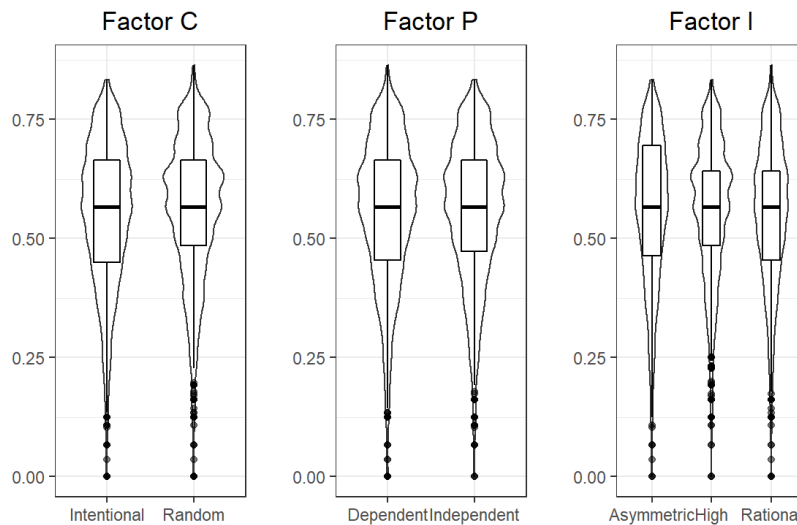


Figure 11. Risk level by factor.

The results of this subsection show that the behavioural measure risk level is the result of the interaction of two different effects. As shown in Table 16, the risk level taken by the subject is positively correlated with her or his general risk seeking attitude as measured by the DOSPERT scale. However, the analysis by socio-demographic profile suggests that risk taken in the experiment is also related to the lack of understanding of the security implications of some of the decisions made during online navigation, specially by sensitive groups of population such as elder participants.

D6.3: Report with Findings of Experiments and Policy implications

2.3.4 Complementarity of protection and insurance strategies

Cybersecurity strategy has three different components and all of them are related. Subjects can invest their cybersecurity budget in two alternative types of cybersecurity products: protection and insurance measures. This issue arises the question if subjects perceive both types of products as substitutive (can insurance replace protection?) or complementary (do insurance and protection work well together?). As a second question, it is convenient to check the existence of moral hazard or, in other words, if subjects behave in a less secure way when they are covered by an insurance policy. These two questions are critical for the development of a Cyberinsurance market in the EU: if insurance were actually perceived as a substitute of cyberprotection and fostered less secure online behaviour, the development of the cyberinsurance market would become critical for the security of the single digital market. These two questions are answered in this and next sections.

In the experiment, subjects are offered two different kinds of cybersecurity products: Security measures, which reduces the probability of suffering a cyberattack (Basic and Advanced), and Cyberinsurance, which reduces the impact of a cyberattack (None, Basic and Premium). Therefore, they can select one out of six combined cybersecurity strategies: BSMs+None, BSMs+Basic, BSMs+Premium, ASMs+None, ASMs+Basic, ASMs+Premium.

Almost half of the subjects selected the most secure strategy ASMs+Premium (45.8%), meanwhile very few decided to not purchase any product at all (3.4%). Table 18 shows the distribution of subjects selecting each strategy. The behaviour between subjects who bought the BSMs and subjects who bought the ASMs is different.

		<i>Cyberinsurance</i>			
		None	Basic	Premium	Total
<i>Security measures</i>	BSMs	3.44	8.77	4.44	16.65
	ASMs	3.56	34.02	45.77	83.35
	Total	7.00	42.79	50.21	100.00

Table 18. Cybersecurity strategies.

To analyse the relation between insurance and protection, the above table can be rewritten in the following way:

<i>Security measures</i>	<i>Cyberinsurance</i>			<i>Total</i>
	None	Basic	Premium	
BSMs	20.65	52.69	26.66	100.00
ASMs	4.27	40.81	54.91	100.00

Table 19. Cybersecurity strategies by protection measure.

D6.3: Report with Findings of Experiments and Policy implications

If we focus on subjects who bought ASMs, we notice that the majority of this subjects decide to purchase the Premium insurance whereas the majority of subjects who bought the BSMs decide to purchase the Basic insurance. The combination of the products should therefore be complementary (Figure 12): insurance does not substitute protection, but both types of products are purchased by the participants who are more sensitive to cybersecurity.

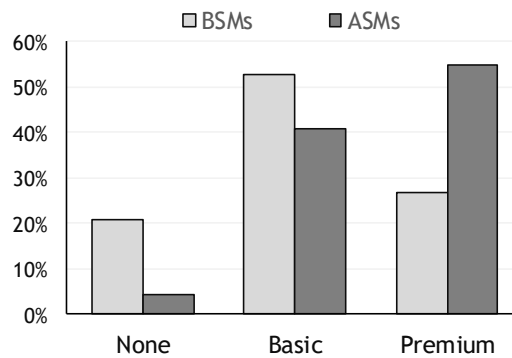


Figure 12. Cyberinsurance purchases by protection purchases.

A relevant question is how this complementarity between protection and insurance is influenced by the different experimental conditions. As shown in Table 15, only factor P (price dependence of protection and insurance) has a significant impact on the purchase of Premium insurance by subjects with basic and advance security measures. As expected, price dependence increases significantly the complementarity of ASMs and Premium insurance. For this reason, this price architecture seems especially useful to nudge for combinations of protection and insurance.

Factor		BSMs				ASMs			
		None (%)	Basic (%)	Premium (%)	p-value (X ² test)	None (%)	Basic (%)	Premium (%)	p-value (X ² test)
Context of the cyberattack (C)	C1: Random	19.95	51.31	28.74	0.371	4.40	41.84	53.76	0.353
	C2: Intentional	21.43	54.23	24.34		4.15	39.81	56.03	
Price dependency (P)	P1: Independent	16.99	52.69	30.32	0.002**	4.96	44.34	50.70	0.000***
	P2: Dependent	25.75	52.69	21.56		3.63	37.51	58.86	
Features of the cyberinsurance (I)	I1: Medium	21.59	50.76	27.65	0.833	4.42	38.85	56.74	0.423
	I2: Asymmetric	19.55	55.64	24.81		3.90	41.75	54.35	
	I3: High	20.82	51.67	27.51		4.51	41.85	53.64	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 20. Cyberinsurance purchases by protection purchases and factor.

D6.3: Report with Findings of Experiments and Policy implications

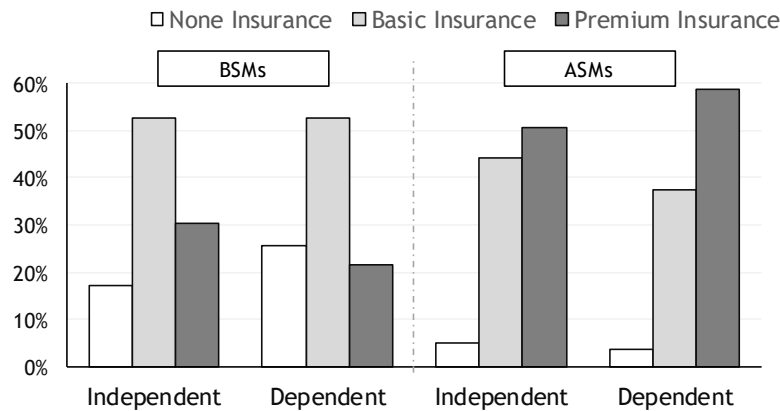


Figure 13. Cyberinsurance purchases by protection purchases and factor P.

2.3.5 Moral hazard: insurance taken and online risky behaviour.

Moral hazard is a critical issue for the efficient behaviour of an insurance market. In our case, if subjects behave in a less secure way after taken a cyberinsurance policy, the development of the cyberinsurance market could have the undesired consequence of increase the vulnerability of the single digital market as a whole. Fortunately, the results of the experiment show that this is not the case.

As presented in Table 21 and Figure 14 there are no significant differences in the risk taken by those subjects with no insurances or those with a basic or premium insurance policy. However, subjects behave in a significantly less safe way if they have not acquired advance protection. Once more the experiment shows a complementarity between safe components of the cybersecurity strategy (ASMs and safe online behave in this case).

Product		Risk level of online behaviour				p-value (ANOVA)
		n	Mean	SD	Max-Min	
Security measures	BSMs	799	0.583	0.140	0-0.833	0.000***
	ASMs	4001	0.552	0.151	0-0.864	
Cyberinsurance product	None	336	0.557	0.168	0-0.833	0.200
	Basic	2054	0.561	0.148	0-0.864	
	Premium	2410	0.553	0.148	0-0.833	
Cybersecurity strategy	BSMs + None	165	0.5953	0.153	0.125-0.833	0.000***
	BSMs + Basic	421	0.5877	0.1273	0.107-0.833	
	BSMs + Premium	213	0.5627	0.1525	0-0.833	
	ASMs + None	171	0.5207	0.1747	0-0.797	
	ASMs + Basic	1633	0.554	0.1525	0-0.864	
	ASMs + Premium	2197	0.5519	0.1471	0-0.833	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 21. Risk level by protection and insurance strategies.

D6.3: Report with Findings of Experiments and Policy implications

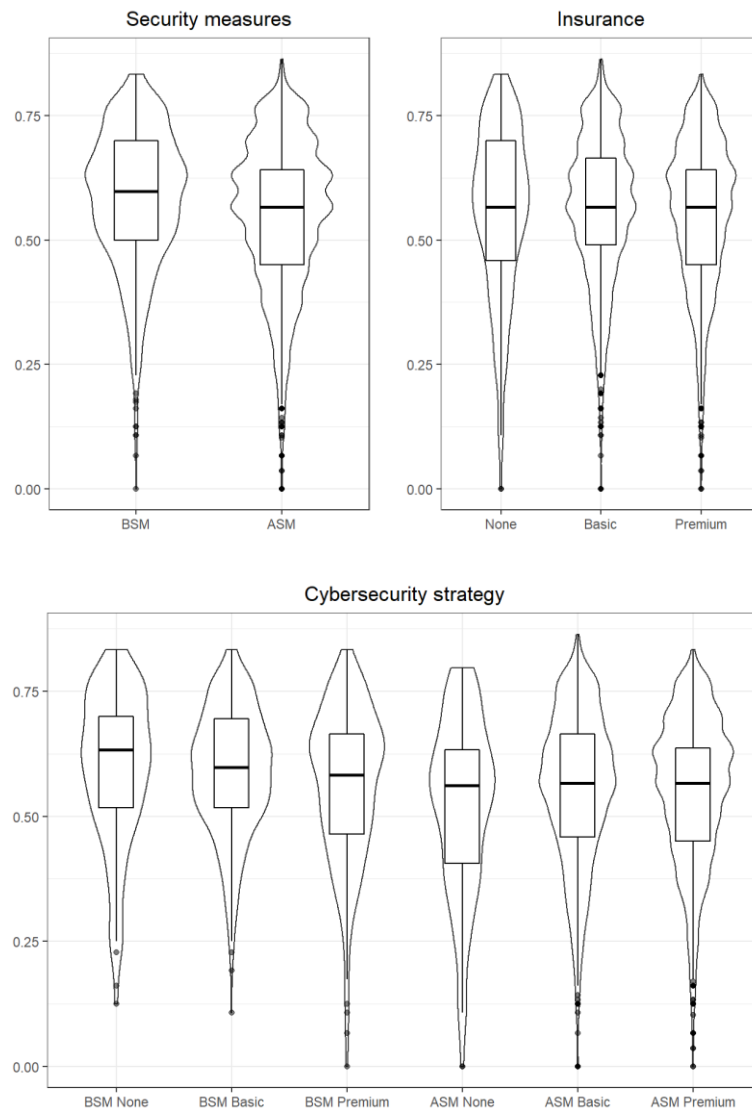


Figure 14. Risk level by protection and insurance strategies.

D6.3: Report with Findings of Experiments and Policy implications

2.4 Learning process and updating of believes

This section presents how subjects change their cybersecurity strategy from the first to the second round of the experiment, after having the experience of suffering or not a cyberattack. Since there are no significant changes in the risk level of the online behaviour in both rounds, this section focuses in the analysis of the protection and insurance strategies of the subjects.

2.4.1 Protection strategy

Table 22 shows the SMs purchases distribution between the two periods. We observe that there the acquisition of advance protection is a significant although slightly higher in the second round (p value = 0.042).

Period	Security Measures		p -value (χ^2 test)
	BSMs (%)	ASMs (%)	
1st	16.64	83.36	0.042**
2nd	15.44	84.56	

* p -value < 0.1; ** p -value < 0.05; *** p -value < 0.001

Table 22. Protection strategy by period.

However, the relevant analysis here is that of the transition between both levels of protection from the first to the second round and how such transition matrix is affected by suffering or not the cyberattack. It must be highlighted that 16.5% of subjects changed their decision between periods, although attacks in the first and second period are independent and equally likely. As shown in Table 23 and in Figure 15, more than half subject who bought the BSMs in the 1st period decided to buy the ASMs in the second one while only the 9.2% of subject who bought the ASMs in the 1st period, purchased the BSMs in the second one.

SMs	1st Period		2nd Period	
	BSMs		ASMs	
	n	%	n	%
BSMs	374	46.81	425	53.19
ASMs	367	9.17	3634	90.83

Table 23. Transition between protection strategies.

D6.3: Report with Findings of Experiments and Policy implications

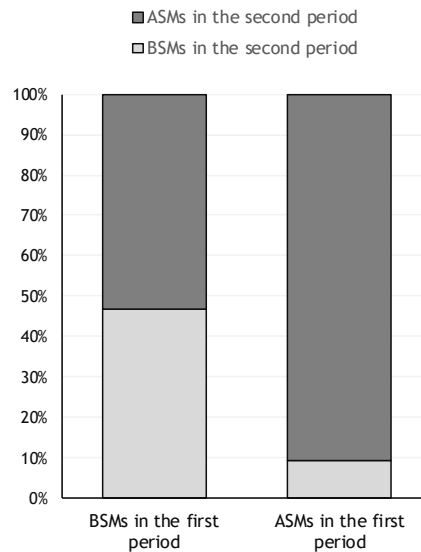


Figure 15. Transition between protection strategies (%).

Let us analyze how the experience of the cyberattack affects the transition matrix. Table 24 shows the distribution splitting the sample between subjects who suffer and not the attack in the 1st period.

1 st Period		2 nd Period			
SMs	Attack	BSMs		ASMs	
		n	%	n	%
BSMs	No	151	49.83	118	50.17
ASMs		152	5.03	2228	94.97
BSMs	Yes	223	44.96	273	55.04
ASMs		249	15.05	1406	84.95

Table 24. Transition between protection strategies by experience of cyberattack.

The experience of the cyberattack nudges to change the protection strategy to a higher extend than the experience of not suffering it. Specifically, only 10.2% of the subject that suffered the attack updated their protection strategy, in comparison to the 24.3% of the participants being attacked. Moreover, meanwhile the transition with no attack is almost always to a higher protection, the experience of the cyberattack can change the subject's believes in two opposite directions, as shown it Table 24 and Figure 15:

- More than half (55.0%) of the subjects with basic protection in the first period purchase advance protection in the second one. This can be only motivated by a variation of the believes of the likelihood of the attack. Although this update can have a rational component (coming from an update of the increase of the probability of the attack that specific online action may produce), the size of the effect suggests

D6.3: Report with Findings of Experiments and Policy implications

the action of behavioural levers that may increase the salience of the cyberattack and the concern of the subject to suffer it³.

- 15.1% of the subjects acquiring advance protection measures in the first period do not purchase them in the period two. In other words, the experience of the cyberattack reduced their trust in the efficacy of advance protection, even they know that the reduction of the probability of the ASMs is the same in both periods, reducing the chances to suffer the attack in 20 percentual points.

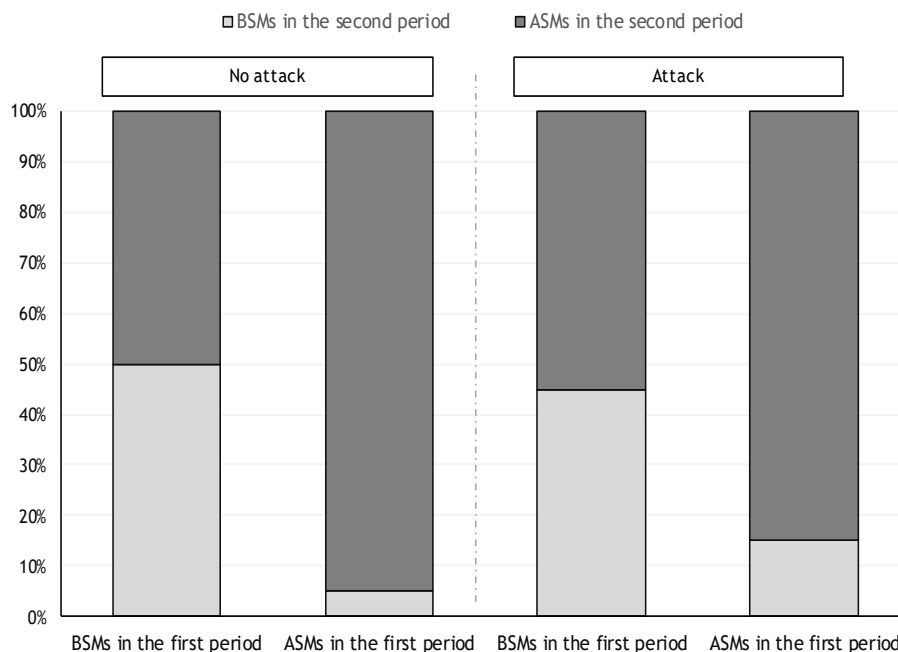


Figure 16. Transition between protection strategies by experience of cyberattack.

2.4.2 Cyberinsurance strategy

Table 25 shows the cyberinsurance purchases distribution in both two periods, which are significantly different (p value = 0.000). Although a similar share of subjects does not take any insurance in the first (7.0%) and second (6.3%) periods, there is a relevant increase of Premium policies and reduction of basic policies in the second.

³ This issue was discussed in the qualitative in-depth interviews run during the face-to-face pilot of the experiment. The most general answer when subjects were inquired about this change of protection strategy was that after suffering an attack they know that nothing has changed from the first period but they were 'more afraid' of the possibility of receiving the attack. This discussion point out to a difference between the probabilities themselves (that they considered as unchanged) and the decision weights applied in decision making, as considered in Prospect Theory (Kahneman and Tversky, 1979).

D6.3: Report with Findings of Experiments and Policy implications

Period	Cyberinsurance policy			p-value (x2 test)
	None (%)	Basic (%)	Premium (%)	
1st	7.00	42.80	50.21	0.000***
2nd	6.25	26.92	66.84	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 25. Cyberinsurance strategies by period.

One third of subjects changed their insurance decision between periods. As shown in Table 27 and in Figure 17, the general trend is to increase the coverage level in the second period: 74.7% of the subjects who change the insurance decision improve their insurance. Specifically, almost half of subjects who did not contract any insurance in the 1st period decided to take a policy in the second one. On the other hand, 51.2% of subjects who purchased the Basic insurance in 1st period decided to contract the premium one in the second one. Alternatively, only the 11.7% of subject who bought the Premium insurances in the 1st period, decided to change to basic insurance in the 2nd period.

Cyberinsurance	1st Period		2nd Period			
	None		Basic		Premium	
	n	%	n	%	n	%
None	185	55.06	80	23.81	71	21.13
Basic	72	3.51	931	45.33	1051	51.17
Premium	43	1.78	281	11.66	2086	86.56

Table 26. Transition between cyberinsurance strategies.

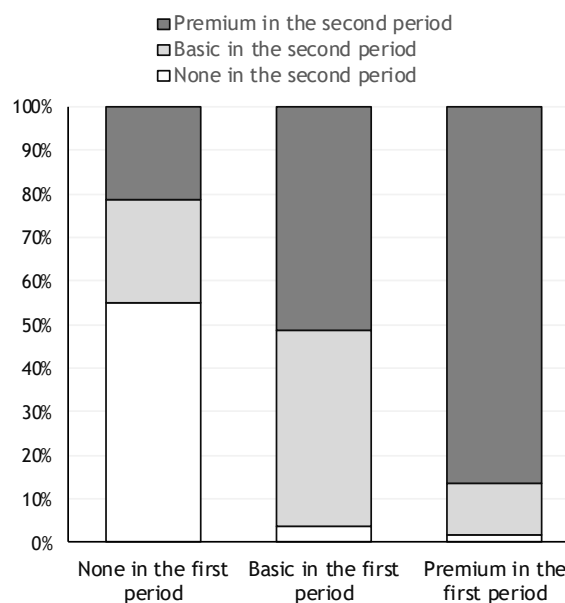


Figure 17. Transition between cyberinsurance strategies.

D6.3: Report with Findings of Experiments and Policy implications

The impact of the experience of the cyberattack in the change of insurance strategy is shown in Table 27. As discussed for the protection strategy, the experience of suffering the attack increases the percentage of subjects changing their cyberinsurance decision: 39.2% of the subjected suffering the attack change the insurance decisions, meanwhile 28.5% of the subjects who did not suffer the cyberattack changed.

<i>1st Period</i>		<i>2nd Period</i>					
<i>Cyberinsurance</i>	<i>Attack</i>	<i>None</i>		<i>Basic</i>		<i>Premium</i>	
		<i>n</i>	<i>%</i>	<i>n</i>	<i>%</i>	<i>n</i>	<i>%</i>
None	No	88	54.32	42	25.93	32	19.75
Basic		35	3.14	564	50.58	516	46.28
Premium		12	0.87	117	8.53	1243	90.60
None	Yes	97	55.75	38	21.84	39	22.41
Basic		37	3.94	367	39.08	535	56.98
Premium		31	2.99	164	15.80	843	81.21

Table 27. Transition between cyberinsurance strategies by experience of cyberattack.

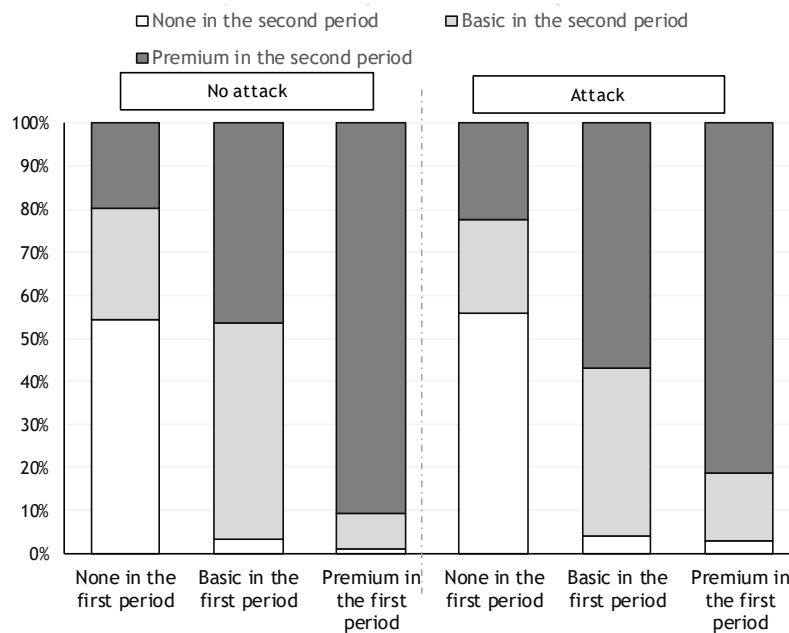


Figure 18. Transition between cyberinsurance strategies by experience of cyberattack.

3 Experiment 2: Behavioural insights of CYBECO toolbox.

3.1 Rationale of experiment 2

Experiment 2 aims to test the CYBECO toolbox. The toolbox takes the form of an online calculator to guide the user through analyzing their current cybersecurity risk level and deciding the optimal cybersecurity strategy for their needs. The calculator takes the form of a multi-step online form which asks pertinent questions (e.g., SME size, characteristics, relevant threats, available security measures) and offers the best option for the SME based on the outcomes of CYBECO cyber risk management models.

In Experiment 2, participants were invited to use a mock-up version of the cyber-risk analysis tool for SMEs included in the CYBECO toolbox and based in the CYBECO model. Concretely, participants were assigned an initial endowment that could be used to buy a combination of insurance and protection measures. For this task, subject counted with the help of the output page of the CYBECO toolbox to provide information on the results of the cyber-risk analysis and to guide them during the purchase of cyberinsurance and protection measures. The selected cybersecurity strategy and the fact of suffering or not a random cyberattack determined the payoff to be received at the end of the experiment. The experimental session included pre- and post- questionnaires to provide classification information and evaluate the usability of the output page of the CYBECO toolbox. Experiment 2 was run under five experimental conditions or treatments, consisting in five different designs of the output page of the CYBECO toolbox. The five designs are presented in detail in the next section.

Since the aim of experiment 2 is to test the effectivity and usability of the CYBECO toolbox, the selection of the participants become critical. For this reason, the sample of 2,000 participants in experiment 2 was recruited among potential users of the tool from SMEs or autonomous workers (entrepreneurs, freelancers, etc.). Participants were required to work in positions related to decision-making in the areas of cybersecurity and insurance, from a technical, managerial or purchases departments of SMEs. As described in detail in subsection 3.2.4, this challenging recruitment process was successful, since half of the participants have purchased protection measures for their SMEs and forth of them do have even contracted cyberinsurance policies in the past. Since the condition of having already purchased was not explicitly required, we can consider the participants in the sample as potential users of the CYBECO toolbox.

D6.3: Report with Findings of Experiments and Policy implications

3.2 Methodology of experiment 2

This section presents the main methodological features of Experiment 1, specifically its experimental conditions and behavioural measures, as well as a brief report of the implementation of the experimental sessions.

3.2.1 Experimental Conditions

This experiment is focused in the potential framings of the output page of the CYBECO toolbox. This interactive screen presents the costs and impacts of the five best cybersecurity strategies for the subject, according with the CYBECO model. Using the functionalities of this page, subjects are able to analyse in detail the five option and, at a latter step of the experiment, to purchase the protection and insurance strategies that they decide (despite of the recommendations of the CYBECO toolbox).

The experiment considers the following five framings for the interactive risk analysis dashboard of the toolbox:

D6.3: Report with Findings of Experiments and Policy implications

- Treatment 1 (Expected - Losses).** This treatment, shown in Figure 19, presents the risk analysis in terms of the expected values of the losses to be faced by the subject when applying each of the five cybersecurity strategies. The expected value is computed using the probabilities of the two alternative scenarios (suffering or not the cyberattack) and the monetary losses to be suffered in each scenario (prices of protection and insurance products, losses in the commercial value of the data and the potential compensation of the insurance policy taken by the subjects). This framing is the original proposal presented in the CYBECO toolbox.

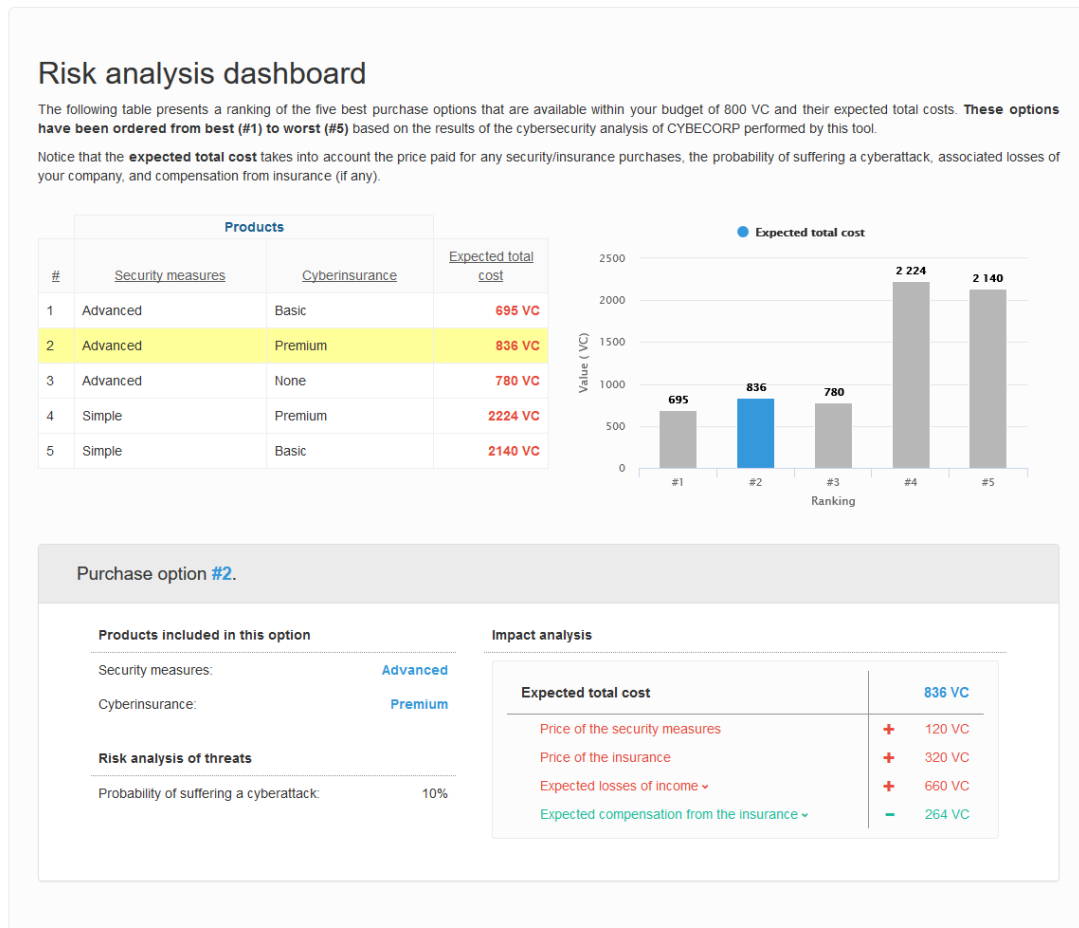


Figure 19. Treatment 1 (Expected - Losses)

D6.3: Report with Findings of Experiments and Policy implications

- **Treatment 2 (Expected - Losses - Salience).** The information is presented here with the same framing than in treatment 1. However, the difference is that treatment 2 includes a high salience message communicating that the first option in the ranking is recommended by the cybersecurity experts and a click for direct purchase of the recommended option. The framing of treatment 2 is presented in Figure 20.

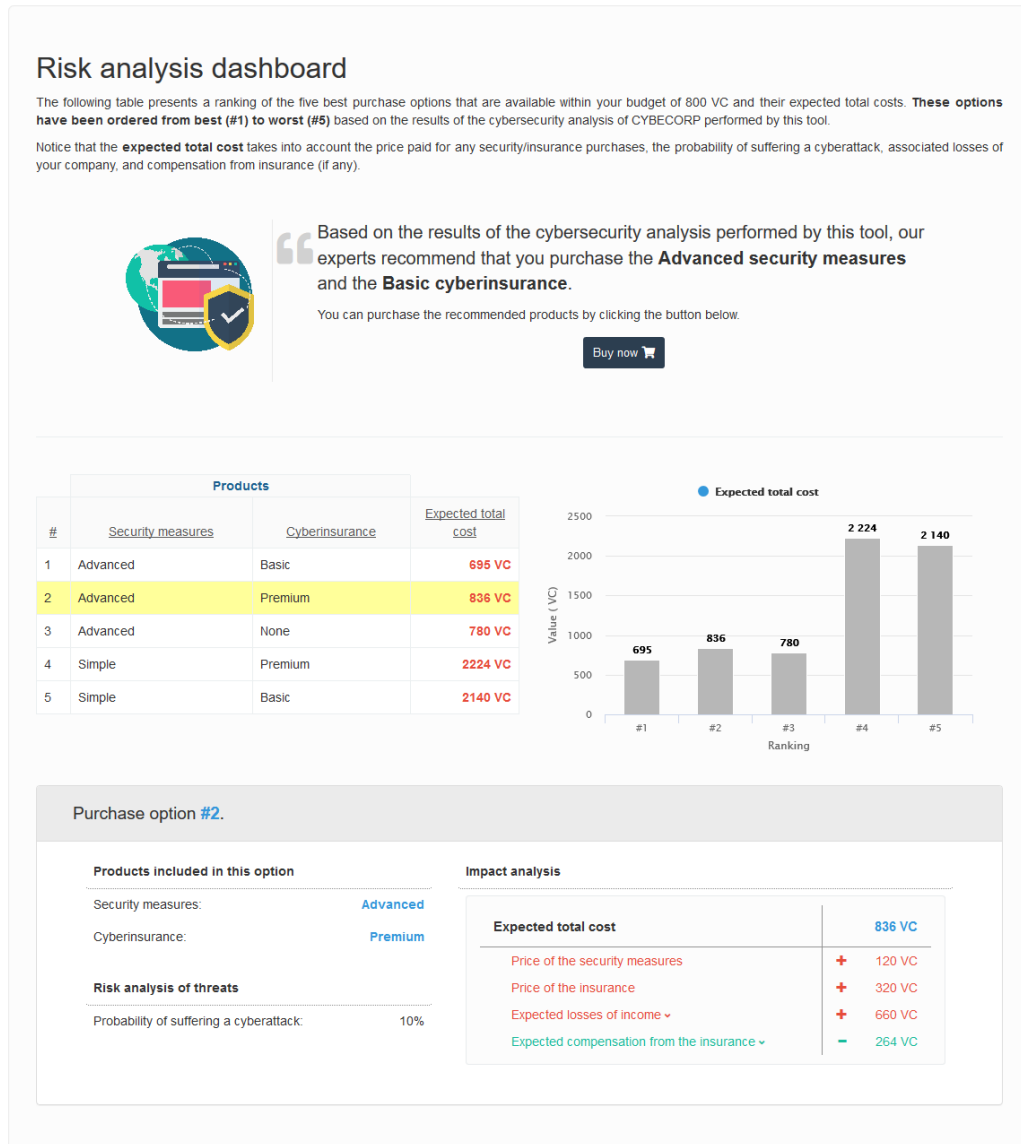


Figure 20. Treatment 2 (Expected - Losses - Salience)

D6.3: Report with Findings of Experiments and Policy implications

- *Treatment 3 (Expected - Gains)*. Although the information is presented again using expected values, the output does not provide information of the expected losses to be suffered by the subjects but on the total income that the company would obtain using each of the analysis cybersecurity strategies. This treatment can be compared to treatment 1 to analyze the impact of loss aversion in subject cybersecurity decision-making. The output under this framing is shown in Figure 21.

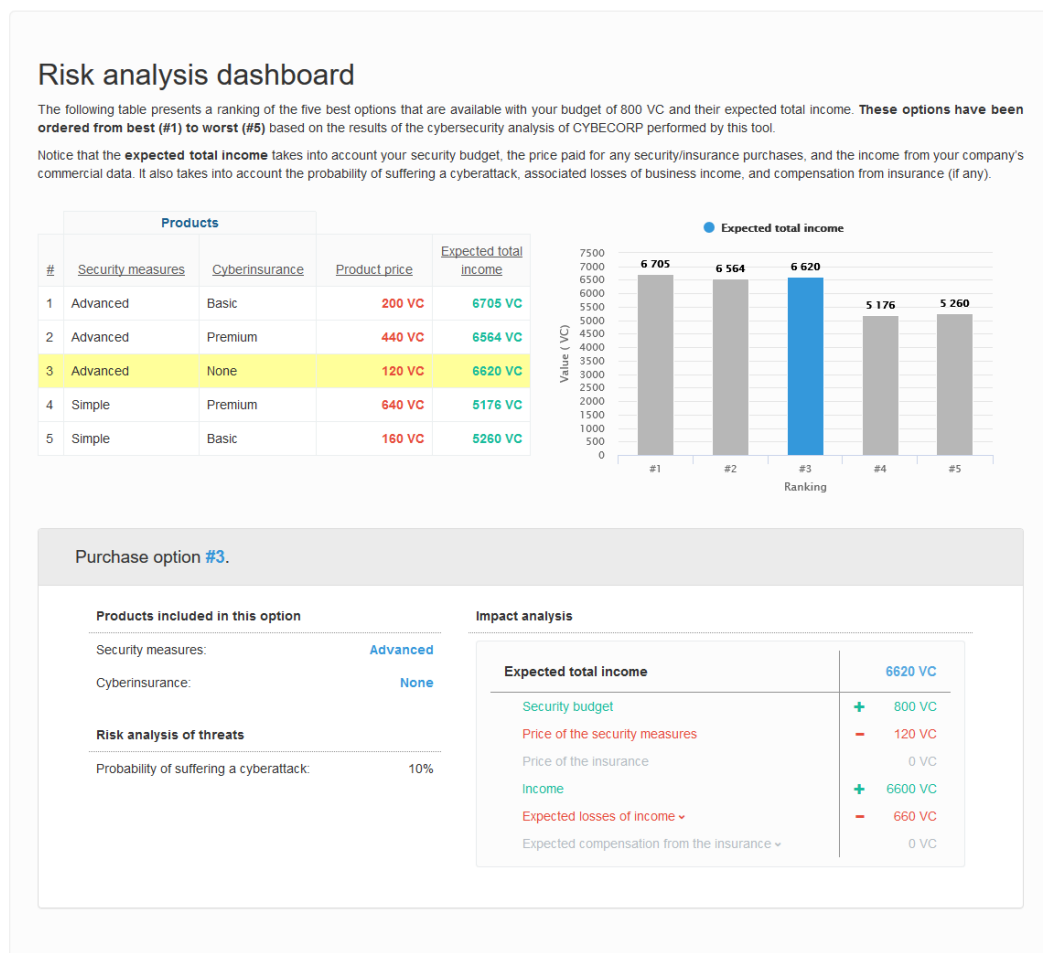


Figure 21. Treatment 3 (Expected - Gains)

D6.3: Report with Findings of Experiments and Policy implications

- **Treatment 4 (Scenario - Losses).** This treatment shares with treatment 1 the feature that the information is presented frames as losses. However, there is a key difference given by the fact that information is not presented as expected values but disaggregated for the scenarios of suffering and not suffering the cyberattack. The output page for this treatment is presented in Figure 22. It must be highlighted that in this treatment the subject is provided with all the information required to determine is optimal cybersecurity strategy in terms of her or his utility function and risk attitude. In treatments 1 to 3, such information was not available and the subject is required to decide using only the expected values.

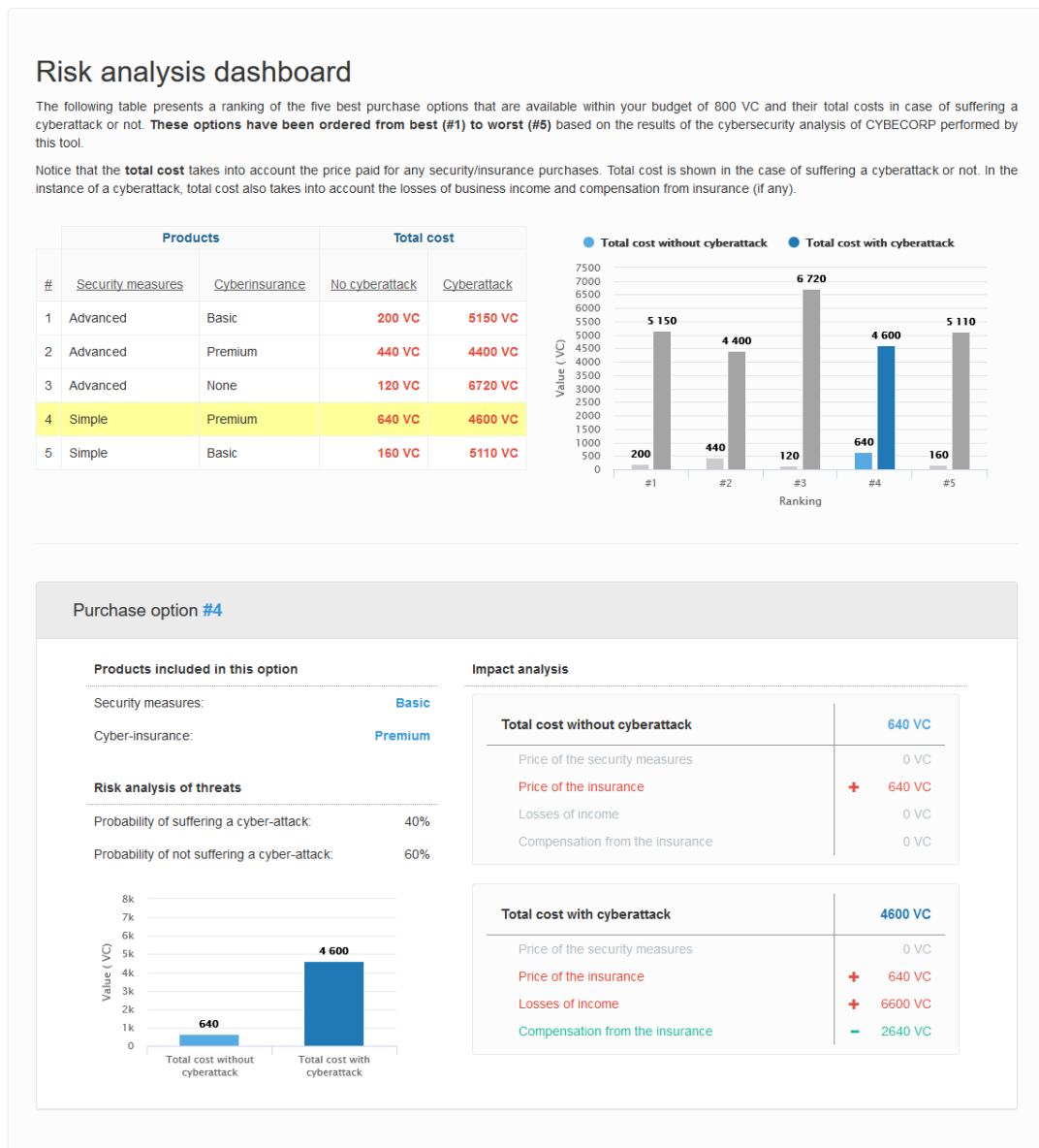


Figure 22. Treatment 4 (Scenarios - Losses)

D6.3: Report with Findings of Experiments and Policy implications

- **Treatment 5 (Scenarios - Gains).** This output page in this treatment, shown in Figure 23, is like that of treatment 2, with the difference that the information is framed as gains instead of as losses.

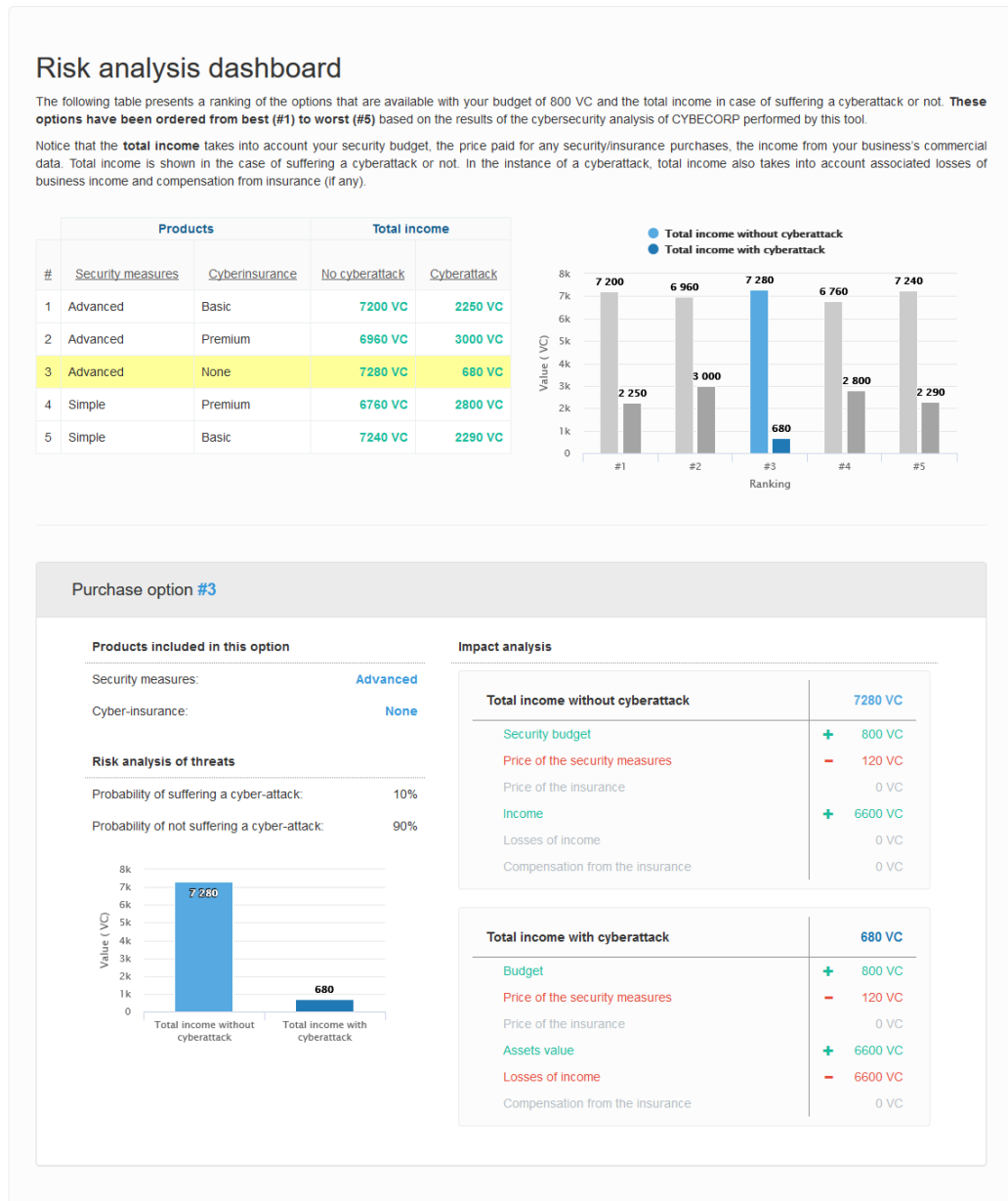


Figure 23. Treatment 5 (Scenarios - Gains)

D6.3: Report with Findings of Experiments and Policy implications

3.2.2 Behavioural measures

Experiment 2 contains two types of behavioural measures:

- The protection and insurance strategies selected by the subject after using CYBECO tool to perform a risk analysis of her or his situation. The available products and their main features (price, coverage, protection level, etc.) are presented in



Measures	Product	Description	Cost
 Security measures Security measures are computer softwares used to prevent, detect and remove malicious software	Simple	Reduces the probability of suffering the attack from 60% to 40% .	0 VC
	Advanced	Reduces the probability of suffering the attack from 60% to 10% . In addition, if you buy our Advanced security measures you will have a <u>50% discount</u> on the purchase of a cyberinsurance.	120 VC
 Cyberinsurance Cyberinsurance is an insurance product used to protect businesses from Internet-based risks	None	Covers 0 VC of lost profits in case of attack.	0 VC
	Basic	Covers 1650 VC of lost profits in case of attack.	160 VC
	Premium	Covers 3300 VC of lost profits in case of attack.	640 VC

Figure 24.



Measures	Product	Description	Cost
 Security measures Security measures are computer softwares used to prevent, detect and remove malicious software	Simple	Reduces the probability of suffering the attack from 60% to 40% .	0 VC
	Advanced	Reduces the probability of suffering the attack from 60% to 10% . In addition, if you buy our Advanced security measures you will have a <u>50% discount</u> on the purchase of a cyberinsurance.	120 VC
 Cyberinsurance Cyberinsurance is an insurance product used to protect businesses from Internet-based risks	None	Covers 0 VC of lost profits in case of attack.	0 VC
	Basic	Covers 1650 VC of lost profits in case of attack.	160 VC
	Premium	Covers 3300 VC of lost profits in case of attack.	640 VC

Figure 24. Available protection and cybersinsurance strategies.

- Usability measures evaluated through the usability questionnaire at the end of the experiment.

3.2.3 Experiment implementation

The fieldwork of experiment started on 25th September 2018 in the four countries. Invitations to participate to the experiment were sent constantly to the online panel during the duration of the experiment in order to reach the required quota by country. Once a quota was reached, the system stopped sending invitations to those profiles, and the speeders (the speeders are respondents completing the experiment in less than one third of the median time allocated by participants in a given country) were identified in the following 24/48 hours and then removed from the quota. After that, the quota was then re-opened to complete it. On 14th October 2018, the final target was reached, and the experiment stopped. In the table below the speeders by country are presented together with the final number of respondents who successfully implemented the experiment.

D6.3: Report with Findings of Experiments and Policy implications

	<i>Country</i>				
	Germany	Spain	Poland	UK	Total
<i>Total subjects click the email</i>	713	614	708	689	2724
<i>Total subjects access the experiment</i>	697	612	695	665	2669
<i>Total subjects complete the experiment</i>	524	526	535	534	2119
<i>Total 'speeders'</i>	4	23	1	13	41
Effective final sample	520	503	534	521	2078

Table 28. Breakdown of participants by country.

A total of 2,724 participants clicked on the email that gave access to the experiment and 2,669 accessed the experiment, Table 2. Out of these, 2,119 completed the experiment. However, 41 of these were classified as 'speeders'. The average dropout, participants who took part but did not complete the experiment, was 22.2%, where the lowest % of dropouts is found in Spain (13.0%) and the highest % is found in Germany (26.2%).

Regarding the duration of the experiment, there were no big differences among the countries: the median duration was 13 minutes, with respondents from Germany taking a little longer (13.5 minutes) and respondents from Poland and UK who were faster (12.0 minutes). Table 5, presents the detailed average and median durations.

	<i>Country</i>				
	Germany	Spain	Poland	UK	Total
<i>Average (sec)</i>	1248.0	1038.0	1080.0	1008.0	1092.0
<i>Average (min)</i>	20,8	17,3	18,0	16,8	18,2
<i>Median (sec)</i>	810.0	720.0	720.0	720.0	780.0
<i>Median (min)</i>	13.5	12.0	12.0	19.0	13.0

Table 29. Breakdown of participants by country

3.2.4 Profile of the participants

The second experiment is aimed to provide insights to improve the design and usability of the CYBECO toolbox. To guarantee the ecological validity of the experiment and the reliability of these insights, it is critical to recruit the participants among real potential users of a cyber-risk analysis tool and potential purchasers of the cybersecurity products (protection measures and insurance policies) to be considered by the CYBECO toolbox.

The 2,078 participants in the experiment have been recruiting among owner and workers in SMEs with positions and responsibilities related to the topic of CYBECO. As shown in Table 30, 23.5% of the participants have previous experience in purchasing of cyberinsurance products and 50.1% of the participants have selected and acquired protection measures. Around one third of the sample (34.7%) has experience in managerial positions of the SME and 30.1% has previously have responsibilities related to purchases for the SME.

D6.3: Report with Findings of Experiments and Policy implications

<i>Experience</i>	n	%
Experience in IT systems	1213	58.37
Experience in management positions	720	34.65
Experience in purchasing	625	30.08
Experience in a cybersecurity	303	14.58
Purchase of protection measures	1041	50.10
Purchase of cyberinsurance	489	23.53

Table 30. Experience of the participants (at last one year).

Regarding education of participants, a third of participants had obtained a university degree (Table 4).

<i>Education level</i>	n	%
0-11 years of education	123	5.92
12 years of education	519	24.98
Some years of university	225	10.83
University degree	706	33.97
Post-graduate degree	505	24.30
<i>Total</i>	<i>2078</i>	<i>100.00</i>

Table 31. Level of education of the participants.

3.3 Impact of the output design in the selection of the cybersecurity strategy of the SME

This section is focused in the analysis of how the different designs of the output webpage can influence the cybersecurity strategy selected by the participants, specifically the selection of the protection and cybersinsurance strategies to be adopted by the SME. For each strategy, this section presents and analyses the impact of the output design for the sample as a whole, as well as for the different potential segment of users in terms of their previous experience.

3.3.1 Protection strategy

The application of advance security measures is the protection strategy suggested by all the three first option in the ranking of recommendations of the CYBECO toolbox. More than four-fifths of subjects (80.8%) have followed the suggestion and bought the ASMs.

However, as shown in Table 32 and Figure 25, the design of the output page influences subjects' behaviour. The shares of subjects purchasing ASMs are significantly different among treatments (p -value = 0.009). As expected, the purchases of ASMs are higher in treatment 2, where a high salience messages highlights that ASMs is the option

D6.3: Report with Findings of Experiments and Policy implications

recommended by the experts and there is a direct purchase button to obtain it. As generally observed in the behavioural literature, this strategy is very effective in situations where the information is complex, since its provide with a predetermined default option to cope with the cognitive charge of processing the information to make the decision.

<i>Treatment</i>		<i>Security Measures</i>	
ID	Conditions	BSMs (%)	ASMs (%)
1	Expected - Losses	19.07	80.93
2	Expected - Losses - Salience	13.30	86.70
3	Expected - Gains	20.33	79.67
4	Scenarios - Losses	20.33	79.67
5	Scenarios - Gains	22.82	77.18

Table 32. Protection strategy by treatment.

Regarding the other four treatments, Figure 25 shows that the percentage of subjects selecting ASMS is higher in treatment 1 (Expected - Losses), similar in treatments 3 (Expected - Gains) and 4 (Scenarios - Losses) and lower in treatment 5 (Scenarios - Gains).

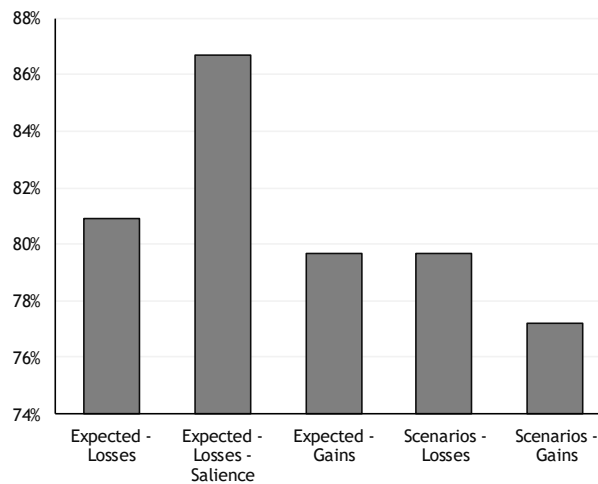


Figure 25. Protection strategy by treatment

In other words, if we compare the ASMs purchases when the framing is in losses and gains, treatment 1 versus 3 and treatment 4 versus 5, we notice that the purchases of ASMs is always higher in losses framings than in gains framing, the other condition kept constant. A possible explanation for that is the effect of loss aversions: subjects react to a framing in losses with more intensity and a higher willingness to get protection.

D6.3: Report with Findings of Experiments and Policy implications

We can also observe that, kept the framing in losses or gains unchanged, the purchases of ASMs higher when the results of the risk analysis are presented as expected values instead of the probabilities of each scenario (attack / not attack) to take place and the impact of the protection strategy for each scenario. Specifically, the adoption of ASMs is more common in treatment 1 (Expected - Losses) than in treatment 4 (Scenarios - Losses) and in treatment 3 (Expected - Gains) than in treatment 5 (Scenarios - Gains). There are different explanations for this result. First of all, if subjects are provided with the detailed information for each scenario, they are able to determine which is the best option for them in terms of their own risk aversion. Since this analysis is not possible from the expected value, they can only decide to follow or not the recommendation that has been proposed by the CYBECO model and presented by the toolbox for similar SMEs.

3.3.1.1 Expertise of the potential user

The experiment sample includes subjects with different experience and fields of expertise. As shown in Table 33 and Figure 26, the selected protection strategy depends significantly of some these characteristics of the participant.

Subjects with experience in the use of IT systems and in cybersecurity purchase significantly more advance protection than those with no experience in IT ($p\text{-value} = 0.008$). On the other hand, only 71.0% of subjects with expertise in cybersecurity selected the advance protection. Moreover, subjects with cybersecurity expertise follow the suggestion of CYBECO toolbox to a significantly lower extend ($p\text{-value} = 0.000$).

Expertise		Security Measures		$p\text{-value}$ (x2 test)
		BSMs (%)	ASMs (%)	
Use IT systems	No	21.85	78.15	0.008**
	Yes	17.23	82.77	
Management position	No	19.22	80.78	0.916
	Yes	19.03	80.97	
Responsibility for purchasing	No	18.72	81.28	0.444
	Yes	20.16	79.84	
Cybersecurity role	No	17.46	82.54	0.000***
	Yes	29.04	70.96	

* $p\text{-value} < 0.1$; ** $p\text{-value} < 0.05$; *** $p\text{-value} < 0.001$

Table 33. Protection strategy by field of expertise.

Experience in management or purchasing department of the SMEs have no significant impact on the adoption or not of advance protection measures.

D6.3: Report with Findings of Experiments and Policy implications

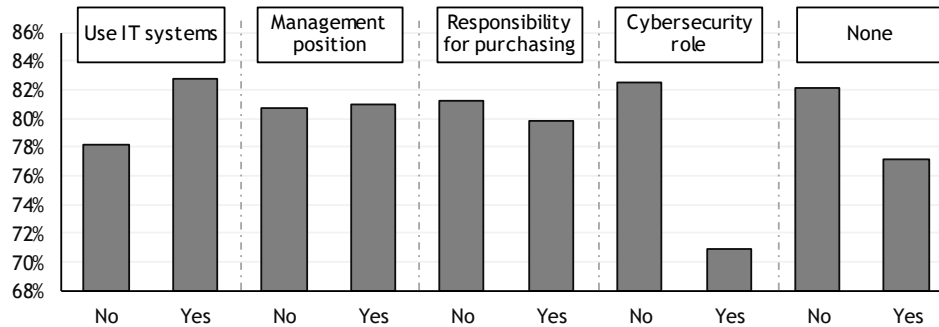


Figure 26. Protection strategy by field of expertise.

A similar conclusion can be obtained from the analysis of the protection measures purchased by those subjects with previous experience in the purchase of protection or cyberinsurance (Table 34). Their expertise translates to more independence at decision-making, since the acquisition of the suggested ASMs are significantly lower among participants within these two expertise segments (p -value = 0.002 and p -value = 0.000, respectively).

Expertise		Security Measures		p -value (χ^2 test)
		BSMs (%)	ASMs (%)	
Buying protection measures	No	17.16	82.84	0.022**
	Yes	21.13	78.87	
Buying cyberinsurance products	No	17.05	82.95	0.000***
	Yes	25.97	74.03	

* p -value < 0.1; ** p -value < 0.05; *** p -value < 0.001

Table 34. Protection strategy by buying expertise.

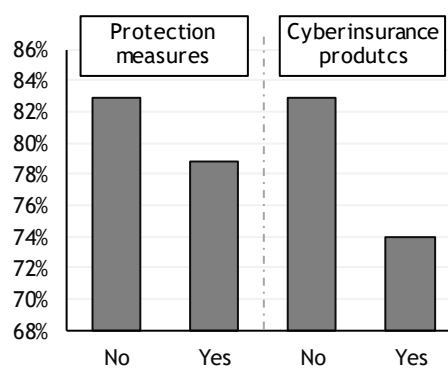


Figure 27. Protection strategy by buying expertise

Notice that the ASMs sales are even lower in participants with experience in buying cyberinsurance products (74.0%) in comparison with participants with expertise buying protection measures (78.9%).

D6.3: Report with Findings of Experiments and Policy implications

3.3.2 Cyberinsurance strategy

This section presents the results for the second individual behavioural measure: the insurance strategy. Subjects are offered to acquire or not two different insurance products, basic and premium insurance, the second one offering a higher coverage at a higher price. It must be highlighted that almost all subjects (92.1%) decided to purchase some type of cyberinsurance. Moreover, more than half of the subjects (57.4%) bought the Basic Insurance policy and 34.7% the Premium Insurance one. Alternatively, only 7.9% of the subjects did not contract any cyberinsurance product.

Table 32 shows how the design of output page of the CYBECO toolbox influences significantly insurance strategy ($p\text{-value} = 0.009$). With the expectation of treatment 2, the design is not able to influence the purchase or not of an insurance policy, but conditions the coverage and prime to be chosen by the insurance taker. Specifically, as shown in Table 35, the percentage of non-insured subjects is around 8.5% for treatments 1, 3, 4 and 5. Alternatively, purchases of Basic Insurance policy is are significantly higher in treatment 2, which highlights that this is the recommended insurance product for similar SMEs and includes a direct-purchase link. This result is similar to that of the protection strategy and can be explained in the same way.

<i>Treatment</i>		<i>Cyberinsurance products</i>		
ID	Conditions	None (%)	Basic (%)	Premium (%)
1	Expected - Losses	8.07	55.99	35.94
2	Expected - Losses - Saliency	4.99	78.15	16.86
3	Expected - Gains	8.85	52.15	39.00
4	Scenarios - Losses	8.61	52.39	39.00
5	Scenarios - Gains	8.98	47.82	43.20

Table 35. Cyberinsurance strategy by treatment.

Treatments 1, 3, 4 and 5 do affect to the decision about the coverage of the acquired insurance, and then purchase of the Basic insurance (that occupies the first position in the ranking of recommendations of the CYBECO toolbox) or of the second recommended option given by the Premium insurance. Moreover, the influence of the design over the cyberinsurance strategy follows similar patterns than their influence over the protection strategy.

Framing the information in losses while keeping constant the other key feature of the output page (i. e. the use of expected values or values for scenarios) increases the coverage of the insurance policies selected by the subjects. The share of the Premium policy is higher in treatment 1 (Expected - Losses) than in 3 (Expected - Gains) and in and in treatment 4 (Scenarios - Losses) than in 5 (Scenarios - Losses). Finally, we can observe that providing the information (gains or losses) disaggregated by scenario reduces the purchase level of the recommended option, i. e. the Basic policy.

D6.3: Report with Findings of Experiments and Policy implications

The reason of the impact of presenting expected values or values per scenario could be similar to those discussed in the protection strategy. Providing information per scenario we allow subjects to check if the suggested option coincides with the best option given their risk attitude and, due to the potential heterogeneity of the subjects, some of them would opt for the Premium policy as their best insurance strategy. However, loss aversion is not able to explain the impact of framing results as losses, since loss-framing nudges to the purchase of premium insurance instead of the basic recommended option.

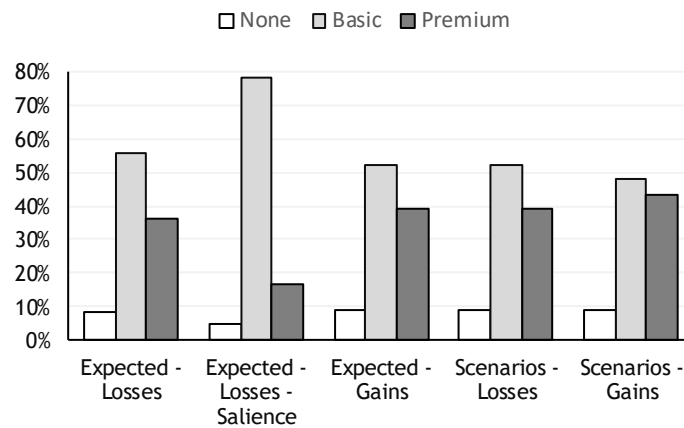


Figure 28. Cyberinsurance strategy by treatment.

3.3.2.1 Expertise of the potential user

The selection of the cyberinsurance strategy depends significantly on the field of expertise of the subject. As shown in Table 36 and Figure 29, previous expertise in management position or purchasing department of the SME increases significantly the purchase of cyberinsurance ($p\text{-value} = 0.000$). The same trend, although the result is not statically significant, can be found in subjects with expertise in IT and cybersecurity. Moreover, the purchase of Basic policies is 6.0 percentage points higher among participants with experience in a management position in the SME and 3.5 points higher in subjects with expertise in SME purchases.

Expertise		Cyberinsurance products			p-value (x2 test)
		None (%)	Basic (%)	Premium (%)	
Use IT systems	No	9.25	56.53	34.22	0.153
	Yes	6.92	57.96	35.12	
Management position	No	9.43	55.30	35.27	0.000***
	Yes	5.00	61.25	33.75	
Responsibility for purchasing	No	9.50	56.37	34.14	0.000***
	Yes	4.16	59.68	36.16	
Cybersecurity role	No	8.23	56.96	34.82	0.353
	Yes	5.94	59.74	34.32	

D6.3: Report with Findings of Experiments and Policy implications

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 36. Cyberinsurance strategy by field of expertise.

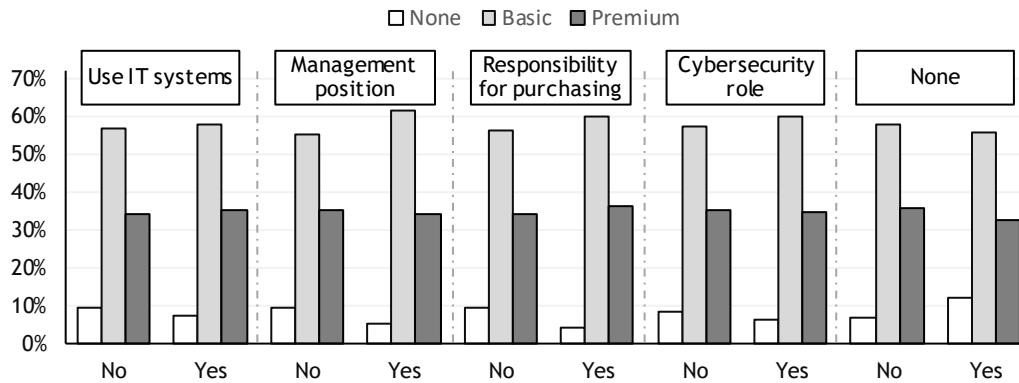


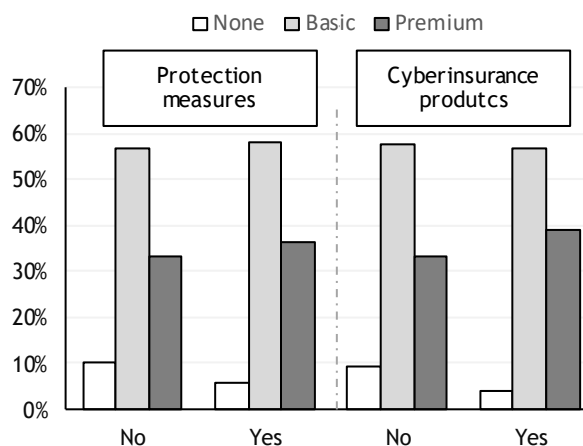
Figure 29. Cyberinsurance purchases by field of expertise.

Subjects with previous experience in the purchase of protection measures and cyberinsurance products for SMEs do also buy cybersinsurance in a significantly higher proportion than the other ($p\text{-value} = 0.001$ and $p\text{-value} = 0.000$, respectively). This results is supported by Table 37 and Cyberinsurance purchases by buying expertiseFigure 30, that also show that experience in buying these products is also related to a higher purchase of Premium policies.

Expertise		Cyberinsurance products			p-value (x2 test)
		None (%)	Basic (%)	Premium (%)	
Buying protection measures	No	10.03	56.70	33.27	0.001**
	Yes	5.76	58.02	36.22	
Buying cyberinsurance products	No	9.06	57.52	33.42	0.000***
	Yes	4.09	56.85	39.06	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 37. Cyberinsurance measures purchases by buying expertise.



D6.3: Report with Findings of Experiments and Policy implications

Figure 30. Cyberinsurance purchases by buying expertise.

In summary, participants with buying experience of product related to cybersecurity are more prone to increase their coverage level, purchasing more insurance products and selected the highest coverage and prime. This effect is more intense for these subjects that already bought cyberinsurance for their SMEs.

3.3.3 Cybersecurity strategy

This section analyses the impact of the different design of the output interactive page of CYBECO toolbox in the adoption of the cybersecurity strategy as a whole. As shown in Table 38, although 48.8% of the subjects selected the first option in the ranking (ASMs + Basic insurance), one third of the participants opted for the second option (ASMs + Premium insurance) that offered the same protection by higher coverage level.

It must also be highlighted that, although the use of the tool increases the purchases of the recommended option, protection and insurance are again complementary and not substitutive goods for the participants. In this sense, only 2.79% of the subjects selected high protection and no insurance and only 1.44% prefer to compensate a low protection level with a high coverage insurance policy.

Rank	Cybersecurity strategy	Purchases (%)
1	ASMs + Basic	44.75
2	ASMs + Premium	33.30
3	ASMs + None	2.79
4	SSMs + Premium	1.44
5	SSMs + Basic	12.61
-	SSMs + None	5.10

Table 38. Cybersecurity strategies.

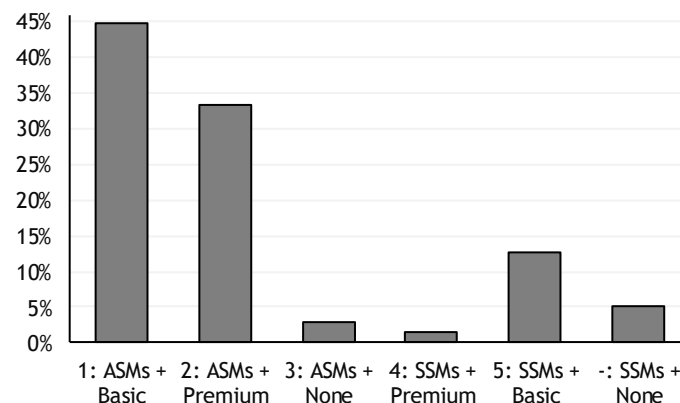


Figure 31. Cybersecurity strategies.

D6.3: Report with Findings of Experiments and Policy implications

The design of the output page of the toolbox has a significant impact on the selection of the cybersecurity strategy for the SME ($p\text{-value} = 0.000$). Firstly, as discussed for the individual components, the inclusion of a high salience message declaring that option 1 is the recommendation of the experts and a direct link to purchases highly increases the purchases of the first option (ASMs + Basic insurance).

Focusing in the other four more comparable treatments (Table 39) we can conclude that:

- Providing the user of CYBECO toolbox with the result of the cyber-risk analysis in terms of expected values instead of in terms of the values for the two alternative scenarios of suffering or not the cyberattack increases the purchases of the first option in the ranking. This result can be observed in both the framing in losses (treatment 1 versus treatment 4) and in gains (treatment 3 versus treatment 5).
- Framing the results of the cyber-risk analysis in terms of losses increases the purchases of the first option in the ranking when the information is provided in expected values (treatment 1 versus treatment 3) and separately for both scenarios (treatment 4 versus treatment 5).

Treatment		Cybersecurity strategies (%) ordered according to the rank					
ID	Conditions	1: ASMs + Basic	2: ASMs + Premium	3: ASMs + None	4: SSMs + Premium	5: SSMs + Basic	-: SSMs + None
1	Expected - Losses	42.79	34.72	3.42	1.22	13.20	4.65
2	Expected - Losses - Salience	68.88	16.39	1.43	0.48	9.26	3.56
3	Expected - Gains	39.47	37.08	3.11	1.91	12.68	5.74
4	Scenarios - Losses	39.00	37.80	2.87	1.20	13.40	5.74
5	Scenarios - Gains	33.25	40.78	3.16	2.43	14.56	5.83

Table 39. Cybersecurity strategies by treatment.

D6.3: Report with Findings of Experiments and Policy implications

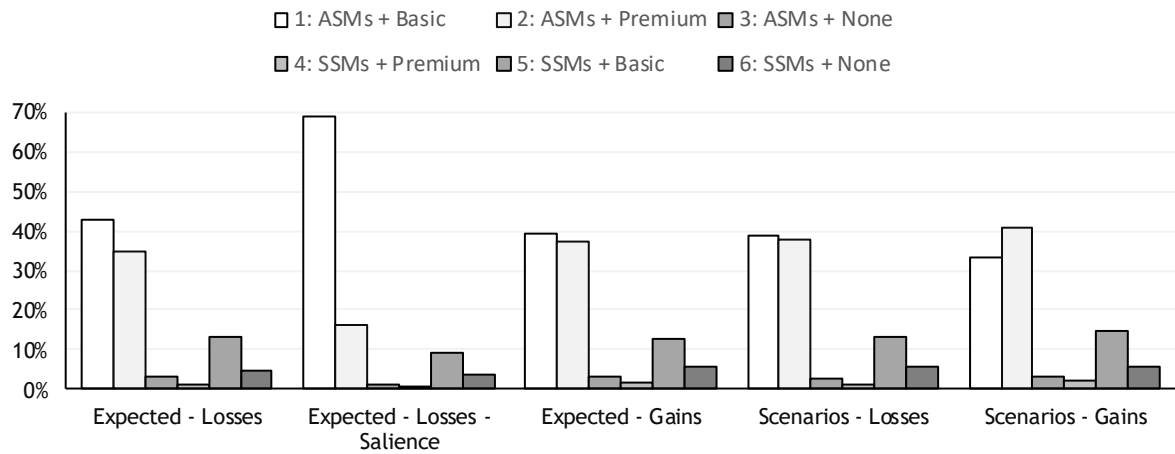


Figure 32. Cybersecurity strategies by treatment.

3.3.3.1 Expertise of the potential user

As discussed in the two previous subsections, the expertise of the subject plays a relevant role on how the use and follow the suggestion of CYBECO toolbox. As presented in Table 40, subjects with experience are less prone to follow the suggestion of the tool and opt for a security strategy that is not the first in the ranking (specifically, to increase the coverage of the insurance, as shown in Table 38). This effect is especially relevant for subjects with expertise in cybersecurity, choosing the first option under treatment 17.0 percentual point less than the whole sample.

The differences between the behaviour of experts in cybersecurity (and in purchases, to lesser extend) and the whole sample does also depend on the design of the output page. Assuming that experts in cybersecurity have the best understanding on designing cybersecurity strategies, we can consider them as a benchmarking. Under this assumption, the closer the behaviour of all the sample is to the behaviour of these expert, we can consider that CYBECO tool is presented the information of the risk analysis in a better way to nudge the decisions of all the potential users of the tool towards their optimal cybersecurity strategy. According to this reasoning, Table 40 shows that presenting values per scenario nudge better cybersecurity strategies than presenting them as expected values. On the other hand, framing the information as losses does also reduce the difference between cyberinsurance experts and the whole sample, and could be considered as a more appropriate framing for CYBECO tool.

Treatment		Purchases of the recommended option (%)				
Conditions		Use IT systems - All subjects	Management position - All subjects	Responsibility for purchasing - All subjects	Cybersecurity role - All subjects	All subjects
1	Expected - Losses	1.29	0.72	-5.39	-16.98	42.79

D6.3: Report with Findings of Experiments and Policy implications

2	Expected - Losses - Salience	0.23	3.09	-1.49	-11.13	68.88
3	Expected - Gains	2.3	-0.16	1.51	-12.2	39.47
4	Scenarios - Losses	3.13	-1.59	0.83	-0.4	39.00
5	Scenarios - Gains	-3.29	-1.11	-8.25	-9.11	33.25

Table 40. Differences in the purchases of the recommended option (%) by treatment and field of expertise.

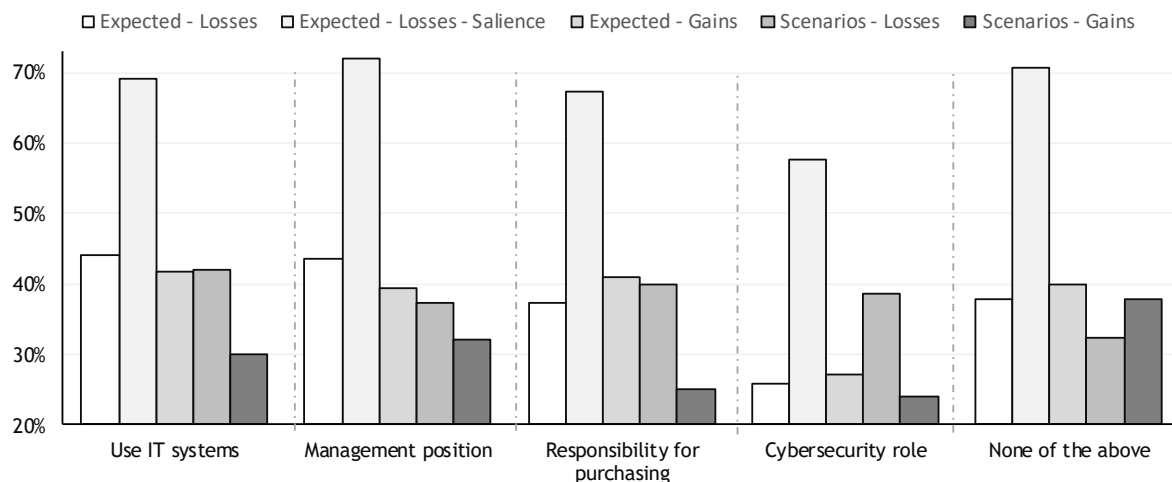


Figure 33. Purchases of the recommended option (%) by participants with experience

3.4 Impact of the output design in the usability of CYBECO toolbox

This section presents the results of the analysis of the impact of the design of the output screen on the usability of the toolbox. Since interactivity is one of the main features of CYBECO toolbox, section 3.4.1 analyses the impact of the different design to nudge towards an active use of the tool. Finally, section 3.4.2 presents some conclusions on the usability and understandability of the toolbox.

3.4.1 Interaction with CYBECO toolbox

When users land in the output page they observe a ranking of options from best to worse in terms of the results of the cyber-risk analysis, as presented in

Figure 34. This ranking presents basic information of each option depending on the treatment, in particular the gains and losses in expected terms or per each scenario.

D6.3: Report with Findings of Experiments and Policy implications

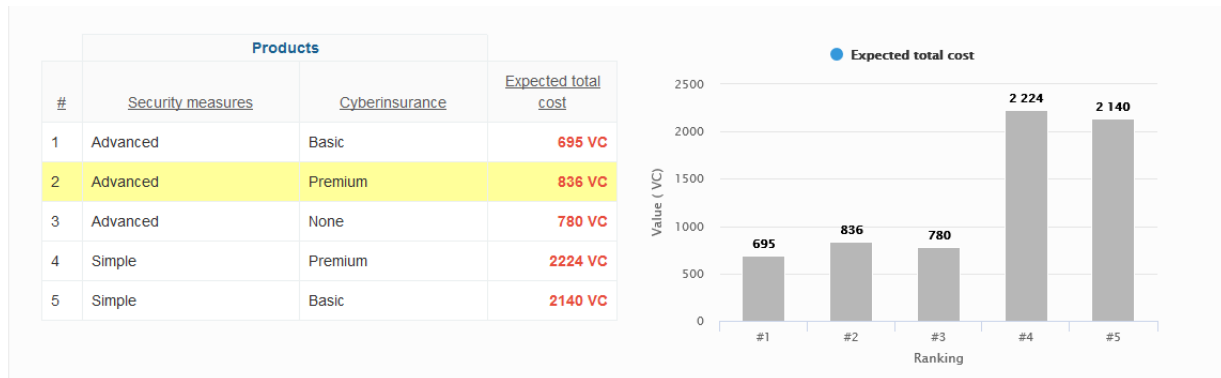


Figure 34. Ranking of options as presented in the output page (Treatment 1).

Using the tool, and before decision-making, subjects can interact with the tool to obtain more detailed information on the individual components of the costs (losses) or income (gains) computed by the tool, as presented in Figure 35.

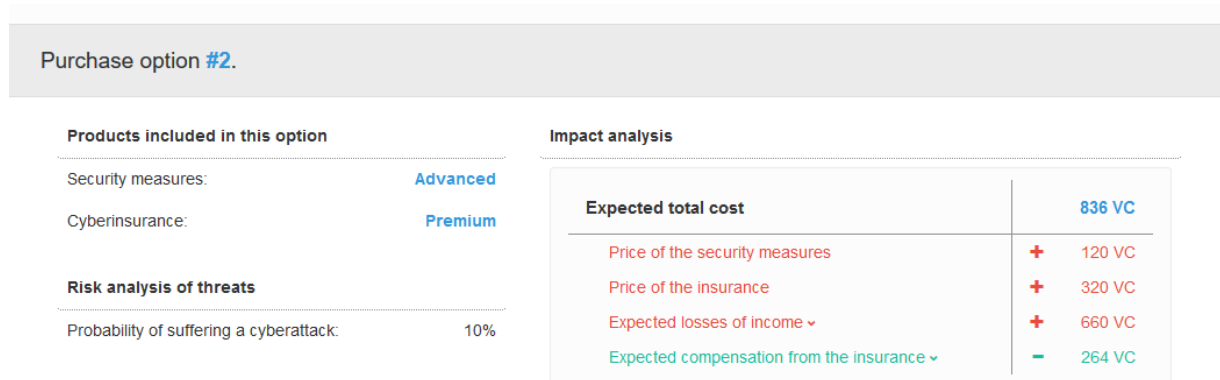


Figure 35. Detailed information of each option as presented in the output page (Treatment 1).

The number of options consulted by the participant varies significantly in terms of the treatment (p -value = 0.000). Table 41 shows that subjects looked in average at 1.4 options in treatment 2. The inclusion of the salient recommendation message and the direct purchase click make participants to skip detailed information and moving for the default option, even without consulting the detailed meaning of the total expected cost for any option (Figure 36). The average number of options checked in the treatments with values per scenario (treatments 4 and 5) are 2.0 and 1.7, respectively. Finally, the presentation of expected values increases the number of options visualised by the subjects, achieving an average of 2.2 options in treatment 3 and 2.8 option in treatment 1.

D6.3: Report with Findings of Experiments and Policy implications

ID	Condition	n	Mean	SD	Min-Max
1	Expected - Losses	409	2.822	3.246	1-29
2	Expected - Losses - Saliency	421	1.411	2.321	0-21
3	Expected - Gains	418	2.237	2.498	1-18
4	Scenarios - Losses	418	1.988	1.961	1-13
5	Scenarios - Gains	412	1.731	1.484	1-10

Table 41. Number of options displayed by treatment.

The reduced number of options displayed by subjects supports that they decide the cybersecurity strategy from the summarised information in the ranking table and graph (

Figure 34) and just display the detailed information to understand the exact meaning of the information in the ranking table and how it is obtained as a result of the cyber-risk analysis performed by the tool. This interpretation is supported by the fact that the number of options displayed is larger when the information is more complex (expected values) and smaller in the simpler cases of information per scenarios and, specially, in the case of the recommendation message of treatment 2.

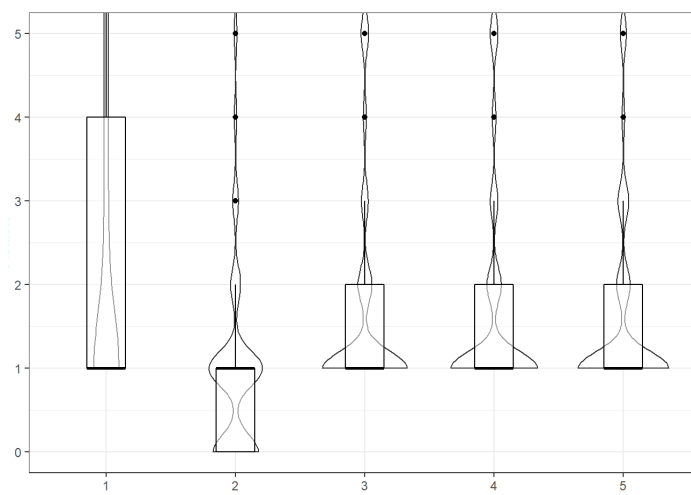


Figure 36. Number of displayed options by treatment.

Treatments do also affect the purchase options displayed by the subjects. Although the most frequently checked options are the first and second in the raking, the interaction pattern depends on the presentation of the results of the analysis in terms of expected values or in terms of values per each scenario. In the former case (Table 42) the most displayed option

D6.3: Report with Findings of Experiments and Policy implications

is the first in the ranking (ASMs + Basic insurance), meanwhile in the latter is the second purchase option (ASMs + Premium insurance).

<i>Treatment</i>		<i>Ranked options displayed by participants (%)</i>				
ID	Conditions	1: ASMs + Basic	2: ASMs + Premium	3: ASMs + None	4: SSMS + Premium	5: SSMS + Basic
1	Expected - Losses	52.81	55.75	36.19	22.33	27.14
2	Expected - Losses - Saliency	34.68	29.69	18.76	13.54	10.93
3	Expected - Gains	49.04	47.85	31.10	28.95	19.86
4	Scenarios - Losses	42.11	52.15	28.95	24.64	20.10
5	Scenarios - Gains	36.17	48.54	24.27	23.54	22.33
<i>p-value (x2 test)</i>		0.000**	0.000**	0.000**	0.000**	0.000**

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 42. Option displayed by treatment.

Table 43 and Figure 37 do also support the interpretation of interactive display as a tool to understand the results of the cyber-risk analysis presented in the ranking, since around half of the participants do not display the detailed information of their selected cybersecurity strategy. The consultation of the details of the purchased option is significantly lower in the treatments providing results per scenario and in treatment 2.

<i>Treatment</i>		Subjects who displayed the purchased option (%)	<i>p-value (x2 test)</i>
ID	Conditions		
1	Expected - Losses	53.06	0.000***
2	Expected - Losses - Saliency	32.30	
3	Expected - Gains	53.35	
4	Scenarios - Losses	50.24	
5	Scenarios - Gains	50.49	

Table 43. Percentage of subjects displaying their purchased option.

D6.3: Report with Findings of Experiments and Policy implications

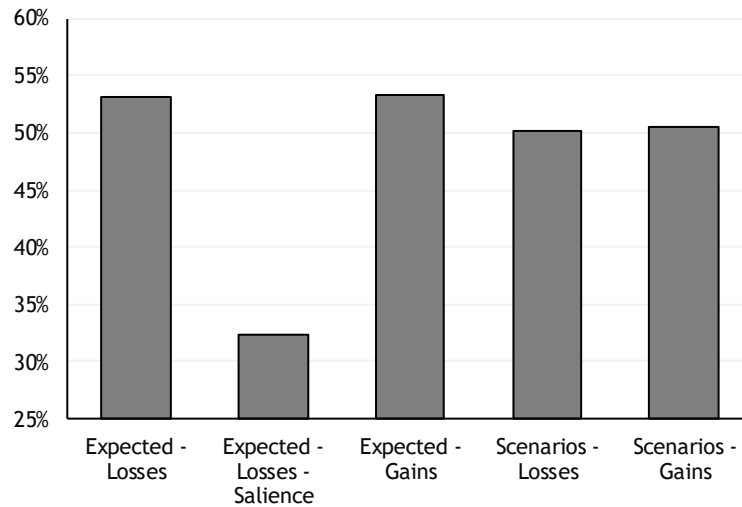


Figure 37. Percentage of subjects displaying their purchased option.

3.4.2 Usability of CYBECO toolbox

The first relevant question is how the participants used CYBECO toolbox to support their decision-making. Table 44 presents the criteria after subjects' election of their cybersecurity strategy. Only 7.0% made the decisions considering that the purchased option was the first in the ranking and 15.7% because it was the recommended by the experts (mostly in treatment 2, where this reason is significantly more important and is the decision lever for 26.4% of the participants). In other words, participants used the tool to get the results of the cyber-risk analysis and make their own decisions, more than as a guidance to follow experts' recommendations. When deviating from the recommendation, they tend to increase the coverage of the insurance, moving from the Basic to the Premium policy, without reducing their protection level.

	Total	Expected - Losses	Expected - Losses - Salience	Expected - Gains	Scenarios - Losses	Scenarios - Gains	p-value (x2 test)
It guaranteed the highest coverage in the case of an attack	38.83	39.61	36.10	39.71	36.84	41.99	0.408
It was the cheapest	23.72	24.69	21.38	23.68	22.97	25.97	0.596
It guaranteed the maximum protection against a cyberattack	49.77	52.08	52.08	49.76	48.56	46.36	0.165
It was the first in the ranking	6.98	7.09	8.55	6.70	5.50	7.04	0.547
It was the option recommended by the experts in cybersecurity	15.69	14.18	26.37	12.92	13.16	11.65	0.000***

D6.3: Report with Findings of Experiments and Policy implications

I selected an option at random	7.41	6.85	6.65	8.37	8.37	6.80	0.754
--------------------------------	------	------	------	------	------	------	-------

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 44. Reasons to purchase the selected cybersecurity strategy.

The only treatment with a significant capacity to nudge towards the recommended option is the inclusion of high silence messages and the inclusion of a direct purchase link (treatment 2). We can conclude that, although different framings of information can facilitate the understanding and use of the results of the CYBECO risk analysis, to nudge towards the recommended option more behavioural levers based in framing and choice architecture, such as salience, social norm or default options, are required.

Only 29.5% of the subjects remember to have purchased the recommended option (Table 45), this percentage reaching 40.1% in treatment 2.

	Did you buy the first option of the ranking?			p-value (x2 test)
	YES (%)	NO (%)	I DON'T KNOW (%)	
Total	29.50	57.17	13.33	0.000***
T1	28.36	58.68	12.96	
T2	40.14	44.42	15.44	
T3	27.99	60.53	11.48	
T4	23.44	61.72	14.83	
T5	27.43	60.68	11.89	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 45. Percentage of participants purchasing the first option in the ranking by treatment.

Only 14.7% of the subjects that did not follow the recommendation of the tool seem not to understand the ranking criterion or considered that there was no special criterion under the ranking (Table 46). The rest of the subjects opted for another option because they considered that the suggested one was not optimal in terms of coverage, protection or price.

	Total						p-value
		Expected - Losses	Expected - Losses - Salience	Expected - Gains	Scenarios - Losses	Scenarios - Gains	(x2 test)
Options were ranked with no special criterion	9.77	11.25	6.95	10.67	12.40	7.60	0.218
The first option was too expensive	20.13	18.33	21.93	20.16	19.77	20.40	0.927
The insurance in first option did not provide enough coverage	39.68	42.50	41.18	36.36	37.21	41.20	0.553
The protection measures in the first option were not safe enough	41.25	40.42	38.50	44.66	42.25	40.40	0.729
I do not understand the criterion of the ranking	4.95	5.00	4.81	2.37	6.20	6.40	0.236

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

D6.3: Report with Findings of Experiments and Policy implications

Table 46. Reasons not to purchase the first option in the ranking by treatment.

Participants rated the clarity and understandability of the terms and concepts used in the output of the CYBECI toolbox in a scale from 1 (Very unclear and difficult to understand) to 7 (Very clear and easy to understand). The average rating of this concept is 5.3. Figure 38 shows that the median understandability for treatments 1 and 4 framed in losses is 5, meanwhile that of treatments 3 and 5 framed in gains is 6. In other words, the framing as gains seems to be slightly easy to understand than the framing in gains.

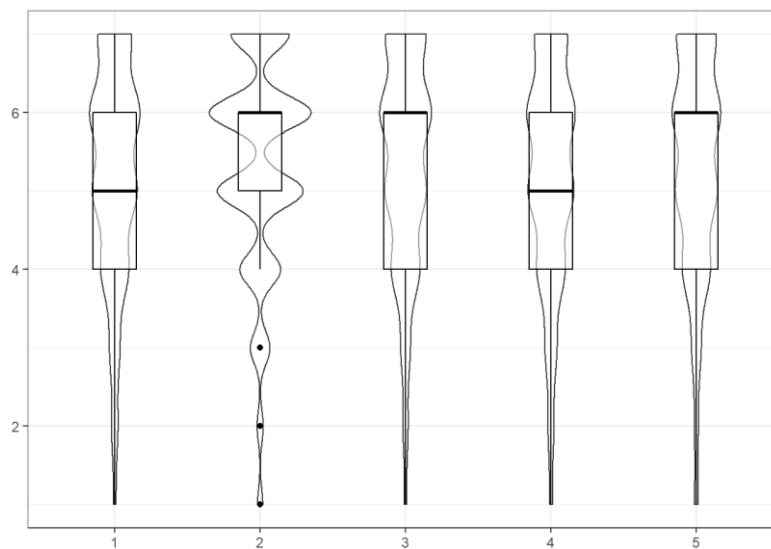


Figure 38. Clarity and understandability of the output by treatment (from 1 very unclear and difficult to understand to 7 very clear easy to understand)

In a scale from 1 to 100, participants rate how confident they are with the option they selected as 70.4. The average rate of the trust in the CYBECO toolbox actually suggesting the best option for the participants is 64.7. Table 47 and Table 48 show that there are no relevant differences in the confidence and trust ratings among the different treatments.

ID	Conditions	N	Mean	SD	Min-Max
1	Expected - Losses	409	69.367	25.249	0-100
2	Expected - Losses - Saliency	421	69.367	25.815	0-100
3	Expected - Gains	418	71.940	24.735	0-100
4	Scenarios - Losses	418	71.065	23.838	0-100
5	Scenarios - Gains	412	70.090	25.950	0-100

Table 47. How confident are you in the option you have chosen? (scale 1 to 100)

ID	Conditions	N	Mean	SD	Min-Max
1	Expected - Losses	409	63.672	24.041	0-100
2	Expected - Losses - Saliency	421	64.029	24.215	0-100

D6.3: Report with Findings of Experiments and Policy implications

3	Expected - Gains	418	66.722	23.569	0-100
4	Scenarios - Losses	418	64.007	25.006	0-100
5	Scenarios - Gains	412	65.170	26.426	0-100

Table 48. How much do you trust that the toolbox will suggest the best option for you? (scale 1 to 100)

It should be highlighted that participants consider in general that the output page of CYBECO toolbox is easy to use (with a rate of 5.4 in scale from 1 to 7) and meets users' requirements (with a rate of 5.2 in the same scale). The analysis does not show significant differences of these two rates among the different treatments.

Finally, as shown in

	Expected - Losses	Expected - Losses - Salience	Expected - Gains	Scenarios - Losses	Scenarios - Gains	p-value (x2 test)
Not all likely	2.93	3.09	1.67	3.11	3.40	0.960
Not likely	3.67	3.33	3.11	2.39	3.16	
Moderately not likely	3.91	4.04	2.63	3.35	4.13	
Indifferent	19.80	17.34	19.14	19.14	19.17	
Moderately likely	26.16	26.13	26.79	29.67	25.97	
Likely	26.65	29.69	28.47	27.03	24.27	
Highly likely	16.87	16.39	18.18	15.31	19.90	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 49, 71.5% of the participants consider that they will use this toolbox in the future, once the CYBECO toolbox will be available (aggregation of the users moderately likely, likely or highly likely the future use of the tool). Again, there are no significant differences in the intention of use by treatment.

	Expected - Losses	Expected - Losses - Salience	Expected - Gains	Scenarios - Losses	Scenarios - Gains	p-value (x2 test)
Not all likely	2.93	3.09	1.67	3.11	3.40	0.960
Not likely	3.67	3.33	3.11	2.39	3.16	
Moderately not likely	3.91	4.04	2.63	3.35	4.13	
Indifferent	19.80	17.34	19.14	19.14	19.17	
Moderately likely	26.16	26.13	26.79	29.67	25.97	
Likely	26.65	29.69	28.47	27.03	24.27	
Highly likely	16.87	16.39	18.18	15.31	19.90	

* p-value < 0.1; ** p-value < 0.05; *** p-value < 0.001

Table 49. Intention to use the CYBECO toolbox by treatment.

D6.3: Report with Findings of Experiments and Policy implications

4 Conclusions and policy implications

Sections 2 and 3 presented the main results of the two behavioural economic experiments designed and implemented within the CYBECO project. Experiment 1, run with a sample of 4,800 users in four EU countries, focus in the CYBECO model and provided behavioural insights on how subjects make the decision of the cybersecurity strategy to be implemented. Experiment 2 analyses the CYBECO toolbox, specifically, the implications of five alternative designs of its interactive output page on cyberinsurance decision-making. This second experiment has been run with a sample of participants that are potential users of the tool: all subjects were working in SMEs in areas related to the topic of CYBECO and any of them do also have previous experience in the purchase of protection and insurance products for their SMEs. This section presents briefly the main implications of the results of these two related experiments

4.1 Behavioural insights of cyberinsurance: implications for market development

Both experiment show that citizens - from general users of the Internet and e-commerce to experts in cybersecurity - are in general aware of the importance of cybersecurity breaches and are prone to invest in cyberprotection and cyberinsurance. The purchase level of protection measures and insurance policies is very high, when they are made available in both economic experiments. However, the experiments also reveal the existence of a segment of subjects that are not concerned at all for cybersecurity issues.

The profile of the subject influences her or his cybersecurity strategy. In particular, women and elder users are in general more prone to acquire protection and insurance, as consequence of their higher risk aversion. The level of safety of online behaviour is not influenced by the sex but for the age of the users. Older users, despite their higher risk aversion, exhibit a riskier online behaviour. An explanation for this fact could be that this segments of users are not aware of the security implications of some of the decisions made when navigating, such as the consequence of sharing private information or log out of a page. This fact highlights the importance of programs and policies focused on how to improve the safety of online behaviour for some special collectives (such as elder citizens), specially when the use of sensitive online services (such is e-banking) is becoming more and more common.

The experiments allows for analysing two behavioural issues that are critical in cyberinsurance: the substitution relation between cyberprotection and cyberinsurance and the potential existence of moral hazard among takers of cyberinsurance policies. The former question is related to analyse if subjects perceive both protection and insurance as substitutive (can insurance replace protection?) or complementary (do insurance and

D6.3: Report with Findings of Experiments and Policy implications

protection work well together?) goods. The latter is related to check if subjects behave in a less secure when they are covered by an insurance policy. These two questions are critical for the development of a cyberinsurance market in the EU: if insurance were actually perceived as a substitute of cyberprotection or fostered less secure online behaviour, the development of the cyberinsurance market would become critical for the security of the single digital market. Experiment 1 shows that:

- Subjects who bought advance protection are more prone to purchase premium insurance whereas the majority of subjects who bought basic protection decide to purchase also basic insurance. In other words, insurance does not substitute protection, but both type of products are purchased by the participants who are more sensitive to cybersecurity.
- There are no significant differences in the risk taken by those subjects with no insurances or those with a basic or premium insurance policy. However, subjects behave in a significantly less safe way if they have not acquired advance protection.

The experiments do also provide insights in how subjects create and updates their beliefs after receiving a cyberattack. In general, the experience of the cyberattack nudges people to change the protection and insurance strategy to a higher extend than the experience of not suffering it. The experience of the cyberattack can change the subject's beliefs in two opposite directions. In some cases, the attack increases the awareness of the risk, making subjects to increase their protection and insurance levels. However, in other cases, the experience of the cyberattack reduced their trust in the efficacy of advance protection.

4.2 The CYBECO model

The results of both experiments are coherent with the assumptions of the CYBECO model and of the Protection Motivation theory (PMT) used as framework for the design of the experimental conditions.

CYBECO model is based in an adversarial approach of risk analysis, which considers the different nature of random and intentional threats. Experiment 1 shows that subjects do actually react in a different way to a cyberattack if they consider it to be intentional or just random, even if the probability to suffer the attack is the same. In general, subjects react more intensely to an intentional risk, increasing both their levels of protection and insurance. The need of distinguishing between these two types of cyberthreats, as included in the model, is supported by the behavioural experimental analysis.

D6.3: Report with Findings of Experiments and Policy implications

A set of questionnaires were administered that captured a range of subjective measures aligned to the constructs described in protection motivation theory. These assessed the perceived risk of an attack in terms of severity and vulnerability, the participant's response efficacy, perceived behavioural control and response cost. In addition, a set of questions addressed attitudes to cyberinsurance and also risk propensity (using the DOSPERT scale). The result of the first experiment show that each of these, with the only exception of perceived vulnerability⁴, is predictive of security behaviour.

4.3 Usability of the CYBECO toolbox

The results of the usability test of the interactive output page of the CYBECO toolbox have been positive. In a scale from 0 (worst rate) to 10 (best rate), the participants in the second experiment rated the facility of use and the clarity and understandability of CYBECO toolbox with marks higher than 7.5. Moreover, more than two thirds of the participants declared that they will likely use it in the future, once the CYBECO toolbox will be available. There are no significant differences in these ratings in term of the design of the output page.

Users interact with the output page to check the detailed results of the cyber-risk analysis for around two different cybersecurity strategies (mainly, the first and the second in the ranking). They seem to do this exercise to understand the meaning of the information presented in the ranking table and how these values are computed by the tool. After checking that, they make their decision from the information in the ranking table and its visual representation in the companion bar chart.

The presentation of the results of the cyber-risk analysis of the available cybersecurity strategies through CYBECO toolbox plays a twofold role. Firstly, the information should help users to evaluate the different protection and cyberinsurance options to choose the best option for an SME, given its main characteristics and the risk attitude of the decision maker. Secondly, the tool should also nudge the user to choose the option identified as the most appropriate for the SME according to the CYBECO model. Notice that, to recommend a cybersecurity strategy, the model can be fed with the objective characteristics of the SME introduced by the input interface of the toolbox but cannot take into account the utility function nor the risk attitude of the decision maker.

⁴ Perceived vulnerability refers to the extent to which an individual feels that it is likely that they will be made a target of an attack. It is possible that we are not seeing an effect on this variable because participants are 'unrealistically optimistic' about the extent to which they will be targeted in an attack

D6.3: Report with Findings of Experiments and Policy implications

Experiment 2 shows that the potential users of CYBECO toolbox tend to use it more as an information source to make this decision than an expert tool able to guide them to the best option and as a source of recommendation (only 30% of the users declared to have purchased the strategy recommended by the tool). It must be highlighted that the recommendation is not followed by a lack of understanding of the ranking criteria but for the fact that users do consciously prefer a different protection, coverage or price level than that in the recommendation of the toolbox.

4.4 Optimal design of the output page

The second economic experiment provided information to optimise the presentation of the results of the risk analysis in the CYBECO toolbox. Specifically, these results were presented to the subjects in five different designs.

One of these five designs is very different to the other, since it adds to the results of the analysis a high salience message stressing that the first option in the ranking is the recommendation of cybersecurity experts and facilitates its purchase through a direct purchase link. The behavioural levers in this design (default option, salience, etc.) are capable to influence user behaviour and increases significantly the adoption of the recommended option. The inclusion of this type of messages could be a good option in this cases that it is desirable to enhance the *normative* features of the toolbox and nudge users towards the recommended option, such us small SMEs or users with no experience in the field.

The other four designs are come from the combination on two criteria to presents the results of the risk analysis. Firstly, information can be framed as losses (prices of protection and insurance products, losses in the commercial value of the data and the potential compensation of the insurance policy taken by the subjects) or gains (income). Secondly, the results of applying each strategy can be presented as expected values (product of the probability of suffering or not the attack and the results of the strategy in each case) or with the values per scenario. Notice that presenting the results per scenario provides the user with all the information required to determine is optimal cybersecurity strategy in terms of her or his utility function and risk attitude.

The results of the experiment shows that, although these four design have similar rates of following of the recommended option, they nudge toward different types of deviation. Framing the results in losses and providing the information as expected values increases the level of protection and the coverage of the insurance in the cybersecurity strategies selected by the users.

The differences between the behaviour of experts in cybersecurity and the whole sample of users does also depend on the design of the output page. Assuming that experts in cybersecurity have the best understanding on designing cybersecurity strategies, we can

D6.3: Report with Findings of Experiments and Policy implications

consider them as a benchmark. Under this assumption, the closer the behaviour of all the sample is to the behaviour of these experts, the better. We can then ask which formulations of the CYBECO tool are most effective in nudging towards this optimal cybersecurity strategy. According to this reasoning, the results of experiment 2 shows that presenting values by losses and by scenario are most effective in nudging the whole sample to behave as cybersecurity experts do and this could then be considered as an appropriate framing for CYBECO tool.

D6.3: Report with Findings of Experiments and Policy implications

CYBECO

Supporting Cyberinsurance from a Behavioural Choice Perspective

ANNEXES - D6.3: Report with Findings of Experiments and Policy implications

Due date: 31/10/2018

Abstract:

This document corresponds to Deliverable 6.3 and presents the results and implications of the two online economic experiments designed and implemented within the scope of the CYBECO project. The first experiment 1, run with a sample of 4,800 subjects in four countries, analysed the 'human actual behaviour' when purchasing cyber protection and insurance. The second experiment was focused in testing and improving the CYBECO toolbox. Run with a sample of 2,000 potential users of the tool, this second experiment tested the usability of the toolbox and established the behavioural implications of five different designs of the interactive risk analysis dashboard of the CYBECO toolbox.

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)	

D6.3: Report with Findings of Experiments and Policy implications

Document Status

Document Title	Report with Findings of Experiments and Policy implications
Version	0.1
Work Package	6
Deliverable #	6.3
Prepared by	DevStat
Contributors	DevStat and Northumbria.
Checked by	IC-MAT and Intrasoft
Approved by	
Date	31/10/2018
Confidentiality	PU

D6.3: Report with Findings of Experiments and Policy implications

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	0.1	October 31, 2018

D6.3: Report with Findings of Experiments and Policy implications

Table of Contents

1	Screenshots.....	7
1.1	Experiment 1	7
1.2	Experiment 2	25
2	Questionnaires	40
2.1	Experiment 1: Sociodemographic questionnaire	40
2.2	Experiment 2: Sociodemographic questionnaire	40
2.3	Experiment 2: Usability questionnaire.....	42
2.4	Experiment 1 & 2: Final questionnaire	45

D6.3: Report with Findings of Experiments and Policy implications

List of Figures

Figure 1. Welcome page	7
Figure 2. Socio-demographic questionnaire	8
Figure 3. Stage 1 and 2 instructions when the context is random, Factor C1	9
Figure 4. Stage 1 and 2 instructions when the context is intentional, Factor C2.	10
Figure 5. Cibersecurity shop when there are not price dependency and the prices of insurance are medium, Factor P1 and I1.	11
Figure 6. Cibersecurity shop when there are price dependency and the prices of insurance are medium, Factor P2 and I1.	12
Figure 7. Cibersecurity shop when there are not price dependency and the prices of insurance are asymmetric, Factor P1 and I2.	13
Figure 8. Cibersecurity shop when there are price dependency and the prices of insurance are asymmetric, Factor P2 and I2.	14
Figure 9. Cibersecurity shop when there are not price dependency and the prices of insurance are high, Factor P1 and I3.	15
Figure 10. Cibersecurity shop when there are price dependency and the prices of insurance are high, Factor P2 and I3.	16
Figure 11. Purchase summary.....	17
Figure 12. Event website.	18
Figure 13. Event registration.....	19
Figure 14. Event website - Logout.	20
Figure 15. Cyberattack simulation.	21
Figure 16. Access to Stage 2	21
Figure 17. Stage 3: Holt & Laury	22
Figure 18. Stage 3 results.....	22
Figure 19. Final questionnaire	23
Figure 20. End page	24
Figure 21. Welcome page.....	25
Figure 22. Socio-demographic questionnaire	26
Figure 23. Stage 1 instructions	27
Figure 24. Risk analysis tool explanation.....	28
Figure 25. Treatment 1 - Risk analysis tool	29
Figure 26. Treatment 2 - Risk analysis tool	30
Figure 27. Treatment 3 - Risk analysis tool	31
Figure 28. Treatment 4 - Risk analysis tool	32
Figure 29. Treatment 5 - Risk analysis tool	33
Figure 30. Cybersecurity shop	34
Figure 31. Cyberattack simulation	35
Figure 32. Usability questionnaire	36
Figure 33. Stage 2: Holt & Laury	37



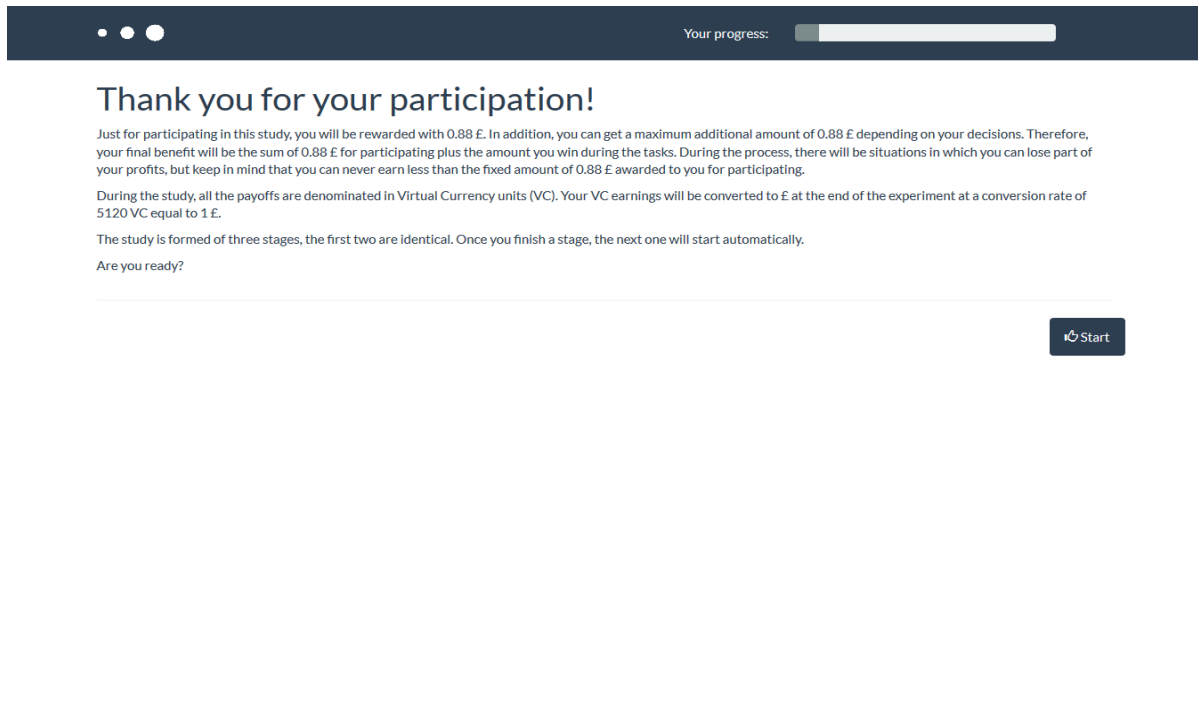
D6.3: Report with Findings of Experiments and Policy implications

Figure 34. Stage 2 results.....	37
Figure 35. Final questionnaire	38
Figure 36. End page	39

D6.3: Report with Findings of Experiments and Policy implications

1 Screenshots

1.1 Experiment 1



© DevStat 2018

Figure 1. Welcome page

D6.3: Report with Findings of Experiments and Policy implications

Your progress:

Before enjoying the experience, we would like to know more about you

1. What is the highest level of education you have completed?

☐ 0-11 years of education

☐ 12 years of education (high school diploma)

☐ Some years of university (not completed)

☐ University degree (BA, BS)

☐ Post-graduate degree (MA, MS, JD, MD, PhD, etc)

2. Employment situation

☐ Self-employed

☐ Public/Private worker

☐ Unemployed

☐ Housewife/Househusband

☐ Student

☐ Retired

☐ Other (rent perceiver, public or private aid)

Continue

Figure 2. Socio-demographic questionnaire

D6.3: Report with Findings of Experiments and Policy implications

• • •

Your progress:

Stage 1

You are the cybersecurity manager of a small business, called CYBECORP. You are aware that **there is a computer virus going around the Internet, that may affect your company**. You know that 40% of companies like yours have suffered this virus attack in the last week.


We will now ask you to make some decisions that will affect the cybersecurity of CYBECORP.

Read the following instructions in detail and press "Continue" when you are ready.


Note: You do not need to have any knowledge about computer systems or cybersecurity for complete the study. There are no right or wrong answers please just answer honestly. Whatever the result, you are guaranteed a minimum of the fixed participation rate at the end of the study.

1. Initial State


Your initial state is the following:



The profit that CYBECORP obtains from its commercial data is 1400 VC



You have a budget of 650 VC to buy security measures



The probability that CYBECORP is randomly affected by the virus is 40%

2. Purchase of security measures

At the beginning of the stage, you will have the opportunity to spend your budget on an advanced security measure and/or insurance against cyberattacks.


3. Registration for a conference

You will then be asked to register CYBECORP for a conference and asked to complete the online registration form (you will have an employee card at the registration page with all the necessary information). As in real life, the probability of CYBECORP suffering a cyberattack may increase depending on your way of surfing the Internet.

4. Results


Once you have registered for the conference, CYBECORP may suffer a cyberattack (the probability of which is affected by your decisions) and you will be presented with your resulting payoff. There are two possible scenarios:

1)



CYBECORP does not suffer any cyberattack and maintains the profit obtained from its commercial data. Therefore, your payout will be 1400 VC of the CYBECORP profit plus what you have left of your budget.

2)



CYBECORP suffers a cyberattack and loses all of the profit obtained from its commercial data. Therefore, your payout will be what you have left of your budget plus the amount you have insured (if you chose to buy insurance).

Continue

Figure 3. Stage 1 and 2 instructions when the context is random, Factor C1

D6.3: Report with Findings of Experiments and Policy implications



Stage 1

You are the cybersecurity manager of a small business, called CYBECORP. You are aware that a **cybercriminal might deliberately target your company**. You know that 40% of companies like yours have suffered a similar attack in the last week.

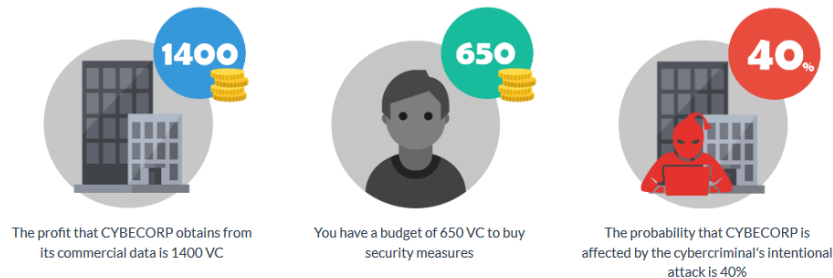
We will now ask you to make some decisions that will affect the cybersecurity of CYBECORP.

Read the following instructions in detail and press "Continue" when you are ready.

Note: You do not need to have any knowledge about computer systems or cybersecurity for complete the study. There are no right or wrong answers please just answer honestly. Whatever the result, you are guaranteed a minimum of the fixed participation rate at the end of the study.

1. Initial State

Your initial state is the following:



2. Purchase of security measures

At the beginning of the stage, you will have the opportunity to spend your budget on an advanced security measure and/or insurance against cyberattacks.

3. Registration for a conference

You will then be asked to register CYBECORP for a conference and asked to complete the online registration form (you will have an employee card at the registration page with all the necessary information). As in real life, the probability of CYBECORP suffering a cyberattack may increase depending on your way of surfing the Internet.

4. Results

Once you have registered for the conference, CYBECORP may suffer a cyberattack (the probability of which is affected by your decisions) and you will be presented with your resulting payoff. There are two possible scenarios:

1)



CYBECORP does not suffer any cyberattack and maintains the profit obtained from its commercial data. Therefore, your payout will be 1400 VC of the CYBECORP profit plus what you have left of your budget.

2)



CYBECORP suffers a cyberattack and loses all of the profit obtained from its commercial data. Therefore, your payout will be what you have left of your budget plus the amount you have insured (if you chose to buy insurance).

Continue

Figure 4. Stage 1 and 2 instructions when the context is intentional, Factor C2.

D6.3: Report with Findings of Experiments and Policy implications

Your progress:


Cybersecurity shop

Welcome to our Cybersecurity shop! Below, we present the security measures you can buy for CYBECORP. Select the measures you want to buy and press "Continue". Remember that you have a budget of 650 VC and keep in mind that once you press "Continue" you will not be able to go back. You can reread the instructions at any point by pressing the "Instructions" button on the top right.

Security Measures

Security measures are computer softwares used to prevent, detect and remove malicious software:


Basic security measures



Basic security measures costs 0 VC and the initial probability of suffering the attack is 40%

Cost	0 VC
Attack probability	40%

Advanced security measures



Advanced security measures costs 314 VC and the initial probability of suffering the attack is 20%

Cost	314 VC
Attack probability	20%

Which one do you want to buy?


Basic security measures

Advanced security measures

Cyberinsurance

Cyberinsurance is an insurance product used to protect businesses from Internet-based risks. We offer you three options with different level of coverage:


No insurance



Opting for no insurance costs 0 VC and covers 0 VC of lost profits in case of attack

Cost	0 VC
Coverage	0 VC


Basic insurance



The "Basic insurance" costs 140 VC and covers 350 VC of lost profits in case of attack

Cost	140 VC
Coverage	350 VC

Premium insurance



The "Premium insurance" costs 280 VC and covers 700 VC of lost profits in case of attack

Cost	280 VC
Coverage	700 VC

Which one do you want to buy?

No insurance

Basic insurance

Premium insurance

Continue

Figure 5. Cibersecurity shop when there are not price dependency and the prices of insurance are medium, Factor P1 and I1.

Figure 6. Cibersecurity shop when there are price dependency and the prices of insurance are medium, Factor P2 and I1.

D6.3: Report with Findings of Experiments and Policy implications

Your progress:


Cybersecurity shop

Welcome to our Cybersecurity shop! Below, we present the security measures you can buy for CYBECORP. Select the measures you want to buy and press "Continue". Remember that you have a budget of 650 VC and keep in mind that once you press "Continue" you will not be able to go back. You can reread the instructions at any point by pressing the "Instructions" button on the top right.

Security Measures

Security measures are computer softwares used to prevent, detect and remove malicious software:


Basic security measures



Basic security measures costs 0 VC and the initial probability of suffering the attack is 40%

Cost	0 VC
Attack probability	40%

Advanced security measures



Advanced security measures costs 314 VC and the initial probability of suffering the attack is 20%

Cost	314 VC
Attack probability	20%

Which one do you want to buy?


Basic security measures

Advanced security measures

Cyberinsurance

Cyberinsurance is an insurance product used to protect businesses from Internet-based risks. We offer you three options with different level of coverage:


No insurance



Opting for no insurance costs 0 VC and covers 0 VC of lost profits in case of attack

Cost	0 VC
Coverage	0 VC


Basic insurance



The "Basic insurance" costs 140 VC and covers 350 VC of lost profits in case of attack

Cost	140 VC
Coverage	350 VC

Premium insurance



The "Premium insurance" costs 336 VC and covers 700 VC of lost profits in case of attack

Cost	336 VC
Coverage	700 VC

Which one do you want to buy?

No insurance

Basic insurance

Premium insurance

Continue

Figure 7. Cibersecurity shop when there are not price dependency and the prices of insurance are asymmetric, Factor P1 and I2.

D6.3: Report with Findings of Experiments and Policy implications

Your progress:

Cybersecurity shop

Welcome to our Cybersecurity shop! Below, we present the security measures you can buy for CYBECORP. Select the measures you want to buy and press "Continue". Remember that you have a budget of 650 VC and keep in mind that once you press "Continue" you will not be able to go back.

You can reread the instructions at any point by pressing the "Instructions" button on the top right.

Security Measures

Security measures are computer softwares used to prevent, detect and remove malicious software:

Basic security measures



Basic security measures costs 0 VC and the initial probability of suffering the attack is 40%

Cost	0 VC
Attack probability	40%

Advanced security measures



Advanced security measures costs 314 VC and the initial probability of suffering the attack is 20%

In addition, if you buy our Advanced security measures you will have a 50% discount on the purchase of the cyberinsurance.

Cost	314 VC
Attack probability	20%

Which one do you want to buy?

Basic security measures

Advanced security measures

Cyberinsurance

Cyberinsurance is an insurance product used to protect businesses from Internet-based risks. We offer you three options with different level of coverage:

No insurance



Opting for no insurance costs 0 VC and covers 0 VC of lost profits in case of attack

Cost	0 VC
Coverage	0 VC

Basic insurance



The "Basic insurance" costs ~~140 VC~~ 70 VC and covers 350 VC of lost profits in case of attack

Cost	140 VC 70 VC
Coverage	350 VC

Premium insurance



The "Premium insurance" costs ~~336 VC~~ 168 VC and covers 700 VC of lost profits in case of attack

Cost	336 VC 168 VC
Coverage	700 VC

Which one do you want to buy?

No insurance

Basic insurance

Premium insurance

Continue

Figure 8. Cibersecurity shop when there are price dependency and the prices of insurance are asymmetric, Factor P2 and I2.

D6.3: Report with Findings of Experiments and Policy implications

• • •
Your progress:
i

Cybersecurity shop

Welcome to our Cybersecurity shop! Below, we present the security measures you can buy for CYBECORP. Select the measures you want to buy and press "Continue". Remember that you have a budget of 650 VC and keep in mind that once you press "Continue" you will not be able to go back. You can reread the instructions at any point by pressing the "Instructions" button on the top right.

Security Measures

Security measures are computer softwares used to prevent, detect and remove malicious software:

Basic security measures



Basic security measures costs 0 VC and the initial probability of suffering the attack is 40%

Cost	0 VC
Attack probability	40%

Advanced security measures



Advanced security measures costs 314 VC and the initial probability of suffering the attack is 20%

Cost	314 VC
Attack probability	20%

Which one do you want to buy?

Basic security measures

Advanced security measures

Cyberinsurance

Cyberinsurance is an insurance product used to protect businesses from Internet-based risks. We offer you three options with different level of coverage:

No insurance



Opting for no insurance costs 0 VC and covers 0 VC of lost profits in case of attack

Cost	0 VC
Coverage	0 VC

Basic insurance



The "Basic insurance" costs 168 VC and covers 350 VC of lost profits in case of attack

Cost	168 VC
Coverage	350 VC

Premium insurance



The "Premium insurance" costs 336 VC and covers 700 VC of lost profits in case of attack

Cost	336 VC
Coverage	700 VC

Which one do you want to buy?

No insurance

Basic insurance

Premium insurance

Continue

Figure 9. Cibersecurity shop when there are not price dependency and the prices of insurance are high, Factor P1 and I3.

D6.3: Report with Findings of Experiments and Policy implications

Your progress:

Cybersecurity shop

Welcome to our Cybersecurity shop! Below, we present the security measures you can buy for CYBECORP. Select the measures you want to buy and press "Continue". Remember that you have a budget of 650 VC and keep in mind that once you press "Continue" you will not be able to go back.

You can reread the instructions at any point by pressing the "Instructions" button on the top right.

Security Measures

Security measures are computer softwares used to prevent, detect and remove malicious software:

Basic security measures

Basic security measures costs 0 VC and the initial probability of suffering the attack is 40%

Cost	0 VC
Attack probability	40%

Advanced security measures

Advanced security measures costs 314 VC and the initial probability of suffering the attach is 20%

In addition, if you buy our Advanced security measures you will have a 50% discount on the purchase of the cyberinsurance.

Cost	314 VC
Attack probability	20%

Which one do you want to buy?

Basic security measures

Advanced security measures

Cyberinsurance

Cyberinsurance is an insurance product used to protect businesses from Internet-based risks. We offer you three options with different level of coverage:

No insurance

Opting for no insurance costs 0 VC and covers 0 VC of lost profits in case of attack

Cost	0 VC
Coverage	0 VC

Basic insurance

The "Basic insurance" costs ~~168 VC~~ 84 VC and covers 350 VC of lost profits in case of attack

Cost	168 VC 84 VC
Coverage	350 VC

Premium insurance

The "Premium insurance" costs ~~336 VC~~ 168 VC and covers 700 VC of lost profits in case of attack

Cost	336 VC 168 VC
Coverage	700 VC

Which one do you want to buy?

No insurance

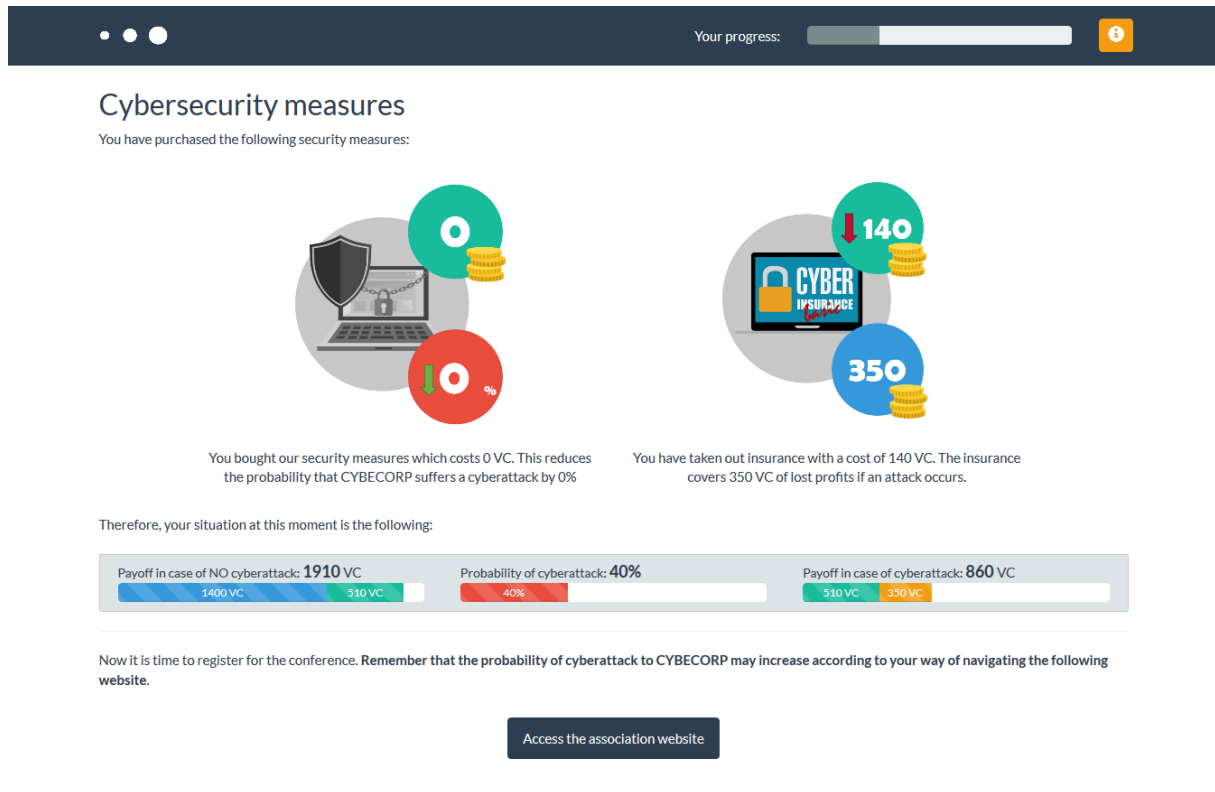
Basic insurance

Premium insurance

Continue

Figure 10. Cibersecurity shop when there are price dependency and the prices of insurance are high, Factor P2 and I3.

D6.3: Report with Findings of Experiments and Policy implications



© DevStat 2018

Figure 11. Purchase summary

D6.3: Report with Findings of Experiments and Policy implications

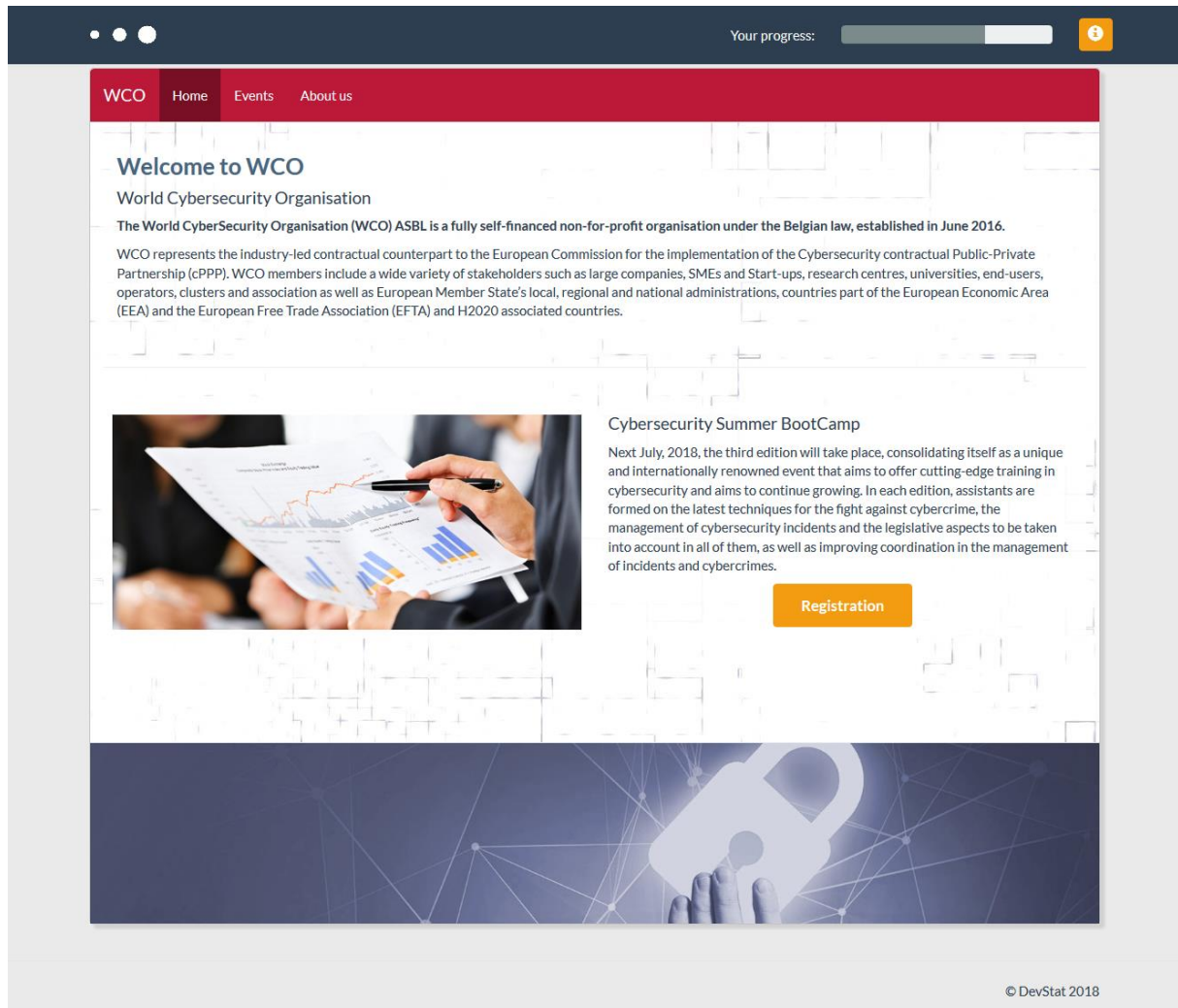
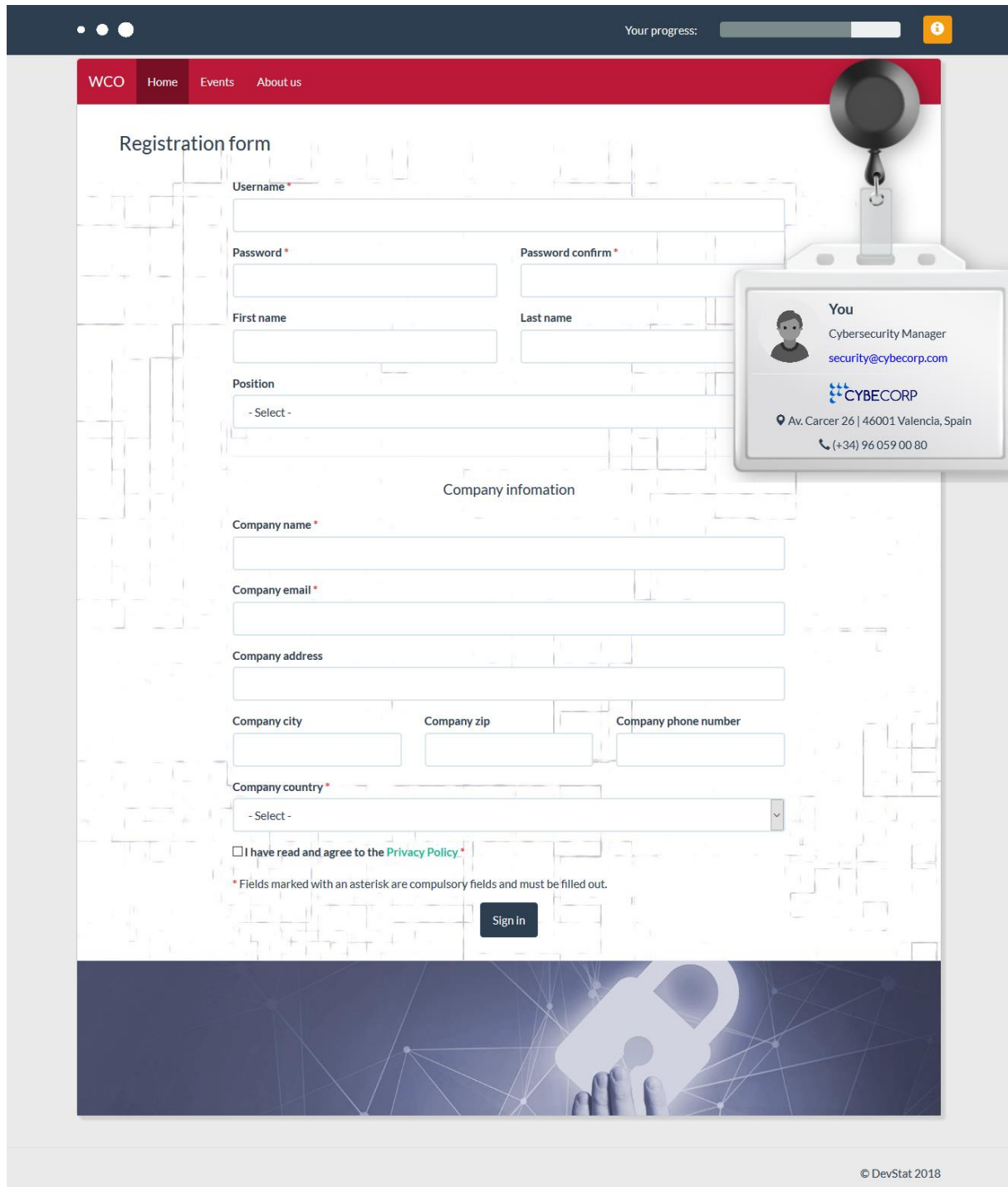
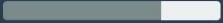


Figure 12. Event website.

D6.3: Report with Findings of Experiments and Policy implications



WCO Home Events About us

Your progress: 

Registration form

Username *

Password *

Password confirm *

First name

Last name

Position

- Select -

Company information

Company name *

Company email *

Company address

Company city

Company zip

Company phone number

Company country *

- Select -

☐ I have read and agree to the [Privacy Policy](#) *

* Fields marked with an asterisk are compulsory fields and must be filled out.

Sign in

You
Cybersecurity Manager
security@cybecorp.com
CYBECORP
Av. Carcer 26 | 46001 Valencia, Spain
(+34) 96 059 00 80

© DevStat 2018

Figure 13. Event registration.

D6.3: Report with Findings of Experiments and Policy implications

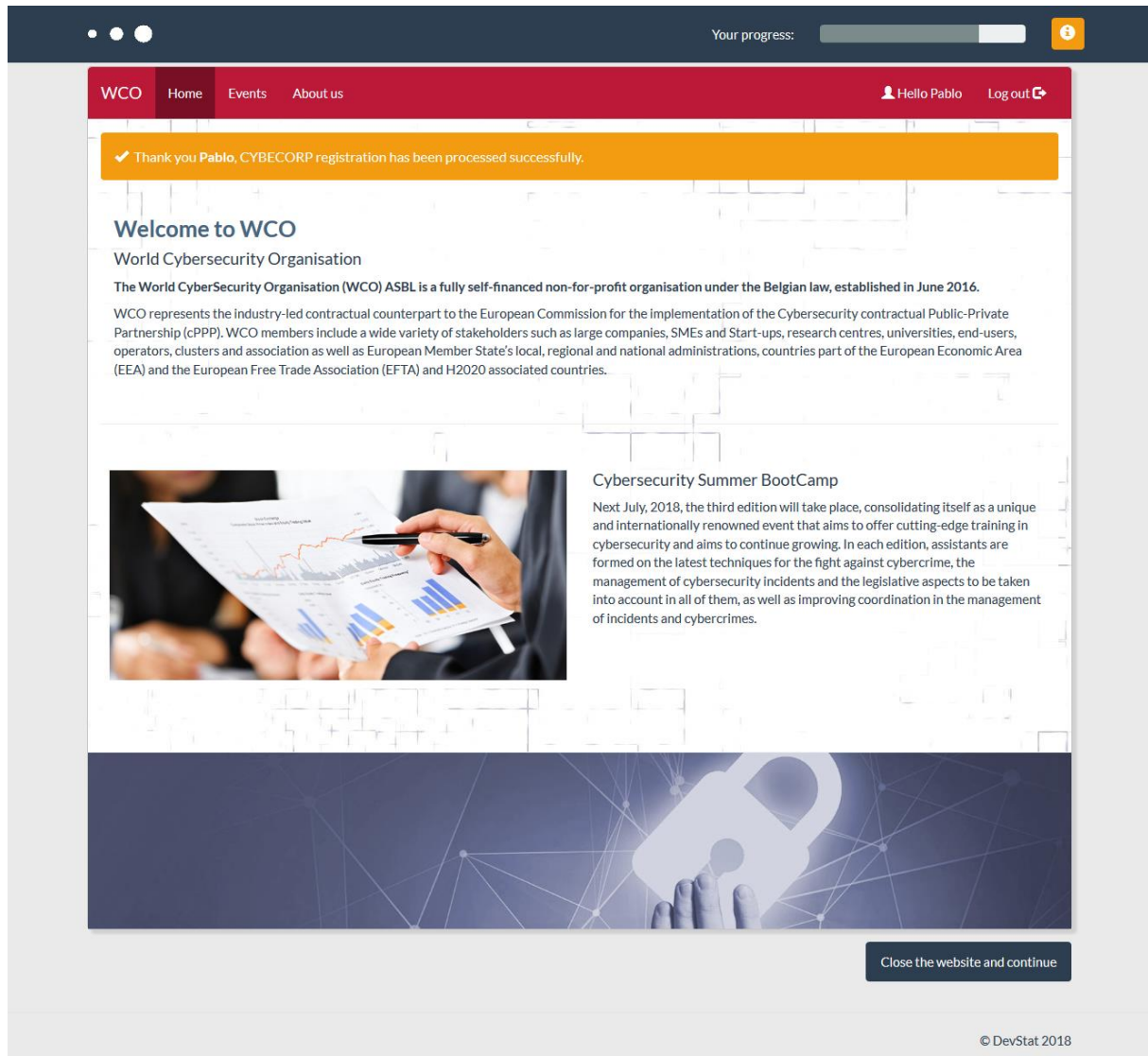


Figure 14. Event website - Logout.

D6.3: Report with Findings of Experiments and Policy implications

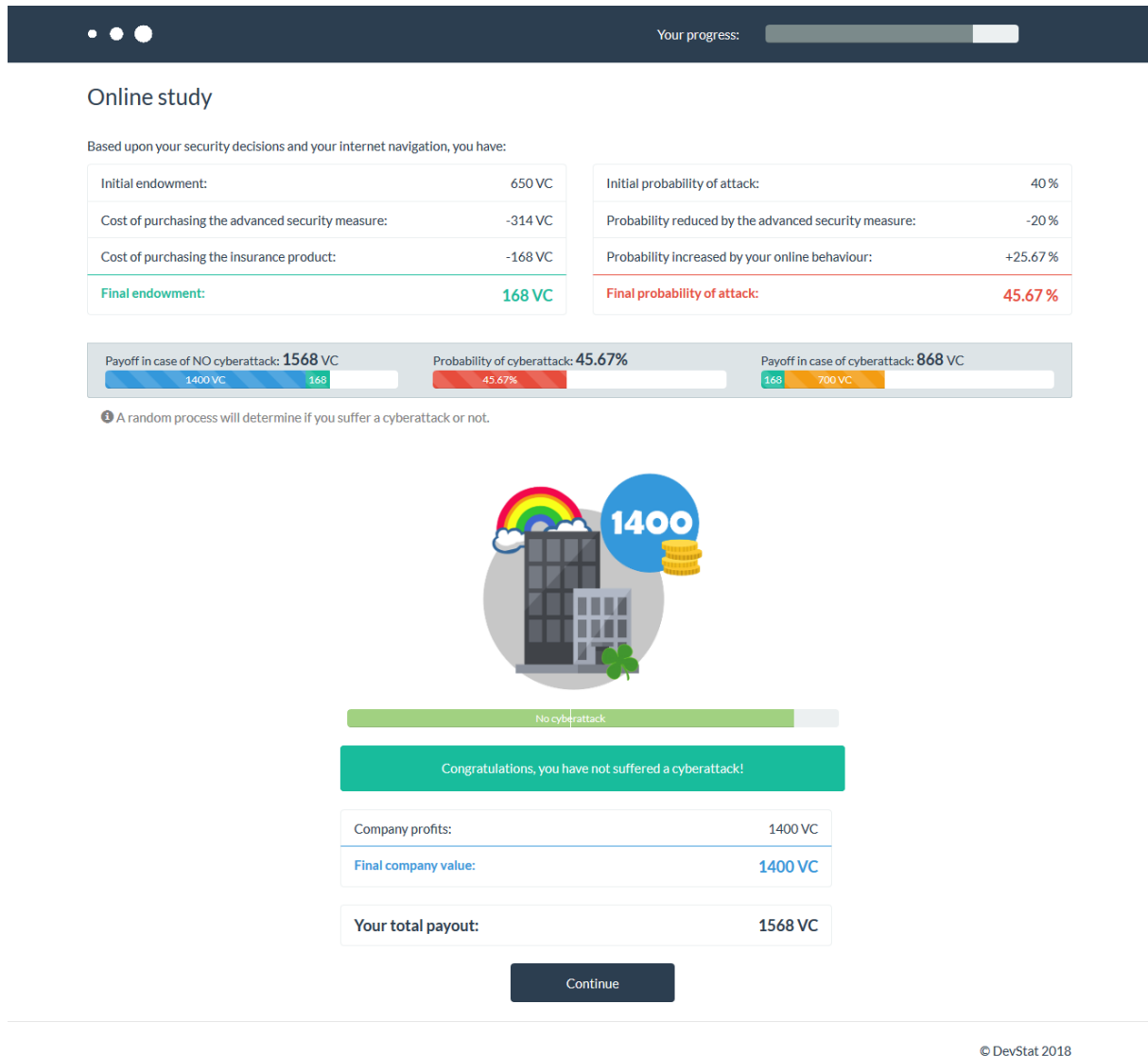


Figure 15. Cyberattack simulation.

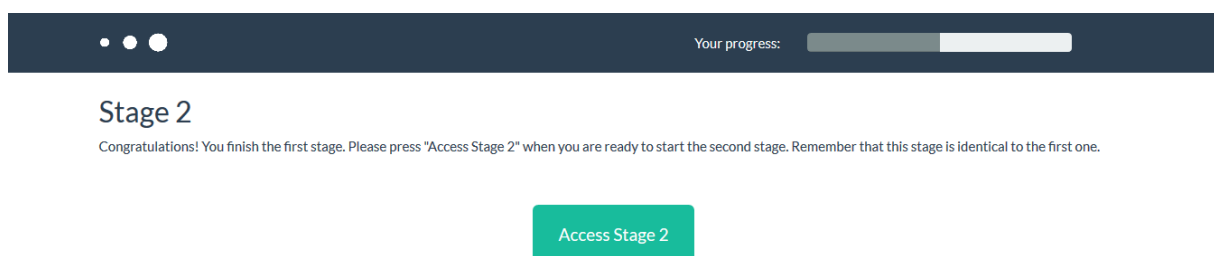


Figure 16. Access to Stage 2

D6.3: Report with Findings of Experiments and Policy implications

Your progress:

Stage 3

Finally, to increase your earnings, we are going to play eleven rounds of a quick and simple game. In each round, you will see a picture with two bags (Bag A and Bag B) with 10 balls in each bag. The balls have four different values:

● = 385 VC ● = 200 VC ● = 160 VC ● = 10 VC

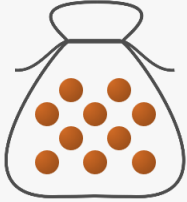
In each round, we will ask you to select one of these two bags. After completing the eleven decisions:

1. One of the 11 rounds of the game will be picked at random
2. A ball will be drawn at random **from the bag that you have actually chosen** in this round
3. The value of this ball will be added to your final payment

Please choose Bag A or Bag B for each decision below.


Decision 0

A



0 balls of 200 VC, 10 balls of 160 VC

B



0 balls of 385 VC, 10 balls of 10 VC

© DevStat 2018

Figure 17. Stage 3: Holt & Laury

Your progress:

Stage 3 - Results

As mentioned before, the first random number will determine which of the eleven decisions will be used. All of them have the same probability to be picked. Click the button to start the draw!

Selected decision

8

Your choice for Decision 8

	Bag A	Bag B
Decision 8	<input type="radio"/> 8 balls of 200 VC, 2 balls of 160 VC	<input checked="" type="radio"/> 8 balls of 385 VC, 2 balls of 10 VC

ⓘ You have selected the bag B for decision 8 in the previous screen. So, now you have 8 balls with a value of 385 VC and 2 balls with a 10 VC. When you click the button, one of the balls will be randomly selected and this will be the number of additional VC you will earn.

385

385

385

385

385

385

385

385

385

10

10

Click here to start the draw

© DevStat 2018

Figure 18. Stage 3 results

Figure 19. Final questionnaire

D6.3: Report with Findings of Experiments and Policy implications

Your progress:

Thank you!


Thank you for taking the time to complete this study. We truly value the information you have provided.

The total profit you earned for all 3 stages are shown below:

Stage 1	832 VC
Stage 2	1568 VC
Stage 3	385 VC
Total	2785 VC

Your VC earnings are converted to £ at a conversion rate of 5120 VC equal to 1 £, therefore, your final payoff in £ is:

2785 VC	0.54 £
Fixed part	0.88 £
Total	1.42 £



Please press "Finish" to complete the process

Finish

Figure 20. End page

D6.3: Report with Findings of Experiments and Policy implications

1.2 Experiment 2

Your progress:

Thank you for your participation!

Just for participating in this study, you will be rewarded with 0.88 £. In addition, you can get a maximum additional amount of 0.88 £ depending on your decisions. Therefore, your final benefit will be the sum of 0.88 £ for participating plus the amount you win during the tasks. During the process, there will be situations in which you can lose part of your profits, but keep in mind that you can never earn less than the fixed amount of 0.88 £ awarded to you for participating.

During the study, all the payoffs are denominated in Virtual Currency units (VC). Your VC earnings will be converted to £ at the end of the experiment at a conversion rate of 8850 VC equal to 1 £.

The study is formed of three stages, the first two are identical. Once you finish a stage, the next one will start automatically.

Are you ready?

Start

© DevStat 2018

Figure 21. Welcome page

D6.3: Report with Findings of Experiments and Policy implications



Before enjoying the experience, we would like to know more about you

1. What is your year of birth?

- Select -

2. Gender

- Select -

3. What is the highest level of education you have completed?

☐ 0-11 years of education

☐ 12 years of education (high school diploma)

☐ Some years of university (not completed)

☐ University degree (BA, BS)

☐ Post-graduate degree (MA, MS, JD, MD, PhD, etc)

4. Which of the following categories best describes the industry you primarily work in (regardless of your actual position)?

- Select -

5. Which of the following best describes your role in industry?

- Select -

6. Employment history (You can select more than one option)

☐ Over 1 years experience of using IT systems

☐ Over 1 years experience in a management position

☐ Over 1 years experience in a role with responsibility for purchasing

☐ Over 1 years experience in a cybersecurity role

☐ None of the above

7. Did you ever buy protection measures (antivirus, firewall, etc.) for you or your company?

☐ Yes

☐ No

8. Did you ever buy cyberinsurance products for you or your company?

☐ Yes

☐ No

Continue

Figure 22. Socio-demographic questionnaire

D6.3: Report with Findings of Experiments and Policy implications

Your progress:

Stage 1

You are the cybersecurity manager of a small business, called CYBECORP. You are aware that **there is a computer virus going around the Internet, that may affect your company**. You know that 60% of companies like yours have suffered this virus attack in the last week.


We will now ask you to make some decisions that will affect the cybersecurity of CYBECORP.

Read the following instructions in detail and press "Continue" when you are ready.

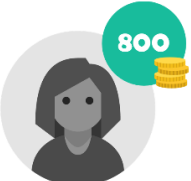
Note: You do not need to have any knowledge about computer systems or cybersecurity to complete the study. There are no right or wrong answers please just answer honestly. Whatever the result, you are guaranteed a minimum of the fixed participation rate at the end of the study.

1. Initial State


Your initial state is the following:



The income that CYBECORP obtains from its commercial data is 6600 VC



You have a budget of 800 VC to buy security measures



The probability that CYBECORP is randomly affected by the virus is 60%

2. Risk analysis tool

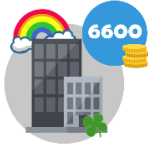
On the next page, you will be given the opportunity to use our Risk Analysis Tool to help you to decide the cyber-protection strategy for your company.

3. Purchase of security measures


After you have used the Risk Analysis Tool, you will have the opportunity to spend some of your budget on purchasing security measures and/or insurance against cyber-attacks.

4. Results

Finally, **CYBECORP may suffer a cyberattack (the probability of which is affected by your decisions)** and you will be presented with your resulting payoff. There are two possible scenarios:

1)

CYBECORP **does not suffer any cyberattack** and maintains the income obtained from its commercial data. Therefore, your payout will be 6600 VC of the CYBECORP income plus what you have left of your budget.

2)

CYBECORP **suffers a cyberattack** and loses all income from its commercial data. Therefore, your payout will be what you have left of your budget plus the amount you have insured (if you chose to buy insurance).

Continue



Figure 23. Stage 1 instructions

D6.3: Report with Findings of Experiments and Policy implications

Your progress:

Risk Analysis Tool

As previously presented, CYBECORP is a small business which obtains a profit of 6600 VC from its commercial data. You know that 60% of companies like yours have suffered this virus attack in the last week. As cyber-security manager, you have a budget of 800 VC to purchase any of the following cyber-protection measures:

Measures	Product	Description	Cost
 Security measures Security measures are computer softwares used to prevent, detect and remove malicious software	Simple	Reduces the probability of suffering the attack from 60% to 40% .	0 VC
	Advanced	Reduces the probability of suffering the attack from 60% to 10% . In addition, if you buy our Advanced security measures you will have a 50% discount on the purchase of a cyberinsurance.	120 VC
 Cyberinsurance Cyberinsurance is an insurance product used to protect businesses from Internet-based risks	None	Covers 0 VC of lost profits in case of attack.	0 VC
	Basic	Covers 1650 VC of lost profits in case of attack.	160 VC
	Premium	Covers 3300 VC of lost profits in case of attack.	640 VC

Our Risk Analysis Tool analyses the impact of the cyberattack for each of the possible combinations of security measures and insurance products. It produces a dashboard with the analysis of the five best options according to some parameters of companies that are similar to CYBECORP. This information can help you to make better purchase decisions.

You can access the Risk Analysis Tool by clicking in the bottom "Generate Risk Analysis".

Note: You will be able to reread this instructions at any point by pressing the "Instructions" button on the top right.

Generate Risk Analysis

Figure 24. Risk analysis tool explanation

D6.3: Report with Findings of Experiments and Policy implications

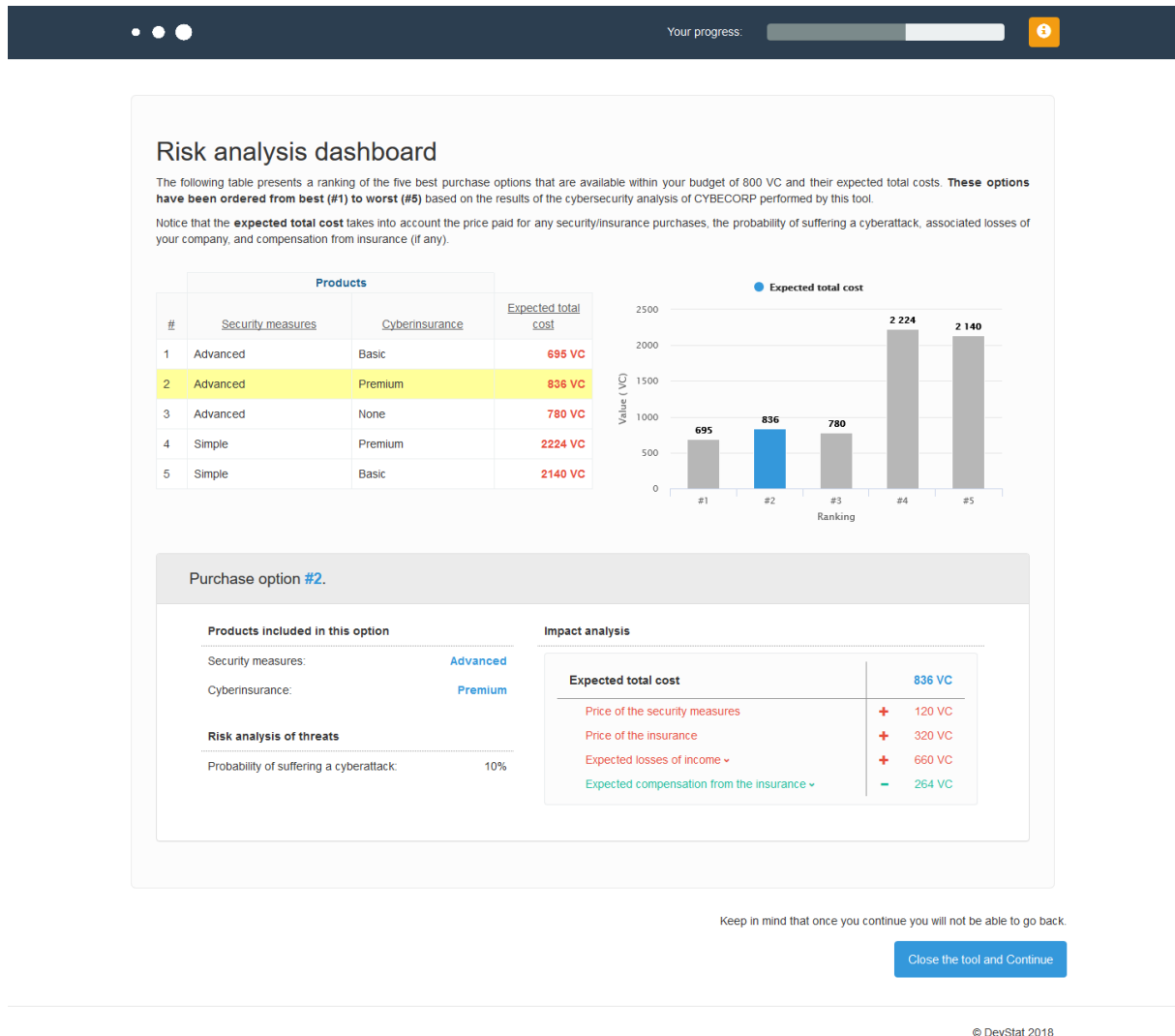


Figure 25. Treatment 1 - Risk analysis tool

D6.3: Report with Findings of Experiments and Policy implications

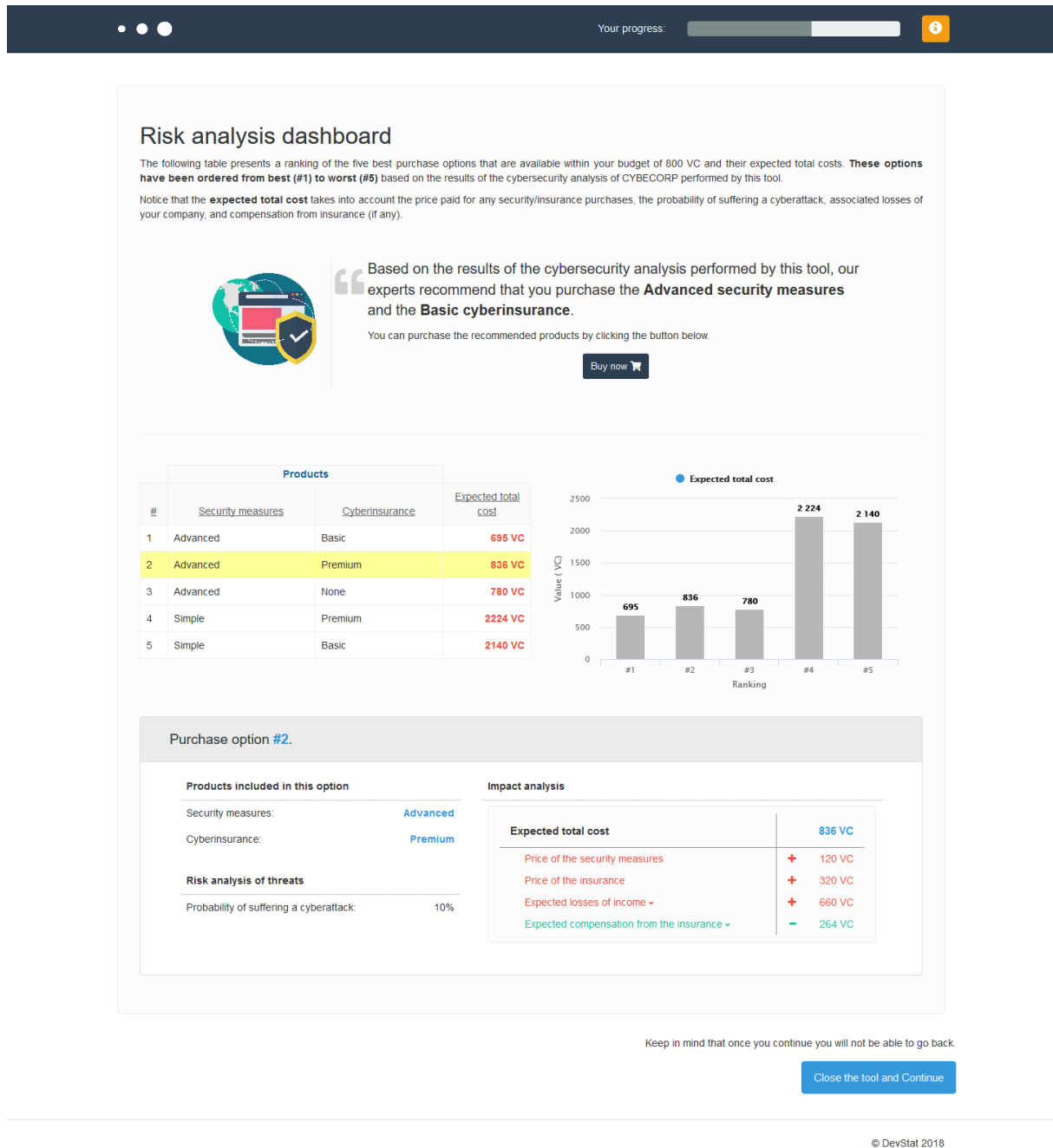


Figure 26. Treatment 2 - Risk analysis tool

D6.3: Report with Findings of Experiments and Policy implications

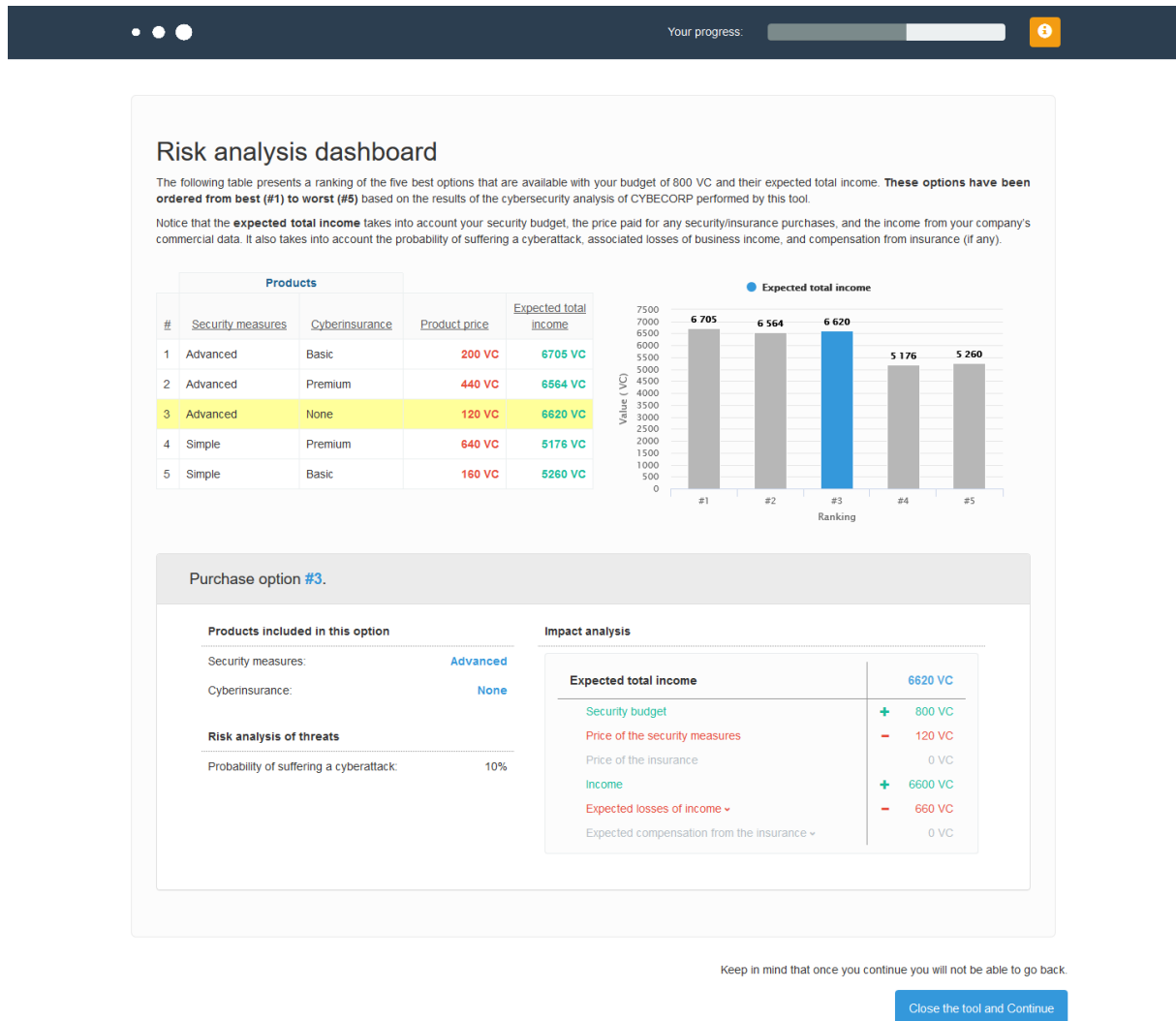


Figure 27. Treatment 3 - Risk analysis tool

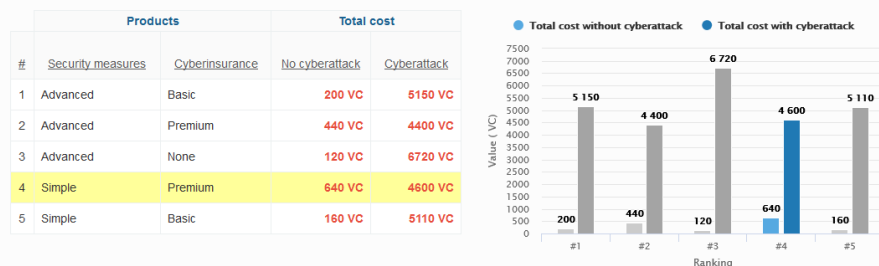
D6.3: Report with Findings of Experiments and Policy implications



Risk analysis dashboard

The following table presents a ranking of the five best purchase options that are available within your budget of 800 VC and their total costs in case of suffering a cyberattack or not. **These options have been ordered from best (#1) to worst (#5)** based on the results of the cybersecurity analysis of CYBECORP performed by this tool.

Notice that the **total cost** takes into account the price paid for any security/insurance purchases. Total cost is shown in the case of suffering a cyberattack or not. In the instance of a cyberattack, total cost also takes into account the losses of business income and compensation from insurance (if any).



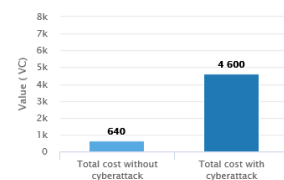
Purchase option #4

Products included in this option

Security measures: **Basic**
Cyber-insurance: **Premium**

Risk analysis of threats

Probability of suffering a cyber-attack: 40%
Probability of not suffering a cyber-attack: 60%



Impact analysis

Total cost without cyberattack		640 VC
Price of the security measures		0 VC
Price of the insurance	+	640 VC
Losses of income		0 VC
Compensation from the insurance		0 VC

Total cost with cyberattack		4600 VC
Price of the security measures		0 VC
Price of the insurance	+	640 VC
Losses of income	+	6600 VC
Compensation from the insurance	-	2640 VC

Keep in mind that once you continue you will not be able to go back.

Close the tool and Continue.

Figure 28. Treatment 4 - Risk analysis tool

D6.3: Report with Findings of Experiments and Policy implications

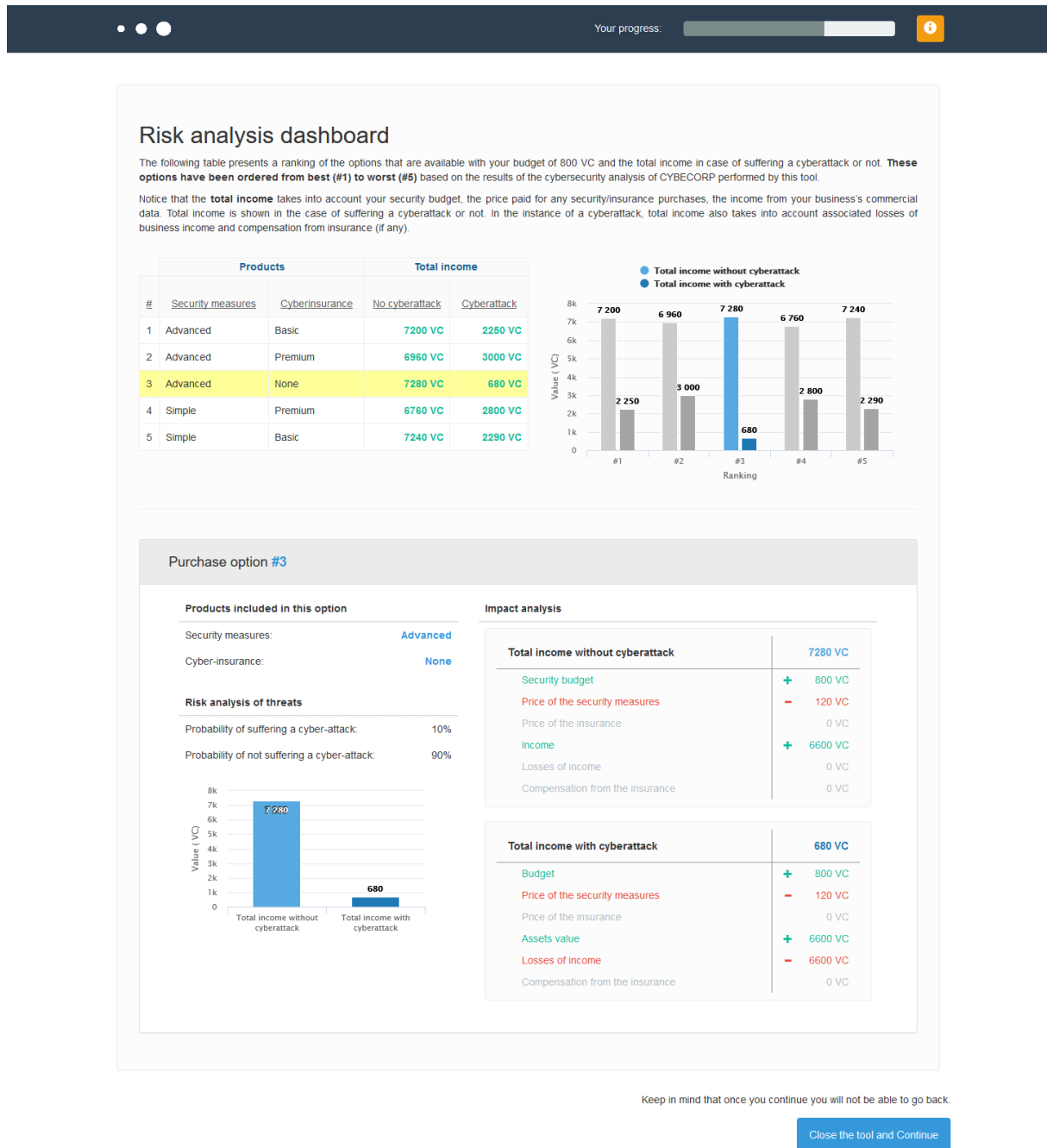


Figure 29. Treatment 5 - Risk analysis tool

D6.3: Report with Findings of Experiments and Policy implications

• • •
Your progress:
?

Cybersecurity shop

Welcome to our Cybersecurity shop! Below, we present the security measures you can buy for CYBECORP. Select the measures you want to buy and press "Continue." Remember that you have a budget of **800 VC** and keep in mind that once you press "Continue" you will not be able to go back.

You can reread the instructions at any point by pressing the "Instructions" button on the top right.

Security measures

Security measures are computer softwares used to prevent, detect and remove malicious software:

Simple security measures



Simple security measures costs 0 VC and the probability of suffering the attack is 40%

Cost	0 VC
Attack probability	40%

Advanced security measures



Advanced security measures costs 120 VC and the probability of suffering the attack is 10%

In addition, if you buy our Advanced security measures you will have a 50% discount on the purchase of a cyberinsurance.

Cost	120 VC
Attack probability	10%

Which one do you want to buy?

Simple security measures

Advanced security measures

Cyberinsurance

Cyberinsurance is an insurance product used to protect businesses from Internet-based risks. We offer you three options with different level of coverage:


No insurance



Opting for no insurance costs 0 VC and covers 0 VC of lost profits in case of attack

Cost	0 VC
Coverage	0 VC


Basic insurance



The "Basic insurance" costs 160 VC and covers 1650 VC of lost profits in case of attack

Cost	160 VC
Coverage	1650 VC

Premium insurance



The "Premium insurance" costs 640 VC and covers 3300 VC of lost profits in case of attack

Cost	640 VC
Coverage	3300 VC

Which one do you want to buy?

No insurance

Basic insurance

Premium insurance

Continue

Figure 30. Cybersecurity shop

D6.3: Report with Findings of Experiments and Policy implications

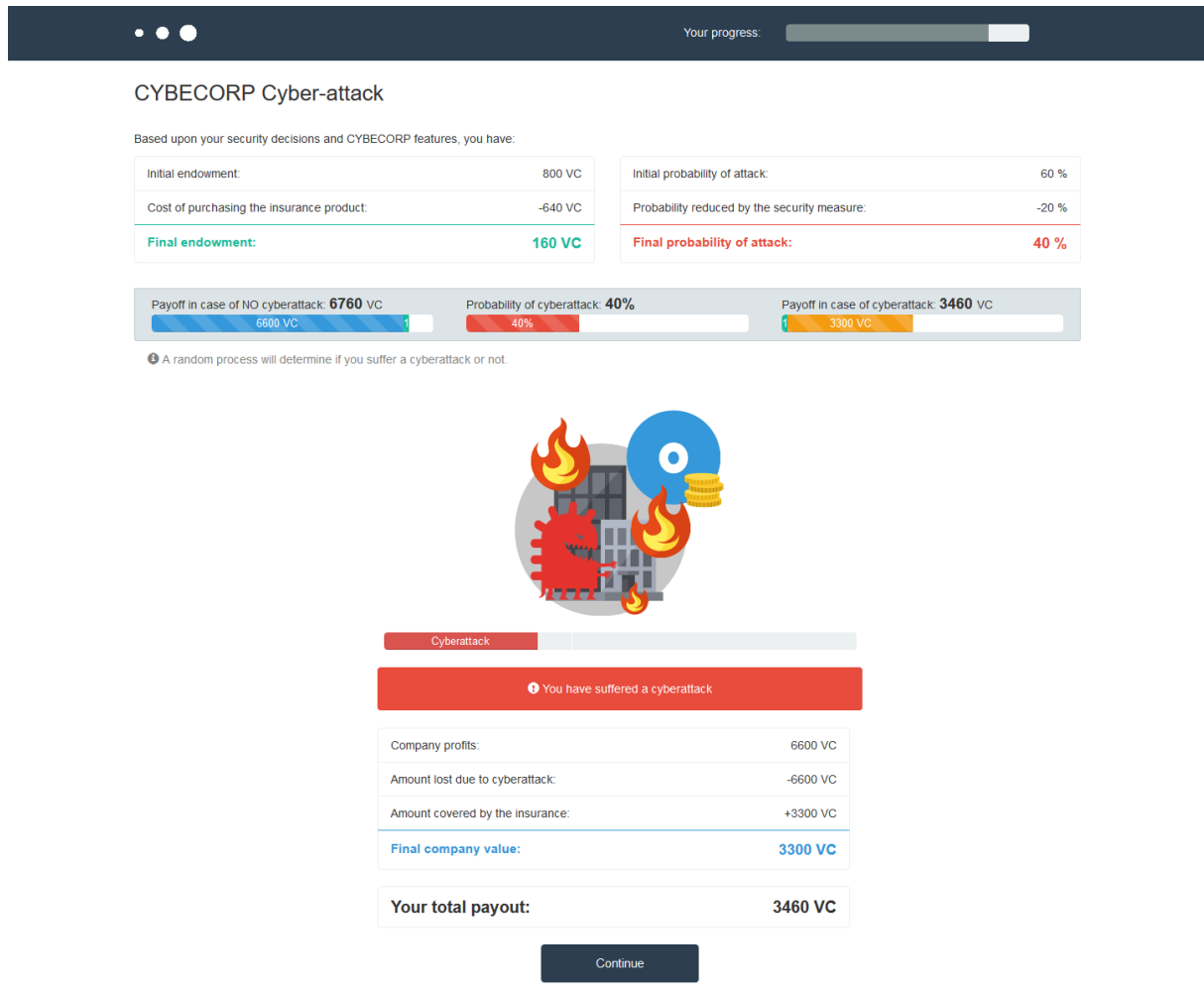


Figure 31. Cyberattack simulation

D6.3: Report with Findings of Experiments and Policy implications

Your progress:

Before continuing, we would like you to answer some questions about your decisions

Why do you selected the option that you purchase from our cybersecurity shop?

☐ It guaranteed the highest coverage in the case of an attack

☐ It was the cheapest

☐ It guaranteed the maximum protection against a cyberattack

☐ It was the first in the ranking

☐ It was the option recommended by the experts in cybersecurity

☐ I selected an option at random

Our Risk Analysis Tool presents a ranking of the five best options that are available with your budget:

Do you consider that the terms and concepts that appear in this risk analysis dashboard are clear and easy to understand?

Very unclear and difficult to understand...

1

2

3

4

5

6

7

 ... Very clear and easy to understand

Do you remember which of the following options was the first one in the ranking provided by the tool?

☐ Simple security measures & No insurance

☐ Simple security measures & Basic insurance

☐ Simple security measures & Premium insurance

☐ Advance security measures & No insurance

☐ Advance security measures & Basic insurance

☐ Advance security measures & Premium insurance

Did you buy the first option of the ranking?

☐ Yes

☐ No

☐ I don't know

Please, indicate the degree to which you agree or disagree with the following statements:

How confident are you in the option you have chosen?

0% Not at all confident 100% Confident

How much do you trust that the toolbox will suggest the best option for you?

0% No trust 100% Complete trust

Please, indicate the degree to which you agree or disagree with the following statements:

If available, how likely would you be to use this toolbox in the future?

Not at all likely...

1

2

3

4

5

6

7

 ... Highly likely

The toolbox's capabilities meet my requirements

Do not meet my requirements at all...

1

2

3

4

5

6

7

 ... Meet all of my requirements

The toolbox is easy to use

Very difficult to use...

1

2

3

4

5

6

7

 ... Very easy to use

Continue

Figure 32. Usability questionnaire

D6.3: Report with Findings of Experiments and Policy implications

• • •

Your progress:

Stage 2

Finally, to increase your earnings, we are going to play eleven rounds of a quick and simple game. In each round, you will see a picture with two bags (Bag A and Bag B) with 10 balls in each bag. The balls have four different values:

● = 385 VC
● = 200 VC
● = 160 VC
● = 10 VC

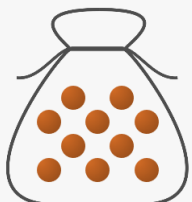
In each round, we will ask you to select one of these two bags. After completing the eleven decisions:

- One of the 11 rounds of the game will be picked at random
- A ball will be drawn at random **from the bag that you have actually chosen** in this round
- The value of this ball will be added to your final payment

Please choose Bag A or Bag B for each decision below.


Decision 0

A



0 balls of 200 VC, 10 balls of 160 VC

B



0 balls of 385 VC, 10 balls of 10 VC

© DevStat 2018

Figure 33. Stage 2: Holt & Laury

• • •

Your progress:

Stage 2 - Results

As mentioned before, the first random number will determine which of the eleven decisions will be used. All of them have the same probability to be picked. Click the button to start the draw!

Selected decision

5

Your choice for Decision 5

	Bag A	Bag B
Decision 5	<input type="radio"/> 5 balls of 200 VC, 5 balls of 160 VC	<input checked="" type="radio"/> 5 balls of 385 VC, 5 balls of 10 VC

ⓘ You have selected the bag B for decision 5 in the previous screen. So, now you have 5 balls with a value of 385 VC and 5 balls with a 10 VC. When you click the button, one of the balls will be randomly selected and this will be the number of additional VC you will earn.

385
385
385
385
385
10
10
10
10
10

ⓘ Draw completed!

Your earnings:

10 VC

Continue

© DevStat 2018

Figure 34. Stage 2 results

D6.3: Report with Findings of Experiments and Policy implications

Final questionnaire

Please indicate the degree to which you agree or disagree with the following statements:

1 - Strongly Disagree

2 - Disagree

3 - Neutral

4 - Agree

5 - Strongly Agree

If my online data is not secure, it would be worse

1

2

3

4

5

My online data is not as secure as I think it is

1

2

3

4

5

I think that my online data is not as secure as I think it is

1

2

3

4

5

I am confident that my online data is not as secure as I think it is

1

2

3

4

5

Insurance is an effective method to protect against loss

1

2

3

4

5

Insurance can be needed to pay out in the event of a disaster

1

2

3

4

5

For the following questions, security measures are technical actions such as installing and updating antivirus software, keeping passwords secure, turning a device when necessary, etc. Security measures are also non-technical actions such as using a secure network.

1 - Strongly Disagree

2 - Disagree

3 - Neutral

4 - Agree

5 - Strongly Agree

I find cyber security measures to be more complex than I think they are

1

2

3

4

5

I find cyber security measures to be more complex than I think they are

1

2

3

4

5

Taking the necessary security measures is making me feel better

1

2

3

4

5

I have the resources and the knowledge to take the necessary security measures

1

2

3

4

5

Taking the necessary security measures is easy

1

2

3

4

5

For the following questions, "insurance" refers to insurance in general. Indicate the degree to which you agree or disagree with the following statements:

1 - Strongly Disagree

2 - Disagree

3 - Neutral

4 - Agree

5 - Strongly Agree

Insurance is necessary to be safe

1

2

3

4

5

Setting up insurance would require too much time

1

2

3

4

5

Insurance is too expensive for me

1

2

3

4

5

Insurance is too complicated for me

1

2

3

4

5

Insurance is not worth it

1

2

3

4

5

Having an insurance could help me in the event of a disaster

1

2

3

4

5

Insurance is a good idea

1

2

3

4

5

Insurance is important

1

2

3

4

5

I have the idea of taking out insurance to protect me

1

2

3

4

5

I think it is important to me that I have an insurance (house, contents, etc.)

1

2

3

4

5

What other types of insurance have you taken in the last 12 months (please list all that apply):

Building Insurance

Contents Insurance

Fire Insurance

Health Insurance

Cyber Insurance

Vehicle Insurance

How many insurance claims have you experienced in the past 12 months?

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

Please indicate the extent to which you agree or disagree with the following statement by selecting the option you prefer. Please do not think too long before answering, usually your first instinct is also the best one.

a. Safety First

1

2

3

4

5

6

7

8

9

10

Not agree

b. I do not take risks with my health

1

2

3

4

5

6

7

8

9

10

Not agree

c. I prefer to avoid risks

1

2

3

4

5

6

7

8

9

10

Not agree

d. I take risks regularly

1

2

3

4

5

6

7

8

9

10

Not agree

e. I really dislike not knowing what is going to happen

1

2

3

4

5

6

7

8

9

10

Not agree

f. I usually enter risks as a challenge

1

2

3

4

5

6

7

8

9

10

Not agree

g. I never missed on a ...

1

2

3

4

5

6

7

8

9

10

Not agree

Please indicate the degree to which you agree or disagree with the following statement:

1 - Strongly Disagree

2 - Disagree

3 - Neutral

4 - Agree

5 - Strongly Agree

I am not in a position to take risks

1

2

3

4

5

What could influence your decision to take cyber risks?

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

Continue

Figure 35. Final questionnaire

D6.3: Report with Findings of Experiments and Policy implications

Your progress:

Thank you!


Thank you for taking the time to complete this study. We truly value the information you have provided.

The total profit you earned for all 2 stages are shown below:

Stage 1	3460 VC
Stage 2	10 VC
Total	3470 VC

Your VC earnings are converted to £ at a conversion rate of 8850 VC equal to 1 £, therefore, your final payoff in £ is:

3470 VC	0.39 £
Fixed part	0.88 £
Total	1.27 £



Please press "Finish" to complete the process

Finish

Figure 36. End page

D6.3: Report with Findings of Experiments and Policy implications

2 Questionnaires

2.1 Experiment 1: Sociodemographic questionnaire

Before enjoying the experience, we would like to know more about you:

1. What is your year of birth?

2. Gender

- Male
- Female

3. What is the highest level of education you have completed?

- 0 -11 years of education
- 12 years of education (high school diploma)
- Some years of university (not completed)
- University degree (BA, BS)
- Post-graduate degree (MA, MS, JD, MD, PhD, etc)
- Employment situationSelf-employed
- Public/Private worker
- Unemployed
- Housewife/Househusband
- Student
- Retired
- Other (rent perceiver, public or private aid)

2.2 Experiment 2: Sociodemographic questionnaire

Before enjoying the experience, we would like to know more about you:

1. What is your year of birth?

2. Gender

- Male
- Female

3. What is the highest level of education you have completed?

- 0 -11 years of education

D6.3: Report with Findings of Experiments and Policy implications

- 12 years of education (high school diploma)
- Some years of university (not completed)
- University degree (BA, BS)
- Post-graduate degree (MA, MS, JD, MD, PhD, etc)

4. Which of the following categories best describes the industry you primarily work in (regardless of your actual position)?

- Software
- Telecommunications
- Information Services and Data Processing
- Computer and Electronics Manufacturing
- Finance and Insurance
- Agriculture, Forestry, Fishing and Hunting
- Utilities
- Wholesale
- Transportation and Warehousing
- Broadcasting
- Other Information Industry
- Real Estate, Rental and Leasing
- Primary/Secondary (K-12) Education
- Health Care and Social Assistance
- Hotel and Food Services
- Legal Services
- Homemaker
- Religious
- Mining
- Construction
- Other Manufacturing
- Retail
- Publishing
- College, University, and Adult Education
- Other Education Industry
- Arts, Entertainment, and Recreation
- Government and Public Administration
- Scientific or Technical Services

D6.3: Report with Findings of Experiments and Policy implications

- Military
- Other Industry

5. Which of the following best describes your role in industry?

- Upper Management
- Middle Management
- Junior Management
- Administrative Staff
- Support Staff
- Student
- Trained Professional
- Skilled Laborer
- Consultant
- Temporary Employee
- Researcher
- Self-employed/Partner
- Other

6. Employment history (You can select more than one option)

- ☐ Over 1 years experience of using IT systems
- ☐ Over 1 years experience in a management position
- ☐ Over 1 years experience in a role with responsibility for purchasing
- ☐ Over 1 years experience in a cybersecurity role
- ☐ None of the above

7. Did you ever buy protection measures (antivirus, firewall, etc.) for you or your company?

- Yes
- No

8. Did you ever buy cyberinsurance products for you or your company?

- Yes
- No

2.3 Experiment 2: Usability questionnaire

Before continuing, we would like you to answer some questions about your decisions:

1. Why do you selected the option that you purchase from our cybersecurity shop?

D6.3: Report with Findings of Experiments and Policy implications

- ☐ It guaranteed the highest coverage in the case of an attack
- ☐ It was the cheapest
- ☐ It guaranteed the maximum protection against a cyberattack
- ☐ It was the first in the ranking
- ☐ It was the option recommended by the experts in cybersecurity
- ☐ I selected an option at random

Our Risk Analysis Tool presents a ranking of the five best options that are available with your budget:

2. Do you consider that the terms and concepts that appear in this risk analysis dashboard are clear and easy to understand?

Very unclear and difficult to understand 1 2 3 4 5 6 7 Very clear and easy to understand

3. Do you remember which of the following options was the first one in the ranking provided by the tool?

- Simple security measures & No insurance
- Simple security measures & Basic insurance
- Simple security measures & Premium insurance
- Advance security measures & No insurance
- Advance security measures & Basic insurance
- Advance security measures & Premium insurance

4. Did you buy the first option of the ranking?

- Yes
- No
- I don't know

5. Why did you not select the first option in the ranking provided by the tool? (If answer to the previous question is "No")

- ☐ Options were ranked with no special criterion
- ☐ The first option was too expensive
- ☐ The insurance in first option did not provide enough coverage
- ☐ The protection measures in the first option were not safe enough
- ☐ I do not understand the criterion of the ranking

D6.3: Report with Findings of Experiments and Policy implications

Please, indicate the degree to which you agree or disagree with the following statements:

6. How confident are you in the option you have chosen?

Not at all confident 0% | 100% Confident

7. How much do you trust that the toolbox will suggest the best option for you?

No trust 0% | 100% Complete trust

8. If available, how likely would you be to use this toolbox in the future?

Not at all likely 1 2 3 4 5 6 7 Highly likely

9. The toolbox's capabilities meet my requirements

Do not meet my requirements at all 1 2 3 4 5 6 7 Meet all of my requirements

10. The toolbox is easy to use

Very difficult to use 1 2 3 4 5 6 7 Very easy to use

D6.3: Report with Findings of Experiments and Policy implications

2.4 Experiment 1 & 2: Final questionnaire

1. Perceived Severity (fits with PMT - threat appraisal). Adapted from Menard, Bott & Crossler, 2017.

1.1. If my online data/accounts were hacked, it would be severe
Strongly disagree 1 2 3 4 5 Strongly agree

2. Perceived Vulnerability (fits with PMT - threat appraisal). Adapted from Menard, Bott & Crossler, 2017.

2.1. My online data/accounts are at risk of being compromised
Strongly disagree 1 2 3 4 5 Strongly agree

2.2. It is likely that my online data/accounts will be breached
Strongly disagree 1 2 3 4 5 Strongly agree

2.3. It is possible that my online data/accounts will be compromised
Strongly disagree 1 2 3 4 5 Strongly agree

3. Response Efficacy (fits with PMT - coping appraisal).

3.1. Insurance is an effective method to protect against loss
Strongly disagree 1 2 3 4 5 Strongly agree

3.2. Insurers can be trusted to pay out in the event of a claim (*e.g., Petrolia et al, 2013, found credibility of insurers affects uptake*)
Strongly disagree 1 2 3 4 5 Strongly agree

D6.3: Report with Findings of Experiments and Policy implications

4. Self-efficacy/Perceived Behavioural Control (fits with TPB & PMT). Adapted from Anderson & Agarwal (2010).

4.1. For the following questions, security measures are individual actions such as running and updating antivirus software, keeping passwords secure, running a firewall when necessary, etc. Indicate the degree to which you agree or disagree with the following statements:

4.1.1. I feel comfortable taking measures to secure my own computer(s)

Strongly disagree 1 2 3 4 5 Strongly agree

4.1.2. I feel comfortable taking security measures to limit the threat to other people and the Internet in general

Strongly disagree 1 2 3 4 5 Strongly agree

4.1.3. Taking the necessary security measures is entirely under my control

Strongly disagree 1 2 3 4 5 Strongly agree

4.1.4. I have the resources and the knowledge to take the necessary security measures

Strongly disagree 1 2 3 4 5 Strongly agree

4.1.5. Taking the necessary security measures is easy

Strongly disagree 1 2 3 4 5 Strongly agree

5. Response Cost [of insuring/claiming] & Rewards [of not insuring] (fits with PMT - threat & coping appraisal). Adapted from Anderson & Agarwal (2010). Last item added.

5.1. Insurance is financially costly for me

Strongly disagree 1 2 3 4 5 Strongly agree

5.2. Setting up insurance would require too much from me

Strongly disagree 1 2 3 4 5 Strongly agree

5.3. Insurance is burdensome for me

Strongly disagree 1 2 3 4 5 Strongly agree

5.4. Insurance is time consuming for me

Strongly disagree 1 2 3 4 5 Strongly agree

5.5. Insurance is not worth it

Strongly disagree 1 2 3 4 5 Strongly agree

5.6. Claiming on insurance could harm a business/organisations reputation

Strongly disagree 1 2 3 4 5 Strongly agree

D6.3: Report with Findings of Experiments and Policy implications

6. Attitudes (fits with TPB). Adapted from Anderson & Agarwal (2010).

6.1. Insurance is a good idea

Strongly disagree 1 2 3 4 5 Strongly agree

6.2. Insurance is important

Strongly disagree 1 2 3 4 5 Strongly agree

6.3. I like the idea of taking out insurance to protect me

Strongly disagree 1 2 3 4 5 Strongly agree

7. Subjective Norms (fits with TPB)

7.1. People who are important to me think that I should have insurance

Strongly disagree 1 2 3 4 5 Strongly agree

8. Past Behaviour

8.1. Which of the following have you had in the last 12 months (please tick all that apply):

- ☐ Buildings Insurance
- ☐ Contents Insurance
- ☐ Flood Insurance
- ☐ Health Insurance
- ☐ Cyber Insurance
- ☐ Vehicle Insurance

9. Past Experience (E.g., Baumann & Sims (1978) found higher insurance uptake if previously experienced flood damage).

9.1. How many insurance claims have you experienced in the past 12 months?

10. Risk Preference Dospert scale (Blais & Weber, 2006)

10.1. Safety first

Totally disagree 1 2 3 4 5 6 7 8 9 Totally agree

10.2. I do not take risks with my health

Totally disagree 1 2 3 4 5 6 7 8 9 Totally agree

10.3. I prefer to avoid risks

Totally disagree 1 2 3 4 5 6 7 8 9 Totally agree

D6.3: Report with Findings of Experiments and Policy implications

10.4. I take risks regularly

Totally disagree 1 2 3 4 5 6 7 8 9 Totally agree

10.5. I really dislike knowing what is going to happen

Totally disagree 1 2 3 4 5 6 7 8 9 Totally agree

10.6. I usually view risks as a challenge

Totally disagree 1 2 3 4 5 6 7 8 9 Totally agree

10.7. I view myself as a...

Risk avoider 1 2 3 4 5 6 7 8 9 Risk seeker

11. Intention (fits with TPB). Adapted from Menard, Bott & Crossler (2017).

11.1. I am likely to purchase cyber insurance

Strongly disagree 1 2 3 4 5 strongly agree

11.2. What would influence your decision to buy cyberinsurance ?