



CYBECO: “Supporting Cyberinsurance from a Behavioural Choice Perspective”

Lorentz Cyberinsurance Open Day
March 27, 2019



Objective

- Research and develop a framework for managing cybersecurity risks, focused on cyberinsurance as key risk management treatment
- How?
 - ✓ By transferring risk of the insured companies to the insurance provides
 - ✓ By providing incentives for improving security

Challenges

- Lack of data => incomplete overall risk picture => inability of insurance companies to design their offerings
- Companies deciding on whether to buy cyberinsurance or not

Activities

- Develop a cybersecurity risk management model
 - ✓ Intentionality of adversaries
 - ✓ Cyberinsurance in the risk management portfolio
 - ✓ Structured expert judgement methodologies for little data
 - ✓ Cyber security behavioural and psychological findings
- Develop a decision support tool, the CYBECO Toolbox implementing the modelling framework
- Conduct behavioural experiments to validate the models and tool
- Provide policy recommendations to cover policy gaps



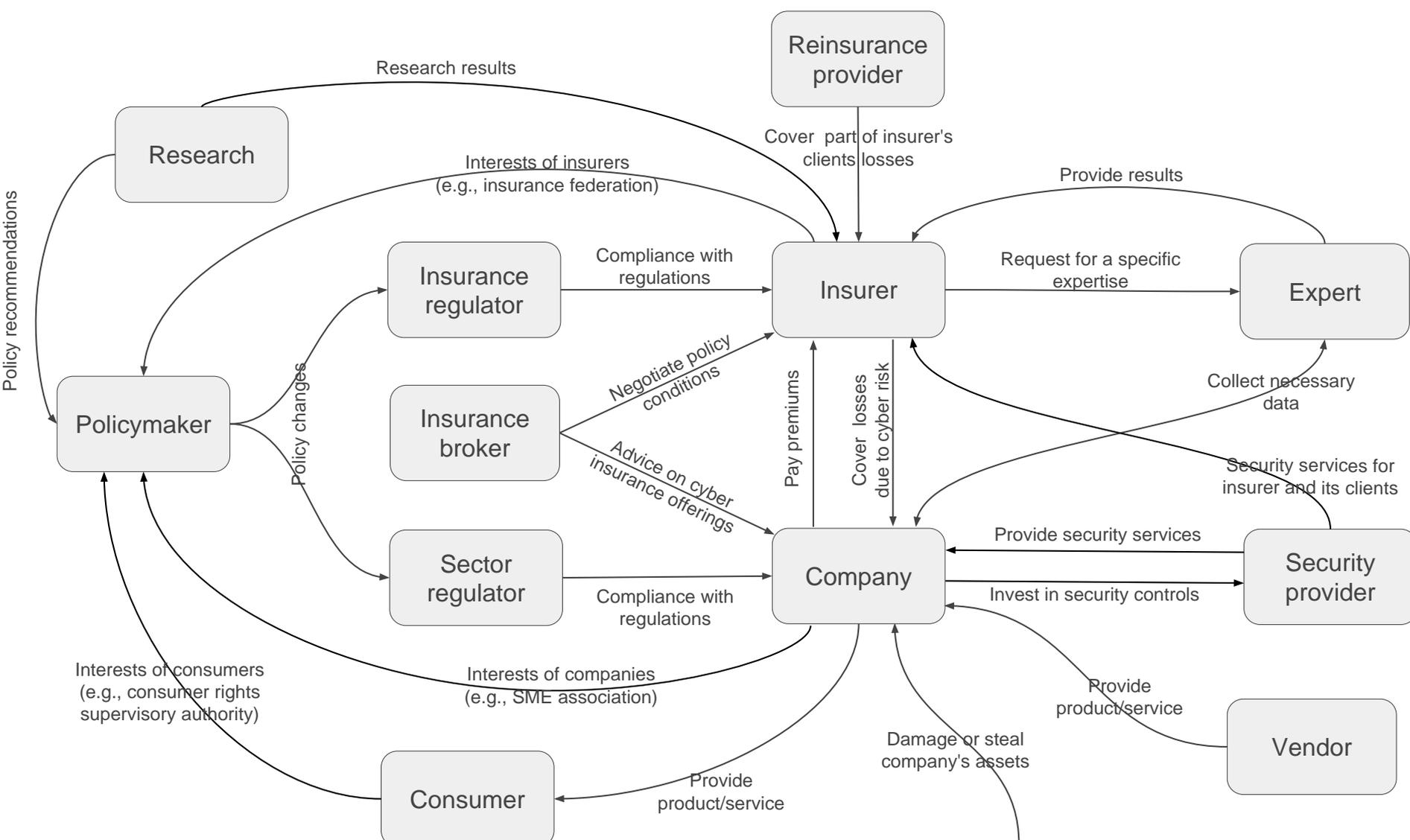
Cyber Insurance Ecosystem & Policy Recommendations

Kate Labunets & Wolter Pieters
TU Delft



Our goal

- What could be optimized in cyber insurance governance?
- Our approach is to identify
 - cyber insurance stakeholders,
 - their relations,
 - their goals, and
 - policy measures.



Actors' objectives toward cyber insurance

- Companies
 - Get advice on security investments
 - Cover possible losses related to cyber risk
 - Help with incident response
- Brokers
 - Provide high quality advice about cyber risks
 - Make profit
- Insurance providers
 - Increase market share
 - Have better actuarial data
 - Profitable business
- Regulator/government
 - Increase overall level of security
 - Resilient ecosystem

Policy measures¹

- Wider adoption
 - Legislation creating a financial cost to cyber events
 - Raise awareness about gaps in traditional insurance products
 - Governments to exercise their procurement power to support market development
 - Mandate insurance for organisations in certain industries
- Defining coverage
 - Encourage the use of cyber exclusions in non-cyber policies
 - Standardise wording of cyber insurance policies
 - Provide certification for acts of cyber war or terrorism

¹ Woods, D. and Simpson, A., 2017. Policy measures and cyber insurance: a framework. *Journal of Cyber Policy*, 2(2), pp.209-226.

Policy measures

- Data collection
 - Standard data formats for assessment or claims process
 - Minimum standards for data collection in assessment process
 - Government collects high-level data on the insurance market
- Information sharing
 - Make data held by government agencies available
 - Open up access to existing information-sharing initiatives
 - Mandate other organisations to make data available
 - Government to create a cyber incident data repository

Policy measures

- Best practices
 - Government can define information security best practice
 - Lead organisations to best practice through regulation
 - Clarify liability related to insurers giving security advice
- Catastrophic loss
 - Government to act as insurer of last resorts
 - Collect funds ex-ante or ex-post
 - Joining scheme is optional or mandatory
 - Premium priced according to underlying risk or priced according to amount of insurance sold
 - Upper limit on the amount the government will cover
 - Upper limit on the amount one insured can claim

Mapping goals and policy measures

		Wider adoption	Defining coverage	Data collection	Information sharing	Security best practices	Catastrophic loss
Company	Get advice on security investments						
	Cover possible losses related to cyber risk						
	Help with incident response						
Broker	Provide high quality advice about cyber risks						
	Make profit						
Insurance provider	Increase market share						
	Have better actuarial data						
	Profitable business						
Regulator / government	Increase overall level of security						
	Resilient ecosystem						

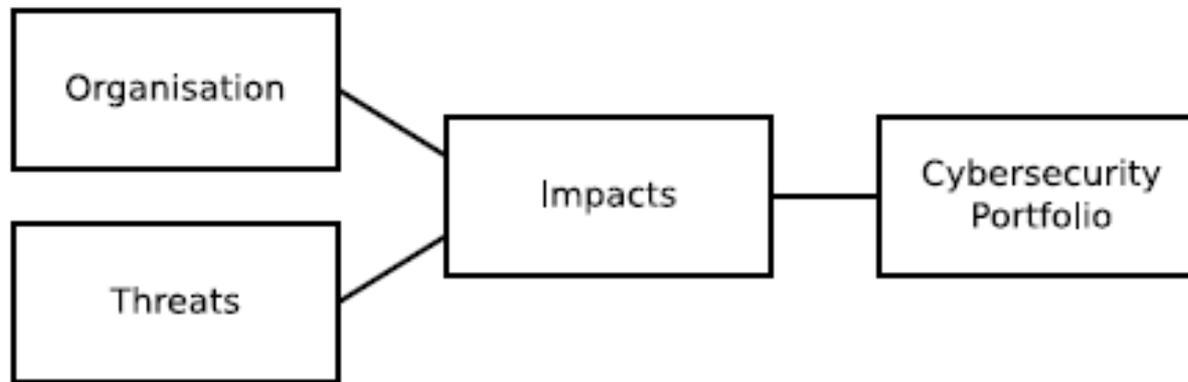


CYBECO models for cyber security risk management

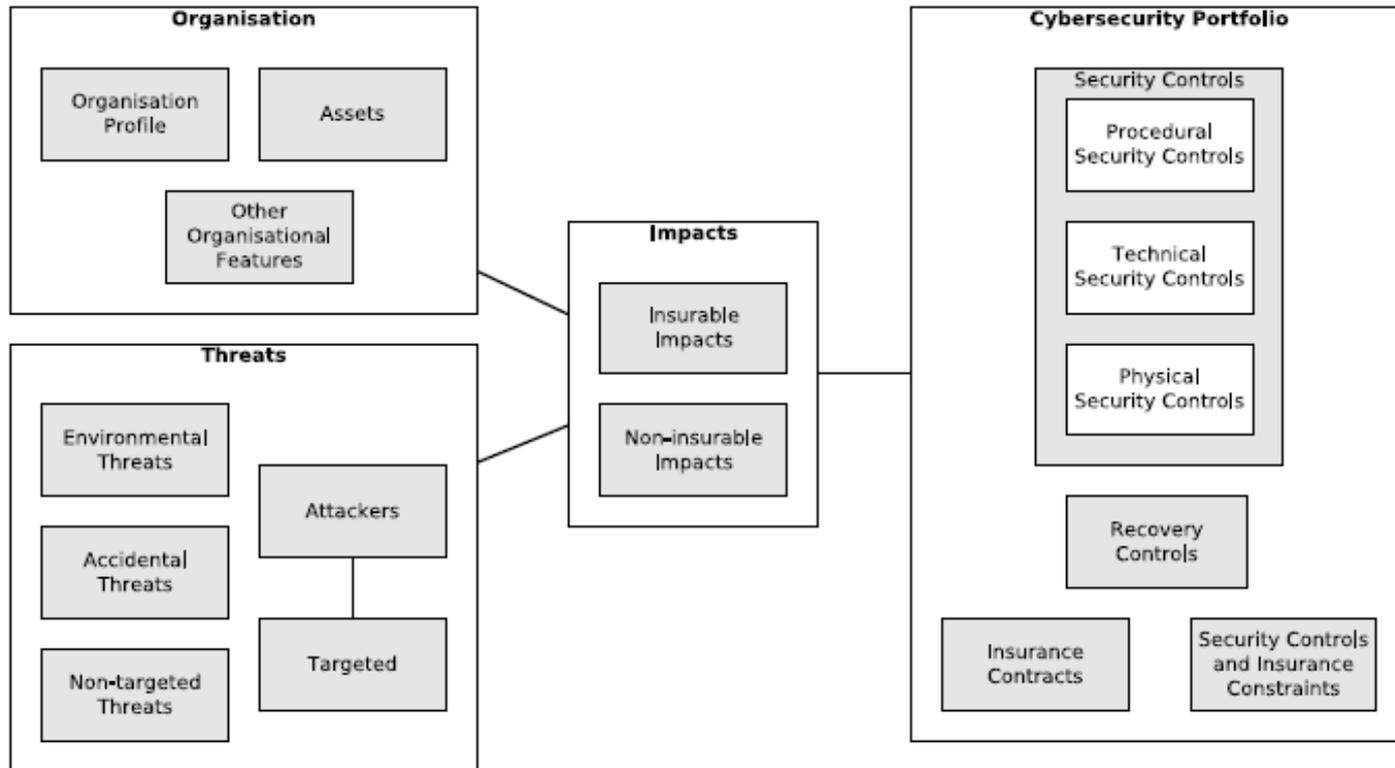
David Rios (CSIC-ICMAT)



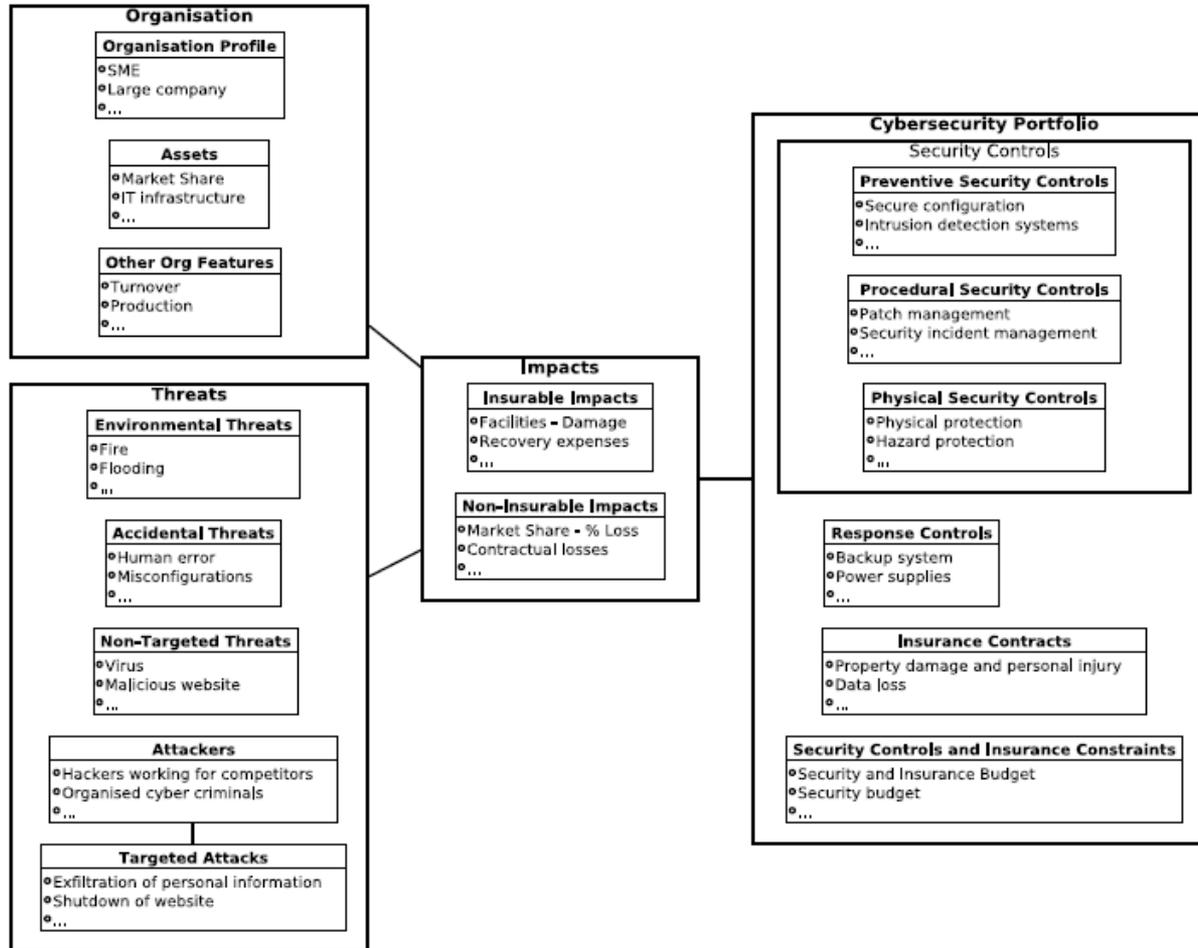
Cyber security risk management



Cyber security risk management



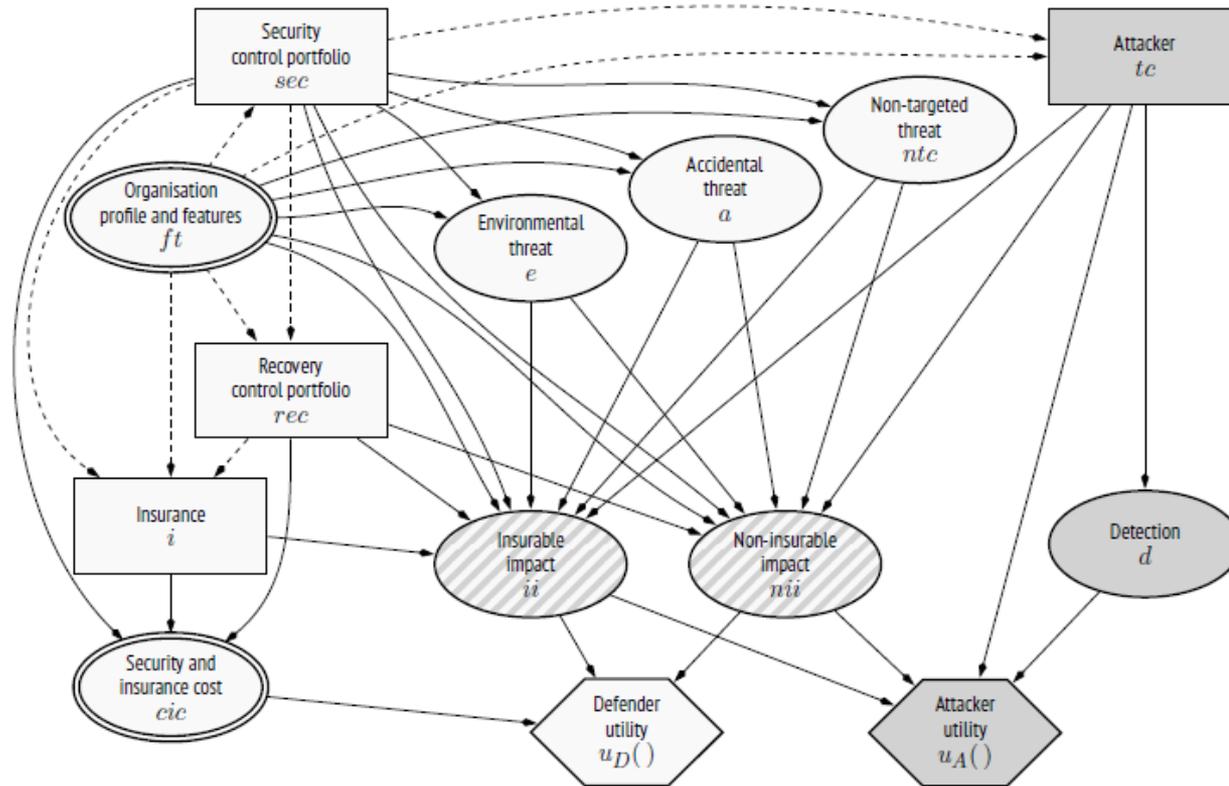
Cyber security risk management



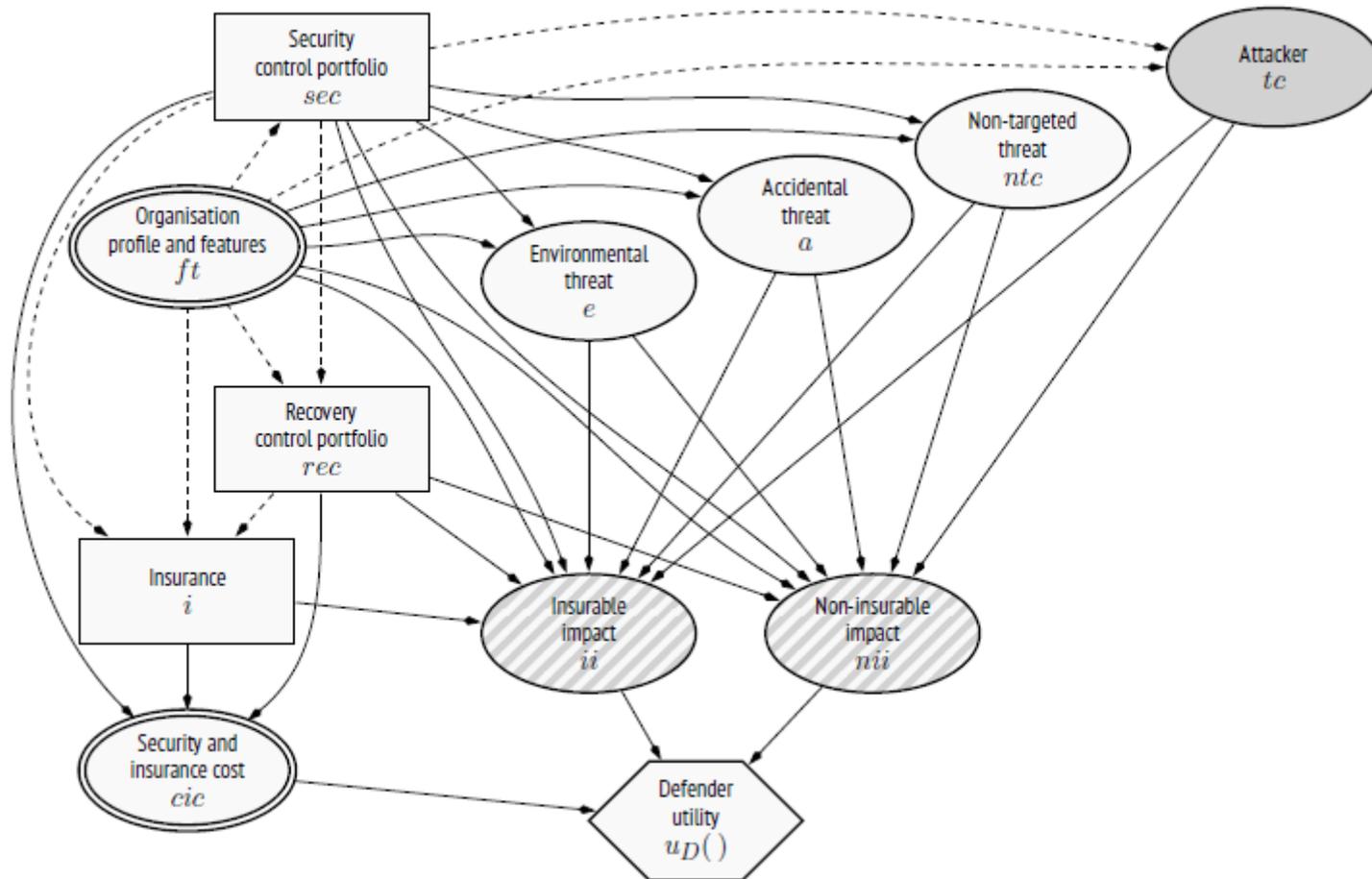
CYBECO security risk management

- Intentionality. Modeling attackers through Adversarial Risk Analysis (robustness, 'smoothness', improved forecasts)
- Structured expert judgement when data unavailable
- Cyber insurance
- Constraints
- Preference models
- Templates, Parametrised models, Catalogs
- Sensitivity analysis

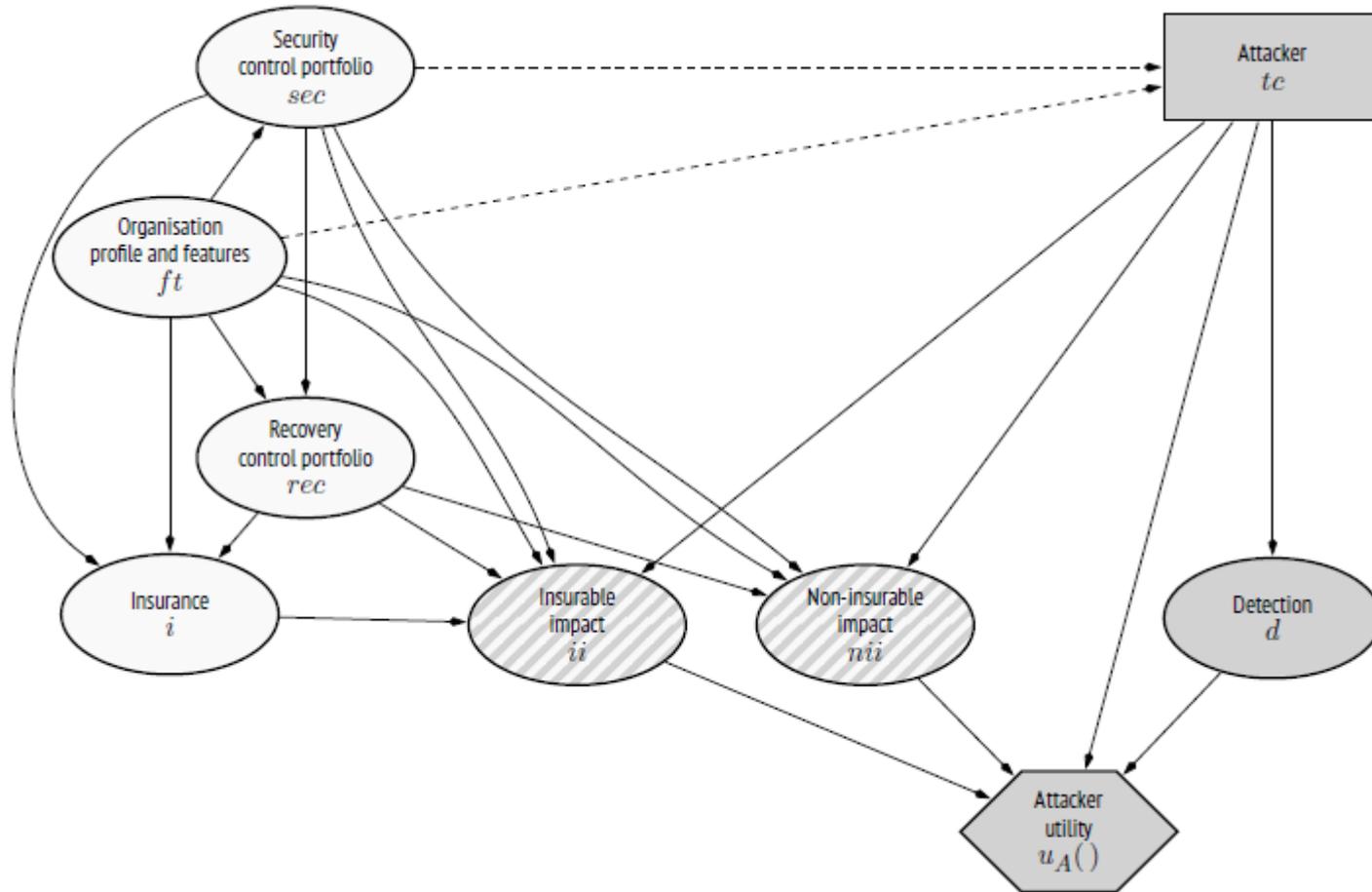
Cyber security risk management



Cyber security risk management



Cyber security risk management



Cyber security risk management

Category	Component	Node
Assets	Number of computers $ft_{computers}$ Number of servers $ft_{servers}$ Number of personal identifiable information (PII) records $ft_{records}$	ft
Other organisation features	Turnover of the organisation in Euros $ft_{turnover}$ Number of employees $ft_{employees}$	ft
Environmental threats	Fire e_{fire}	e
Accidental threats	Employee error $a_{emperror}$	a
Non-targeted cyber threats	Malware $ntc_{malware}$	ntc
Targeted cyber threats: Attackers	Hacktivists (ha, hd, \dots) Cybercriminals (ka, kd, \dots)	
Targeted cyber threats: Targeted Attacks	Targeted data exfiltration, $ha_{targetex}$ and $ka_{targetex}$ Targeted data manipulation, $ha_{targman}$ and $ka_{targman}$ Targeted denial of services, $ha_{targdos}$ and $ka_{targdos}$	ha and ka
Attacker uncertainties	Detection	hd and kd
Impacts	IT infrastructure: damage to physical properties, $ii_{physical}$ and $nii_{physical}$ IT infrastructure: business downtime, $ii_{downtime}$ and $nii_{downtime}$ Personal information: records with personal information exposed, nii_{recept} Personal information: privacy and security liability lost, $ii_{piiliab}$ and $nii_{piiliab}$ Recovery and other post-incident expenses, $ii_{postinc}$ and $nii_{postinc}$	ii or nii
Security controls	Boundary firewalls and internet gateways $sec_{boundary}$ Secure configuration sec_{seconf} Access control sec_{access} Malware protection $sec_{malprot}$ Patch management and vulnerability management $sec_{patchman}$ Hazard protection $sec_{hazprot}$	sec
Insurance contracts	Property damage and personal injury ins_{damage} Data loss $ins_{dataloss}$	ins
Preferences	The defender utility node $u_D()$ The hackers utility node $u_H()$ The cybercriminals utility node $u_K()$	

Cyber security risk management

Parametrised models



Other relevant issues

- Implementing computations
- Insider threats
- Third parties
- Building the forecasting models
- Turning this into a DSS tool
- Behavioral aspects
- Cyber risk management cycle

Other models or model uses

- Pricing. Maximum price
- ROSI
- Market segmentation

- Granting an insurance
- Reinsurance



CYBECO Toolbox

Vassilis Chatzigiannakis (Intrasoft International)
Aitor Couce Vieira (CSIC-ICMAT)



CYBECO Toolbox scope

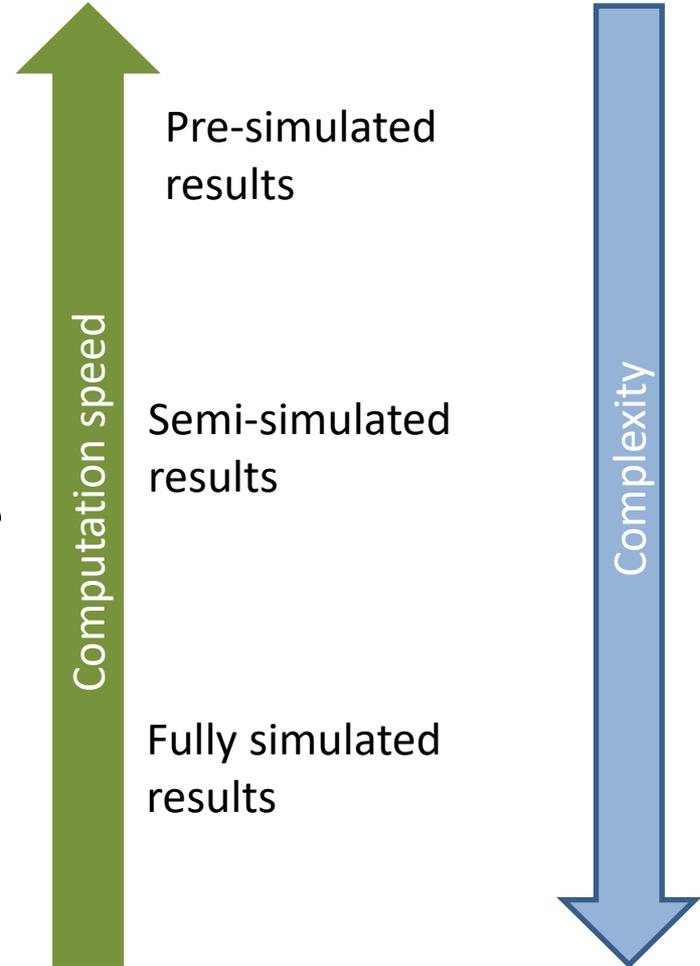
- Web-based information and consultancy tool that includes decision-support elements
 - It facilitates decisions about IT security investments
 - It is based on the results of the CYBECO research and modeling tasks
- Summarizes the most important recommendations for the design, implementation, monitoring, evaluation and exploitation of the CYBECO models
- Enables policy makers, insurance operators and interested enterprises
 - to obtain easy access to information on relevant concepts of cybersecurity insurance,
 - to provide them with a framework of analysis and feedback provisioning on the details of the deployment of the CYBECO models in real world settings

CYBECO Toolbox features

- Can be used by non-experts
- Is translating the Adversarial Risk Assessment models into **a system of algorithms**
- Provides support for three modes of Risk Analysis
- Is supported by a Knowledge Base that:
 - Contains hierarchical taxonomies of entities used in the Risk Analysis Cases
 - Contains information about related cybersecurity entities such as threats or security controls.
 - All entities in the KB are interconnected

Supported Risk Analysis Cases

- **Knowledge Base Risk Analysis Case** options and results are stored in the DB.
- **Calculation-based Risk Analysis Cases:** options, and partial results, are stored in the DB, final results are calculated dynamically.
- **R-based Risk Analysis Templates:** runs simulation on demand in the background and notifies the user when results are ready.



CYBECO Toolbox demonstration

Presented Risk Analysis Case:

- A single **SME facing cybersecurity risks**. Goal:
 - To choose the optimal cyber security portfolio and cyber insurance product.



The behavioural-experimental approach

Devstat (José Vila) & Northumbria University (Pam Briggs)



The role of psychological theory and behavioural economics in promoting cybersecurity

- **Psychological theories** can help explain behaviour and decision making around cybersecurity, and identify factors influencing insurance uptake
- Combined with **behavioural economic experiments**, this provides a strong scientific method to study how participants make security decisions



The human behavioural component...

Traditional approach

Assumes humans are always conscious, logical decision makers



Slow



Conscious



Effortful



Complex Decisions



Reliable

BUT...

human behaviour (including decision making) is not always logical!



Fast



Unconscious



Automatic



Everyday Decisions

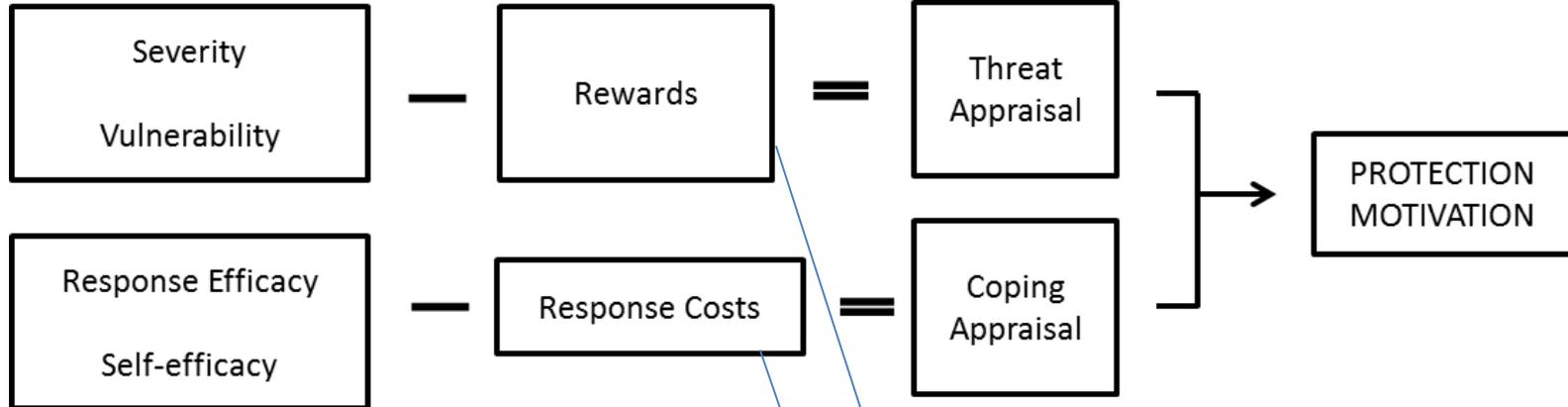


Error prone

Protection-Motivation Theory

SEVERITY: If my online data/accounts were hacked, it would be severe

VULNERABILITY: My online data/accounts are at risk of being compromised



RESPONSE EFFICACY: Insurance is an effective method to protect against loss

SELF-EFFICACY: Taking the necessary security measures is entirely under my control

REWARDS OF NOT HAVING INSURANCE / COSTS OF INSURANCE:

Insurance is financially costly for me
Insurance is not worth it
Setting up insurance would require too much from me

The human behavioural component...

CYBECO economic experiments address this in three ways:

Experiment 1: Testing the model

- Behavioral insights to support design of cyberinsurance products
- Information to produce a '*behavioural version*' of the CYBECO model

Experiment 2: Testing the toolbox

- Usability of CYBECO toolbox
- Nudging SMEs towards optimal protection & cyberinsurance

Experiment 3: Belief formation

- Supporting believe formation in adversarial cyberinsurance models

The human behavioural component...

CYBECO economic experiments address this in three ways:

Experiment 1: Testing the model

- Behavioral insights to support design of cyberinsurance products
- Information to produce a '*behavioural version*' of the CYBECO model

Experiment 2: Testing the toolbox

- Usability of CYBECO toolbox
- Nudging SMEs towards optimal protection & cyberinsurance

Experiment 3: Belief formation

- Supporting believe formation in adversarial cyberinsurance models

Experiment 1: Validating the CYBECO model

- Sample of 4,800 subjects in four countries (Germany, Poland, Spain & UK)
- Subjects' decisions are real and have actual consequences

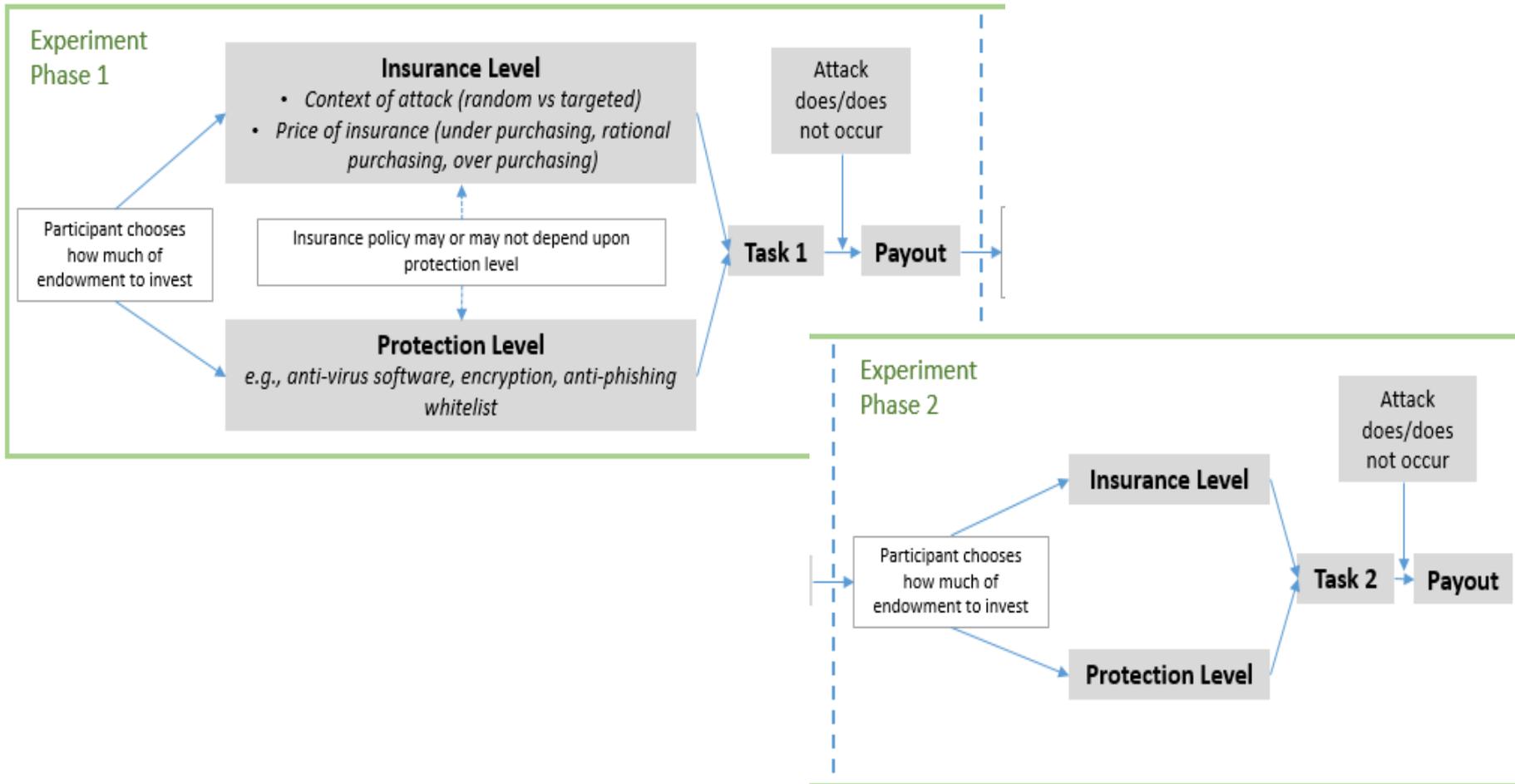
Treatments

Factors	
Context of the cyberattack	The attack is random (virus) / intentional (cyber-criminal).
Price dependence	Insurance price does / does not depend on protection level
Features of the product	Base price (expected utility) Proportional price increment Non-proportion

Behavioural measures

Protection level
Insurance level
Online behaviour
PMT variables
Risk Attitude

Experiment 1: blueprint



Experiment 1: purchase decision-making

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 a 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 payout. There are two possible scenarios:

- 

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.
- 

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](#)

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.

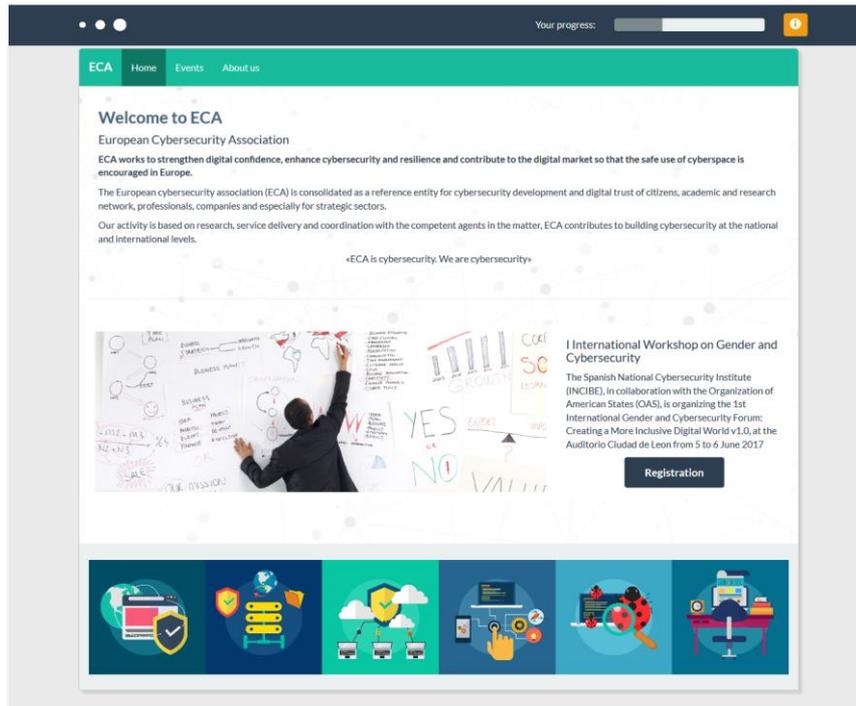
Cost	280 VC
Coverage	700 VC

Which one do you want to buy?

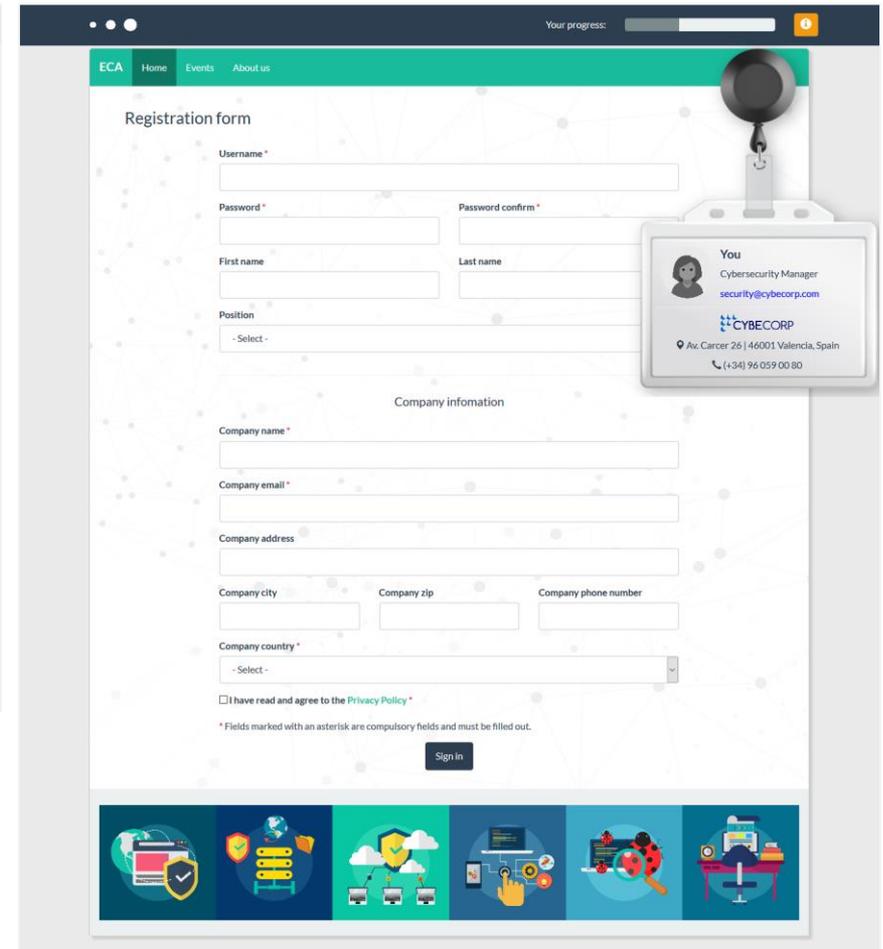
No insurance
Basic insurance
Premium insurance

[Continue](#)

Experiment 1: online surfing



The screenshot shows the home page of the European Cybersecurity Association (ECA). The navigation bar includes 'ECA', 'Home', 'Events', and 'About us'. The main content area features a 'Welcome to ECA' section with a brief description of the association's mission. Below this is a large graphic with the text '«ECA is cybersecurity. We are cybersecurity.»' and a photo of a person writing on a whiteboard. To the right of the whiteboard is an announcement for the '1st International Workshop on Gender and Cybersecurity' held in Leon, Spain, from June 5 to 6, 2017. A 'Registration' button is visible at the bottom of this section. The footer contains a row of six colorful icons representing various cybersecurity concepts.



The screenshot displays the 'Registration form' on the ECA website. The form includes fields for 'Username *', 'Password *', 'Password confirm *', 'First name', 'Last name', and 'Position' (a dropdown menu). Below these is the 'Company information' section, which contains fields for 'Company name *', 'Company email *', 'Company address', 'Company city', 'Company zip', 'Company phone number', and 'Company country *' (a dropdown menu). A checkbox for 'I have read and agree to the Privacy Policy *' is located at the bottom of the form. A 'Sign in' button is positioned at the bottom right of the form area. On the right side of the page, there is a user profile card for 'You', identified as a 'Cybersecurity Manager' at 'CYBECORP' with the email 'security@cybecorp.com' and address 'Av. Carcer 26 | 46001 Valencia, Spain'. The footer features a row of six colorful icons, identical to the home page.

Experiment 1: to be or not to be... attacked

Online study

Based upon your security decisions and your internet navigation, you have:

Initial endowment:	650 VC	Initial probability of attack:	40 %
Cost of purchasing the advanced security measure:	-314 VC	Probability reduced by the advanced security measure:	-20 %
Cost of purchasing the insurance product:	-280 VC	Probability increased by your online behaviour:	+20.67 %
Final endowment:	56 VC	Final probability of attack:	40.67 %

Payoff in case of NO cyberattack: **1456 VC** Probability of cyberattack: **40.67%** Payoff in case of cyberattack: **756 VC**

⚡ A random process will determine if you suffer a cyberattack or not.



no cyberattack

Congratulations, you have not suffered a cyberattack!

Company profits:	1400 VC
Final company value:	1400 VC
Your total payout:	1456 VC

Continue

Online study

Based upon your security decisions and your internet navigation, you have:

Initial endowment:	650 VC	Initial probability of attack:	40 %
Cost of purchasing the Insurance product:	-140 VC	Probability increased by your online behaviour:	+33.33 %
Final endowment:	510 VC	Final probability of attack:	73.33 %

Payoff in case of NO cyberattack: **1910 VC** Probability of cyberattack: **73.33%** Payoff in case of cyberattack: **860 VC**

⚡ A random process will determine if you suffer a cyberattack or not.



Cyberattack

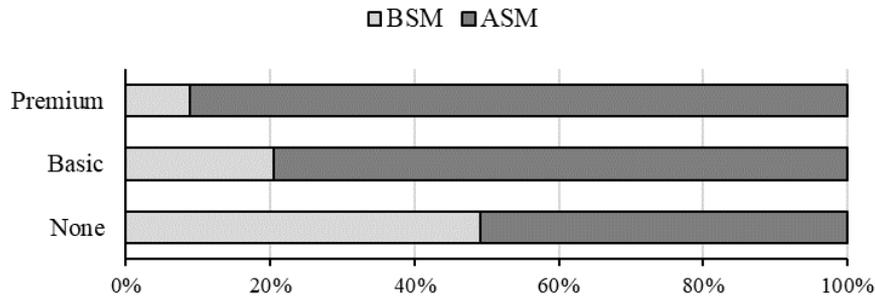
You have suffered a cyberattack

Company profits:	1400 VC
Amount lost due to cyberattack:	-1400 VC
Amount covered by the insurance:	+350 VC
Final company value:	350 VC
Your total payout:	860 VC

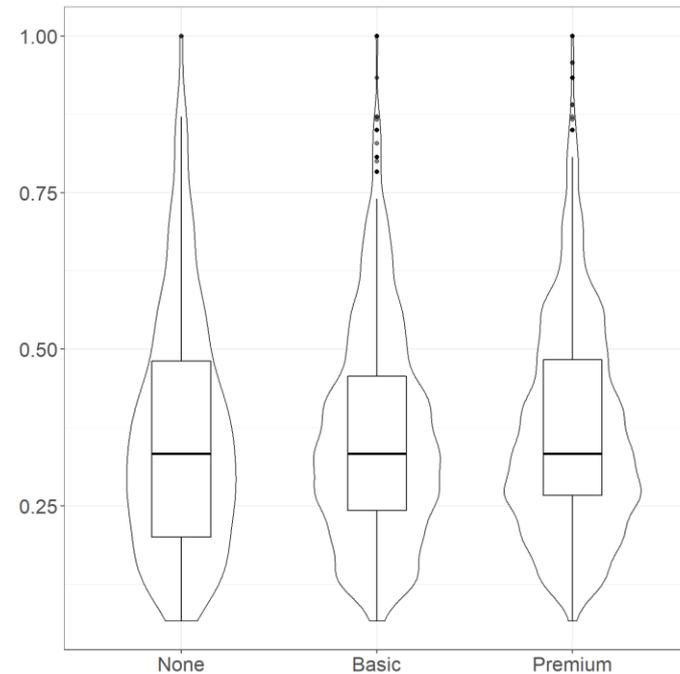
Continue

Moral hazard

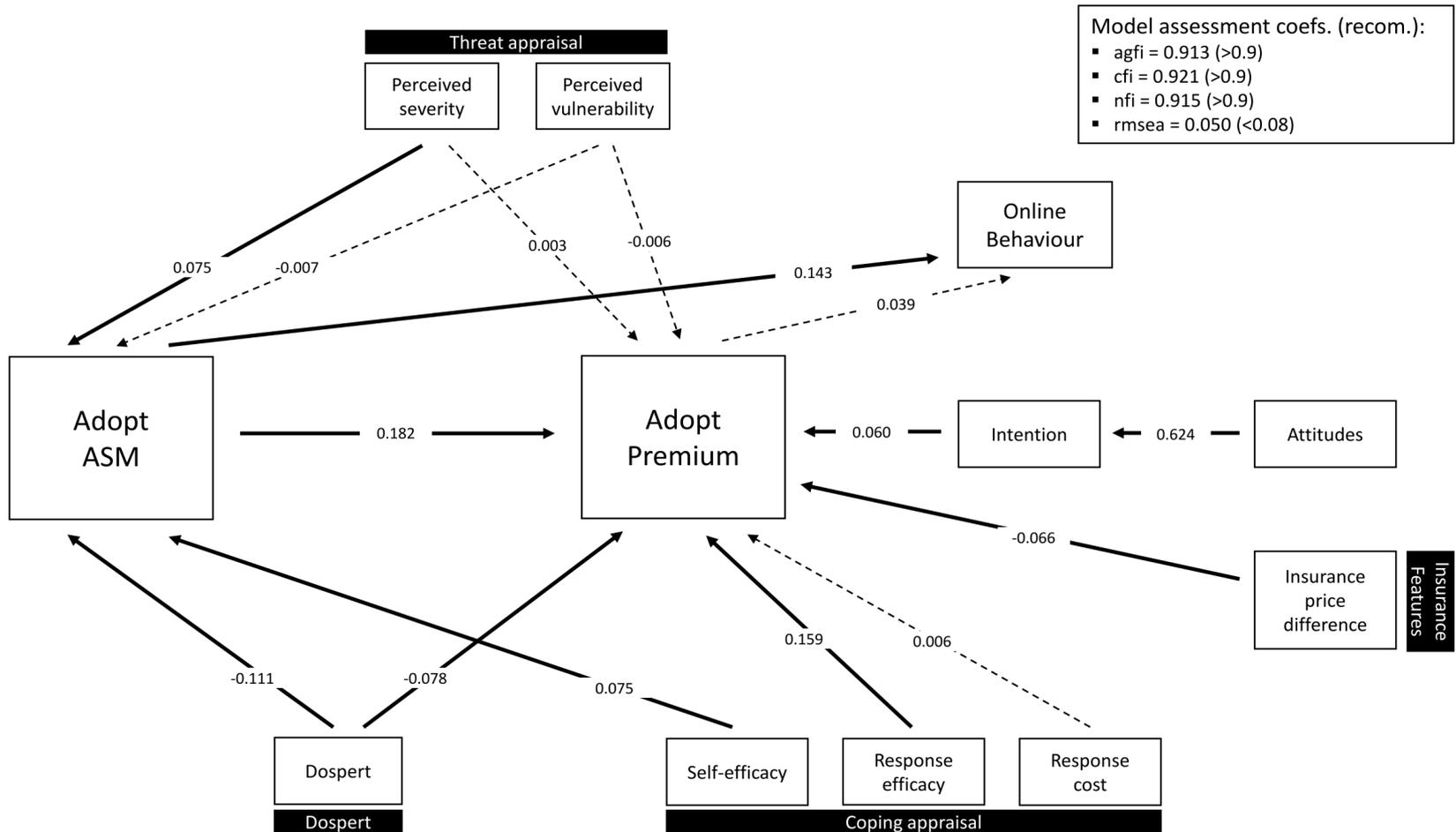
- Protection and insurance are complementary



- Insurance level does not affect online behaviour



ASM and Insurance Adoption





THANK YOU



Co-funded by
the European Union

