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

INTRASOFT INTERNATIONAL

TREK development

GOBIERNO DE ESPAÑA · MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD · CSIC

CYBECO

Cyber Insurance Ecosystem & Policy Recommendations

Kate Labunets & Wolter Pieters
TU Delft

Lorentz center

European Commission
HORIZON 2020

AXA TECHNOLOGY SERVICES redefining / service

TU Delft Delft University of Technology

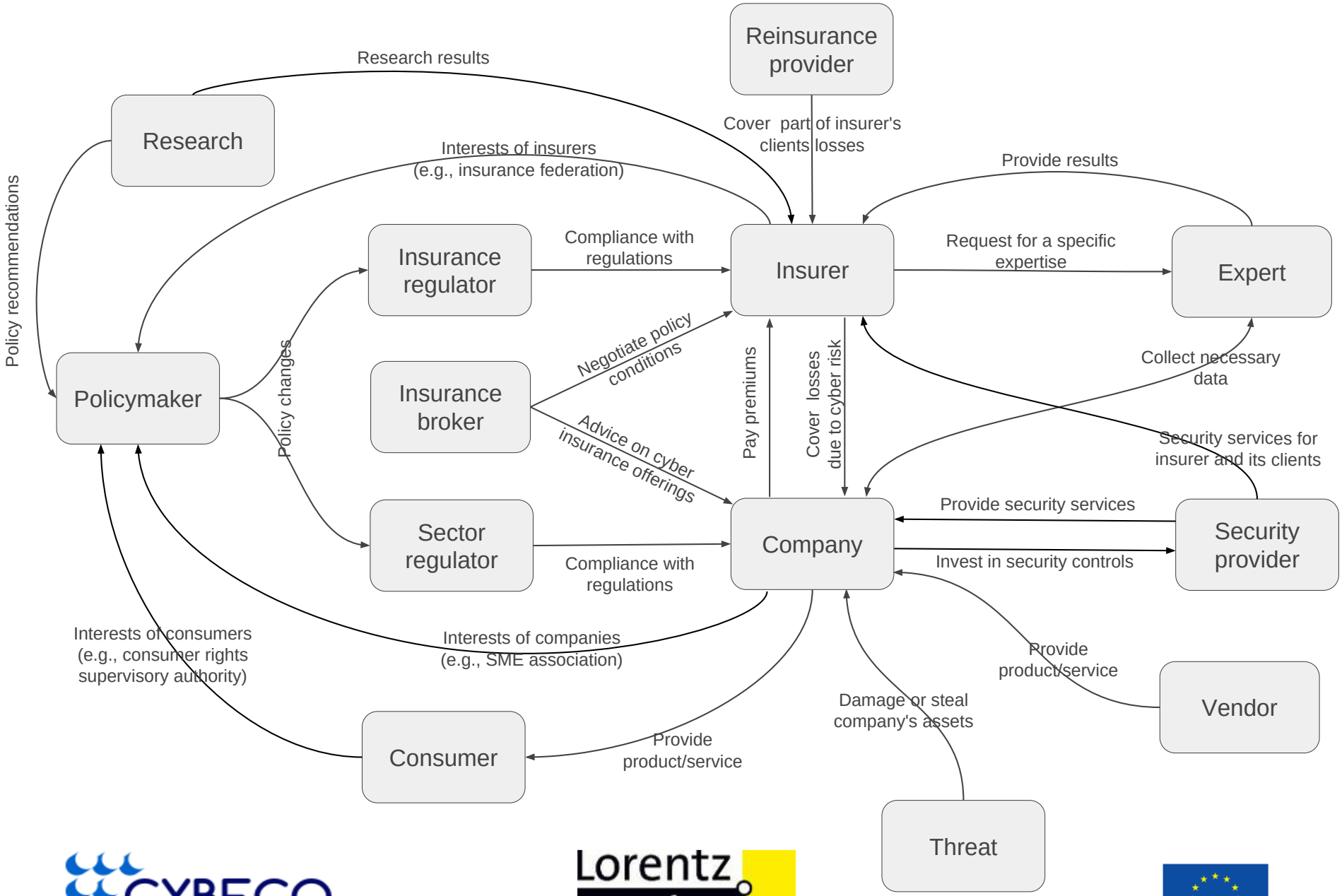
devstat

Northumbria University NEWCASTLE

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.

CYBECO
Lorentz center
Co-funded by the European Union



Co-funded by the European Union

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 measures[1]

- 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
Lorentz center
Co-funded by the European Union

INTRASOFT INTERNATIONAL

TREK development

GOBIERNO DE ESPAÑA · MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD · CSIC

CYBECO

CYBECO models for cyber security risk management

David Rios (CSIC-ICMAT)

Lorentz center

European Commission HORIZON 2020

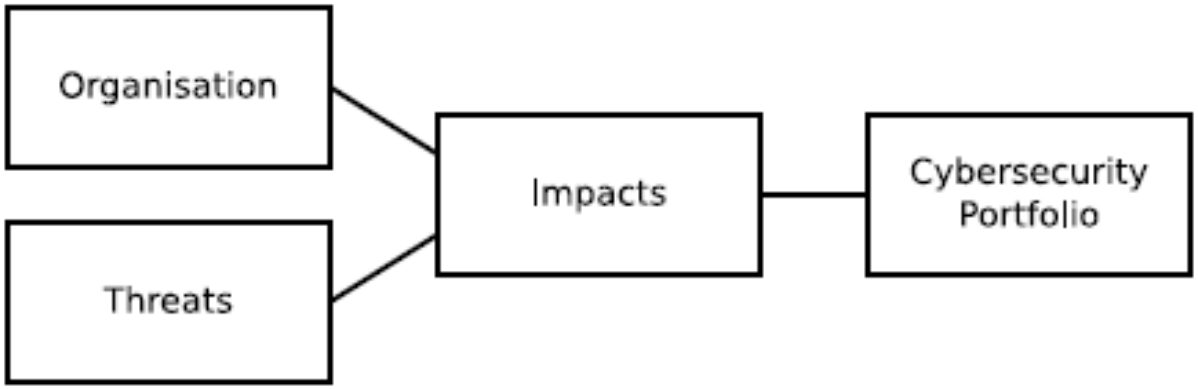
AXA TECHNOLOGY SERVICES redefining / service

TU Delft Delft University of Technology

devstat

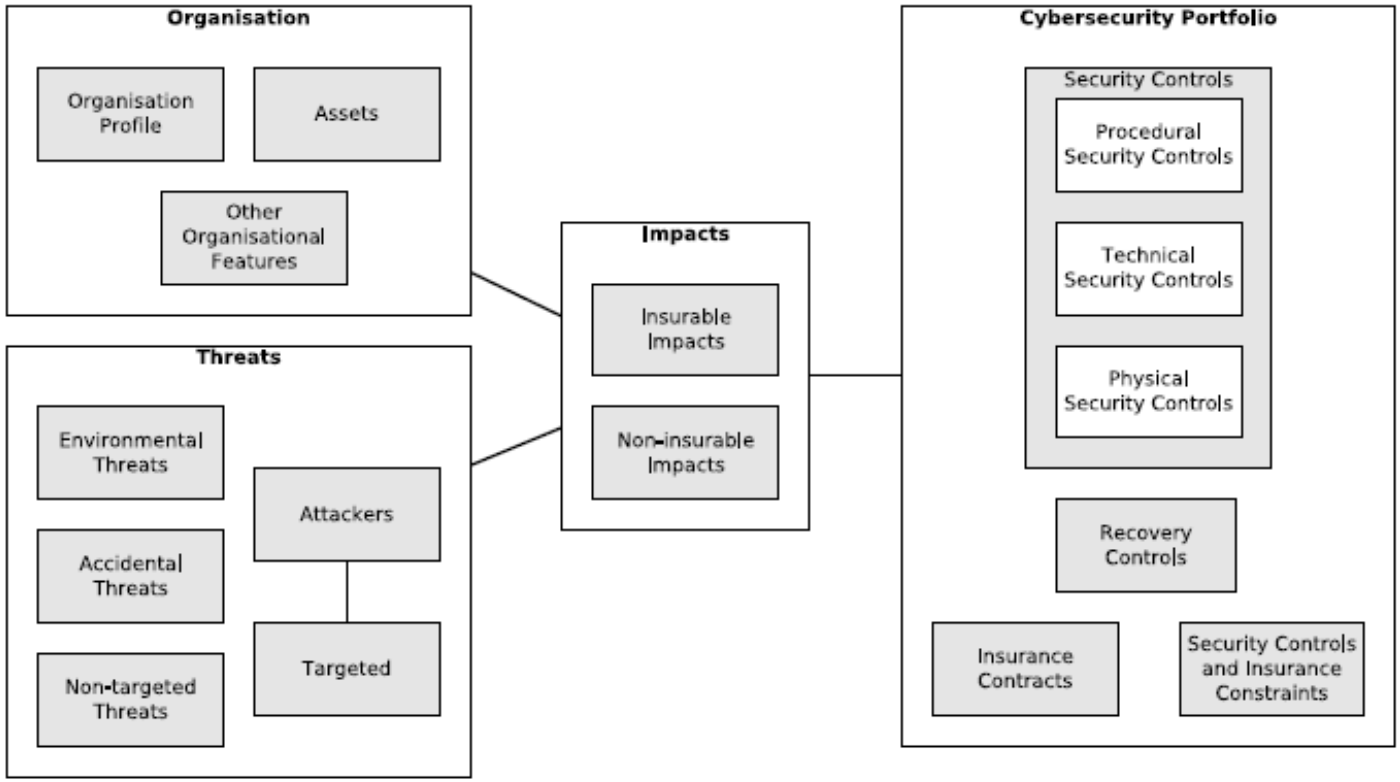
Northumbria University NEWCASTLE

Cyber security risk management



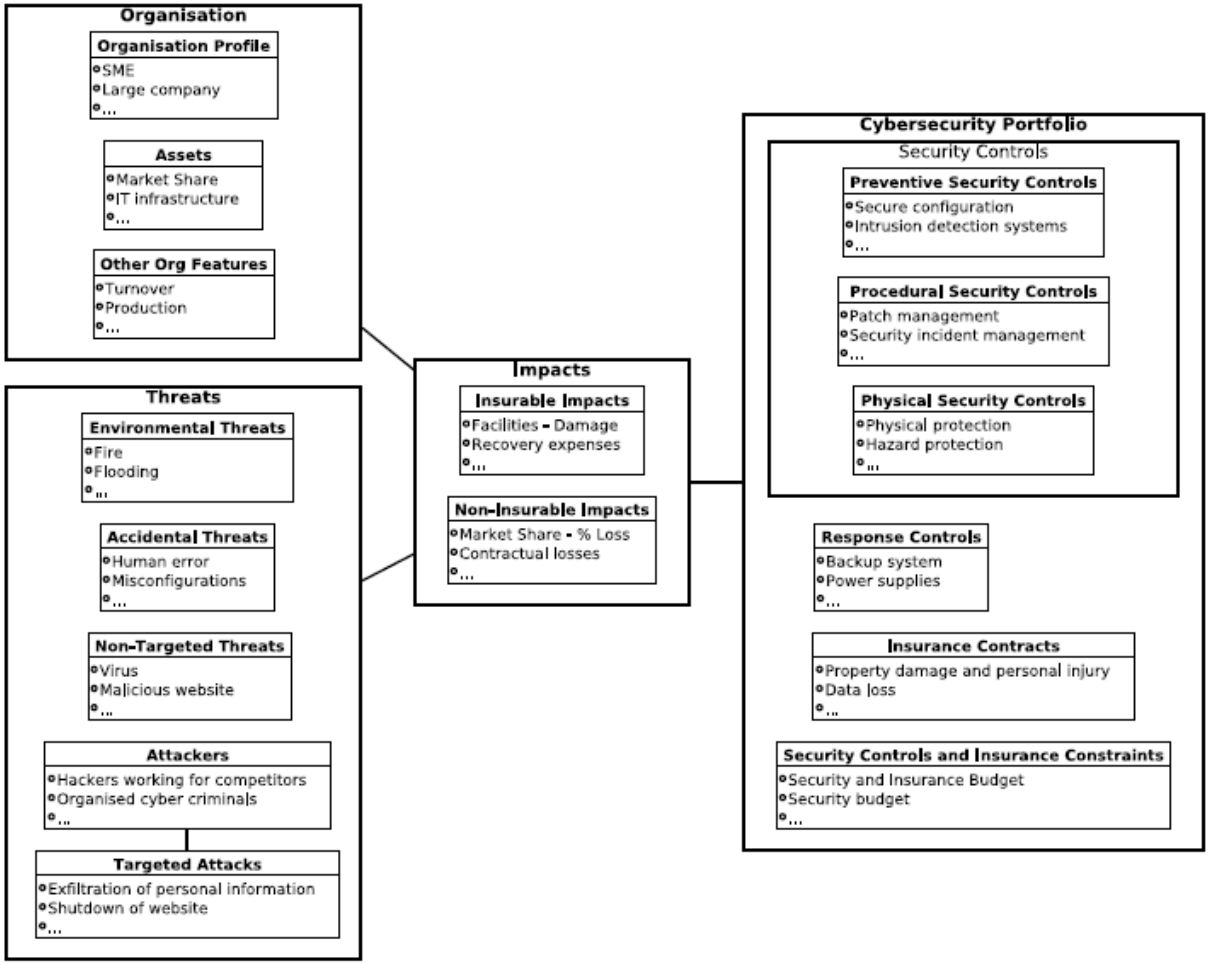
CYBECO
Lorentz center
Co-funded by the European Union

Cyber security risk management



CYBECO
Lorentz center
Co-funded by the European Union

Cyber security risk management

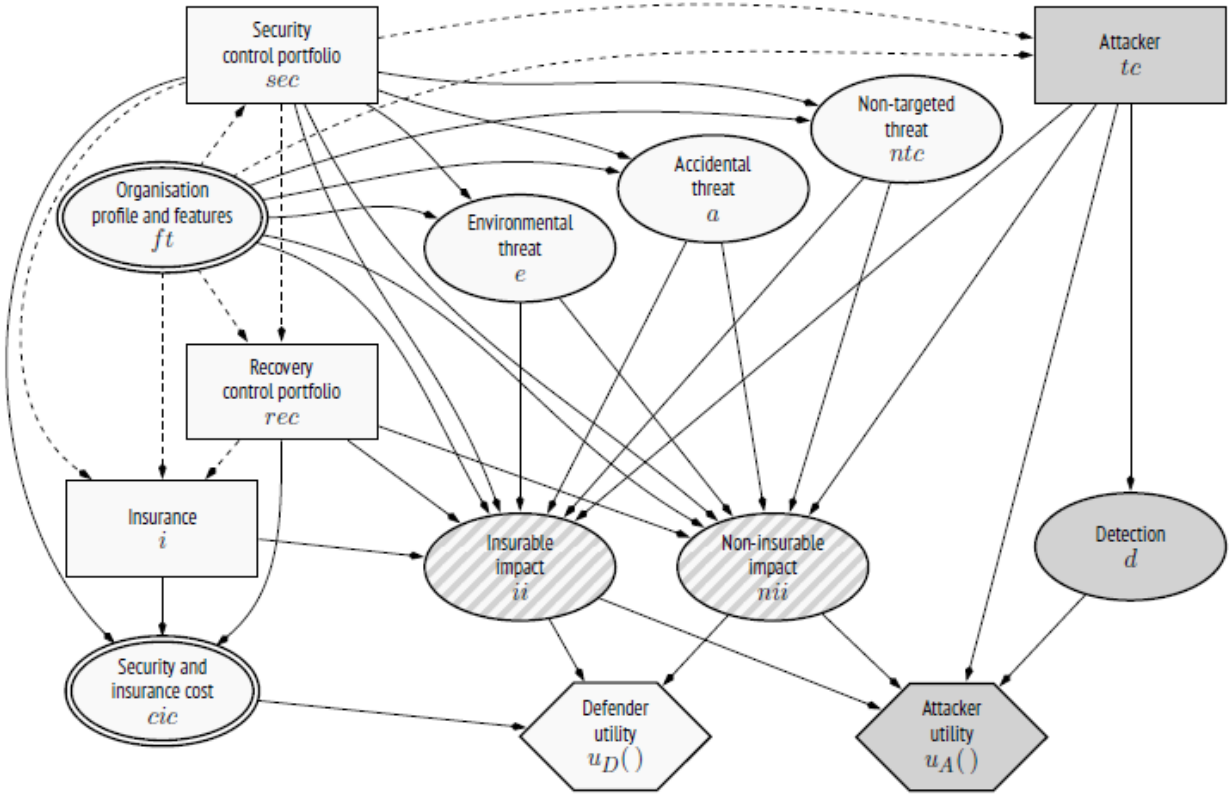


CYBECO
Lorentz center
Co-funded by the European Union

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

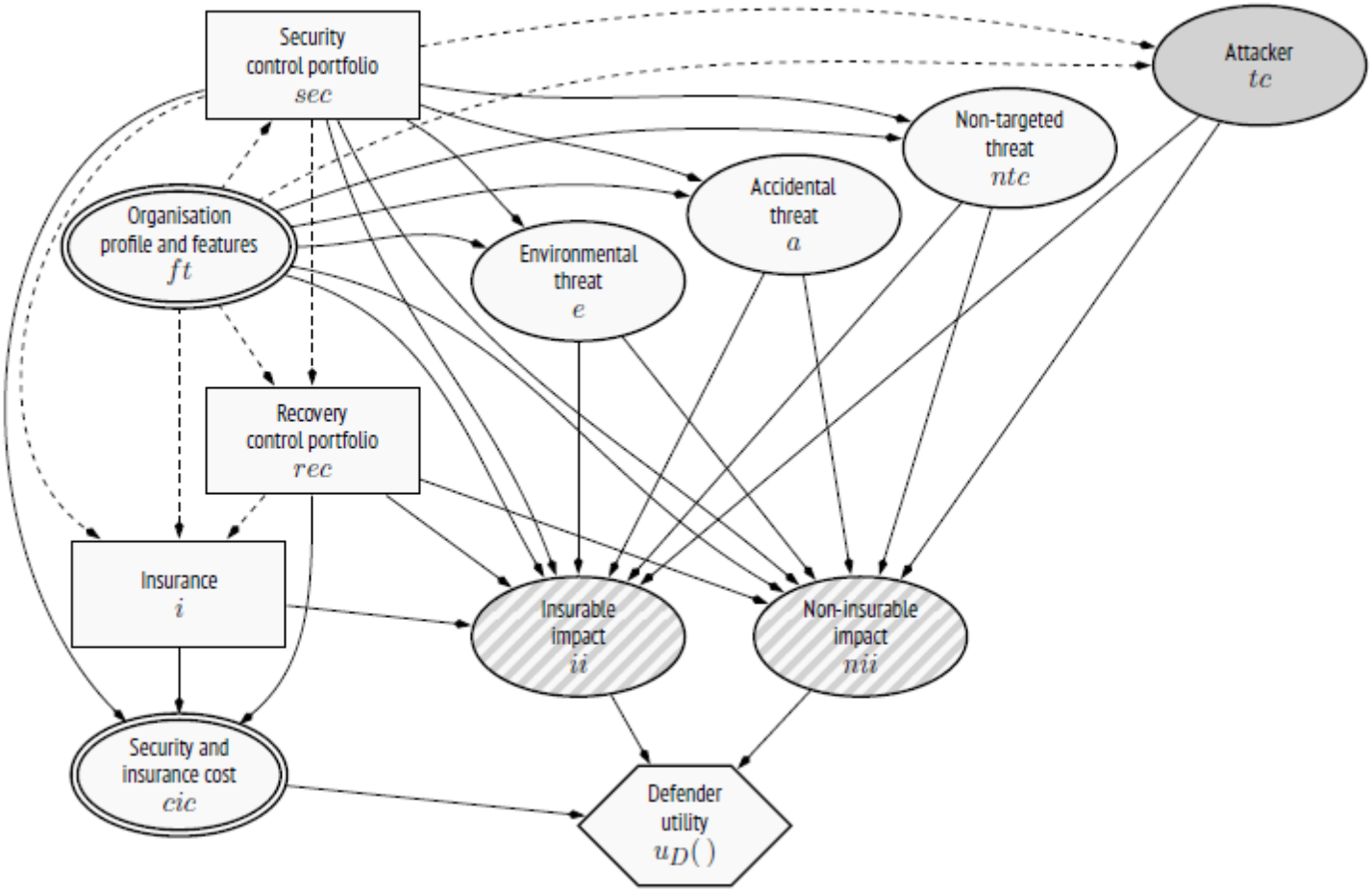


CYBECO

Lorentz center

Co-funded by the European Union

Cyber security risk management

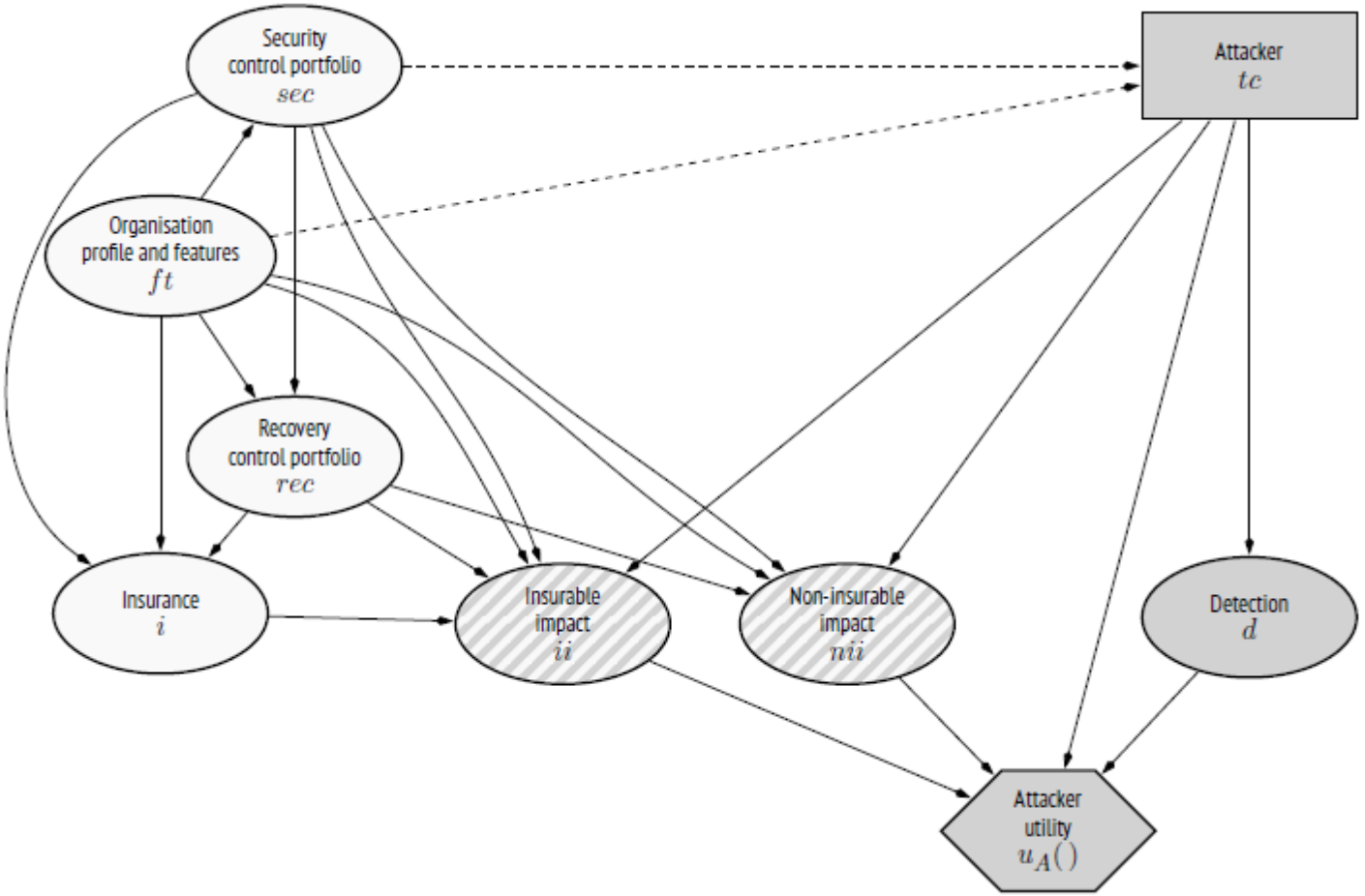


CYBECO

Lorentz center

Co-funded by the European Union

Cyber security risk management



CYBECO
Lorentz center
Co-funded by the European Union

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_{targex} and $ka_{targexf}$ 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_{recexp} 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 $sec_{secconf}$ 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 hacktivists utility node $u_H(\,)$ The cybercriminals utility node $u_K(\,)$	

CYBECO
Lorentz center
Co-funded by the European Union

Cyber security risk management

Parametrised models

CYBECO
Lorentz center
Co-funded by the European Union

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

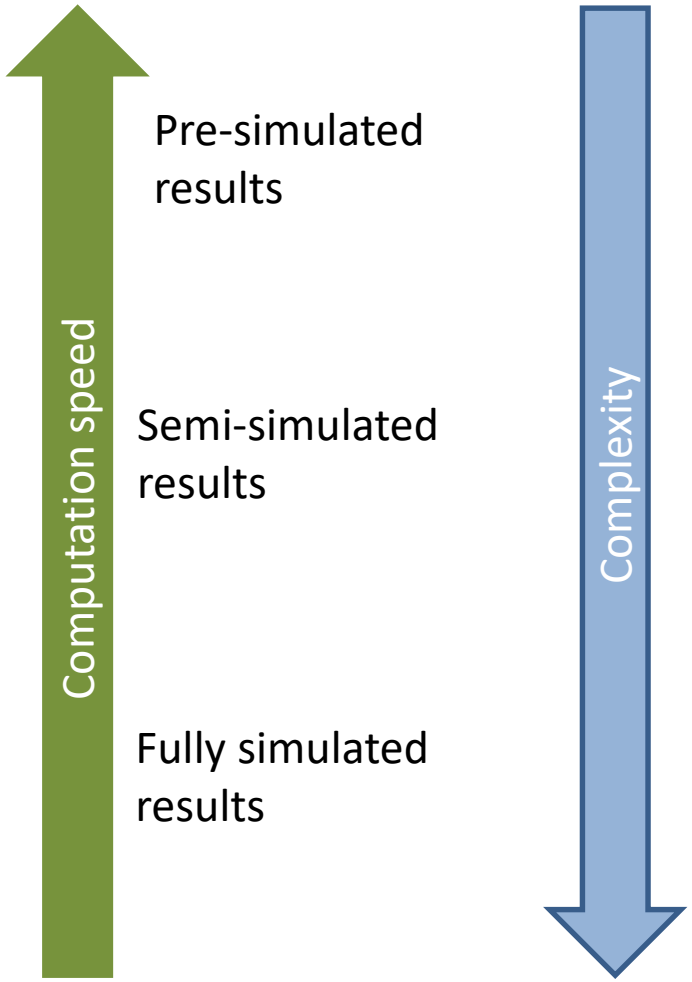
- Web-based information and consultancy tool that includes decision-support elements
  - It facilitates decisions about IT security investments
  - It is based on the results of the CYBECO research and modeling tasks
- Summarizes the most important recommendations for the design, implementation, monitoring, 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
Lorentz center
Co-funded by the European Union

CYBECO Toolbox demonstration

Presented Risk Analysis Case:

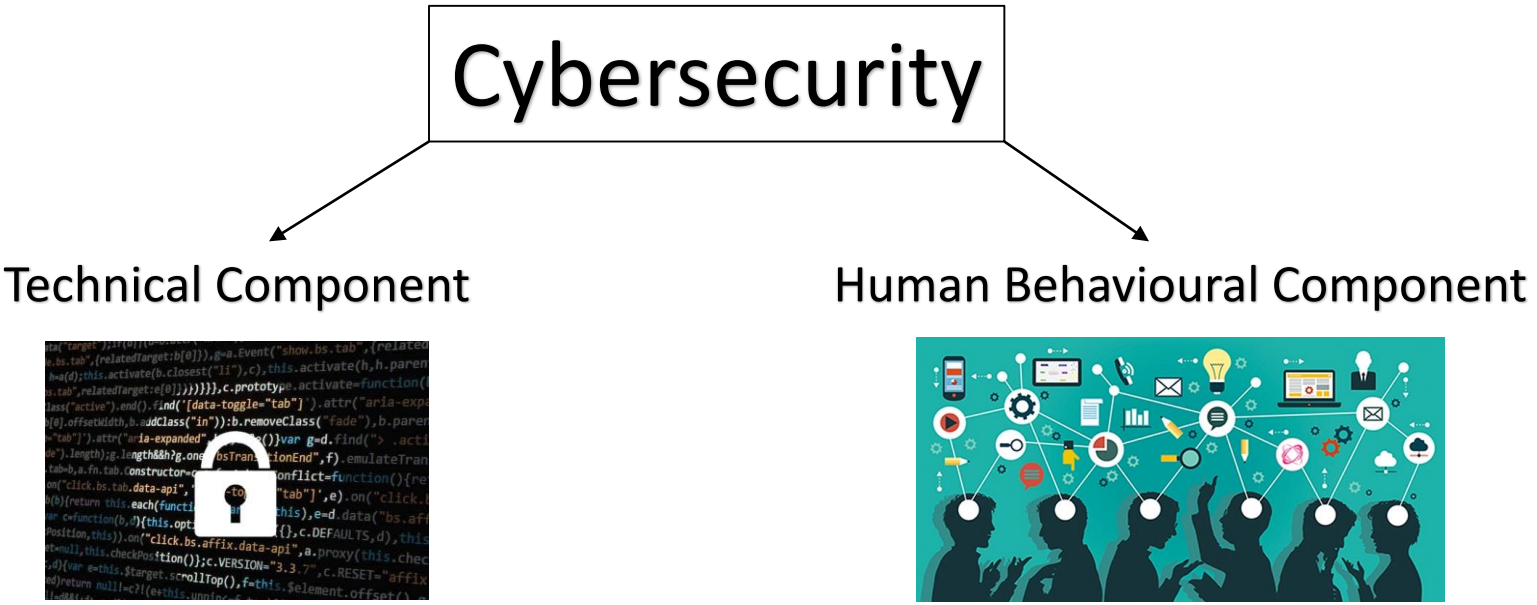
- A single **SME facing cybersecurity risks**. Goal:
  - To choose the optimal cyber security portfolio and cyber insurance product.

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

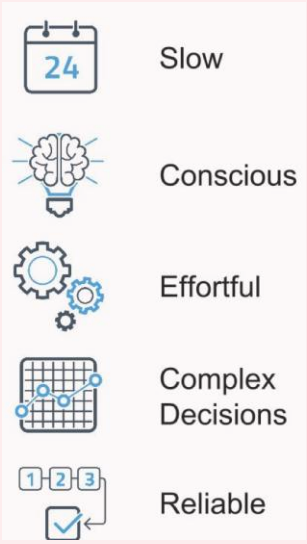


CYBECO
Lorentz center
Co-funded by the European Union

The human behavioural component…

Traditional approach

Assumes humans are always conscious, logical decision makers



BUT…

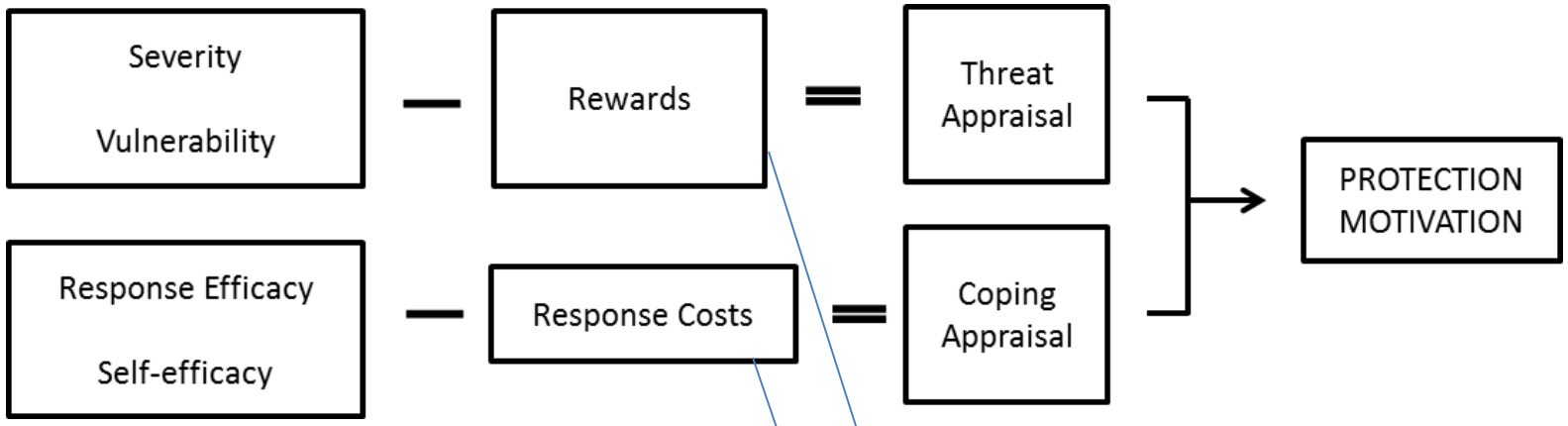
human behaviour (including decision making) is not always logical!

CYBECO
Lorentz center
Co-funded by the European Union

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

CYBECO
Lorentz center
Co-funded by the European Union

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

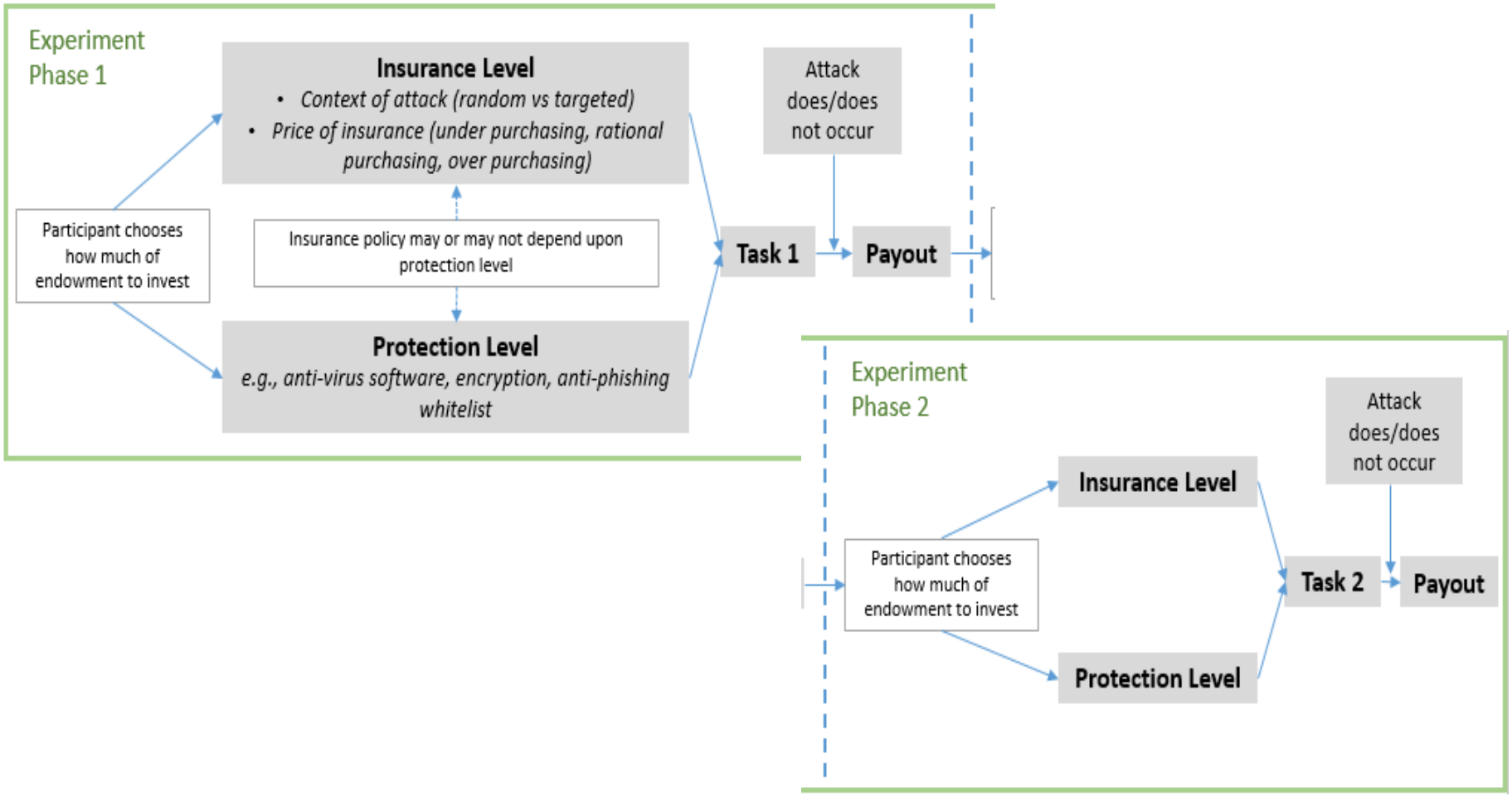
Factors	
Context of the cyberattack	The attack is random (virus) / intentional (cyber-criminal).
Price dependence	Insurance price does / does not depend on protection level
Features of the product	Base price (expected utility) Proportional price increment Non-proportion

Behavioural measures

- Protection level
- Insurance level
- Online behaviour
- PMT variables
- Risk Attitude

CYBECO
Lorentz center
Co-funded by the European Union

Experiment 1: blueprint

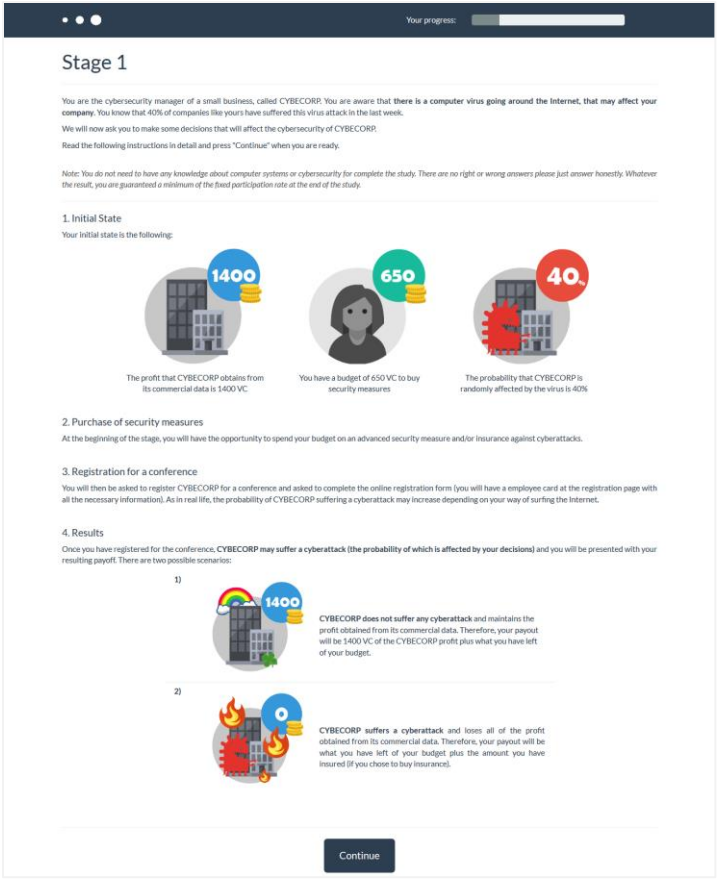


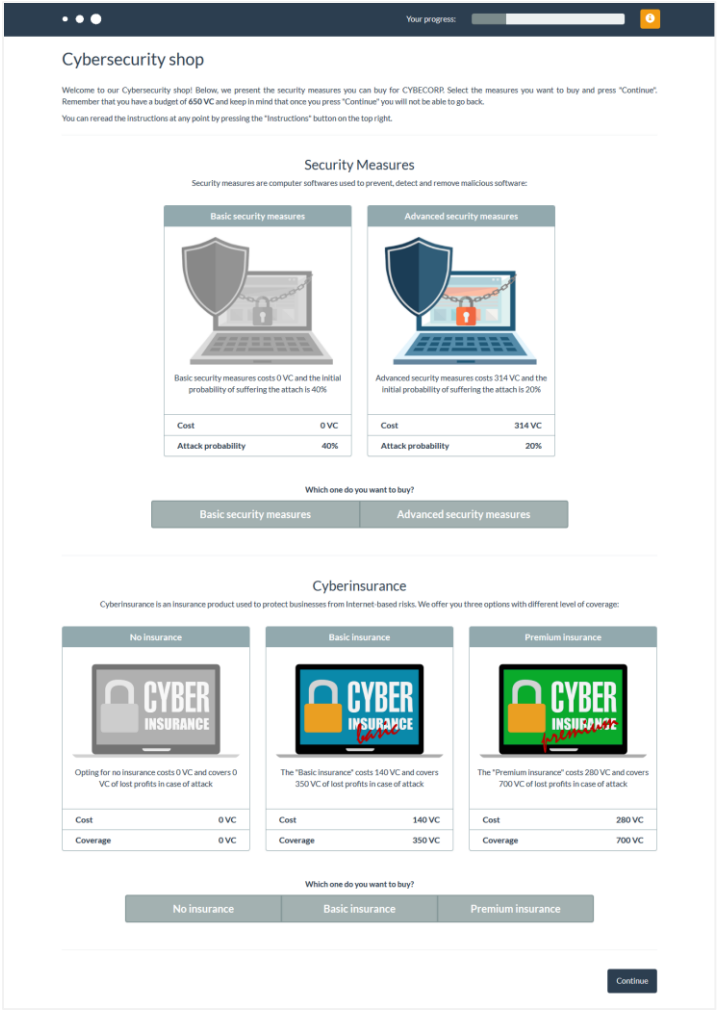
CYBECO

Lorentz center

Co-funded by the European Union

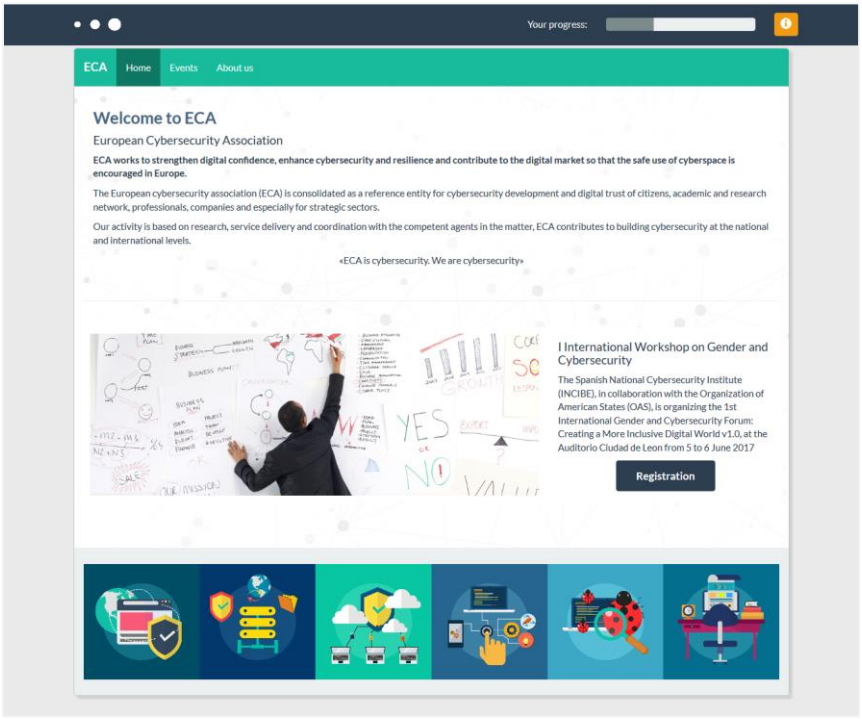
Experiment 1: purchase decision-making

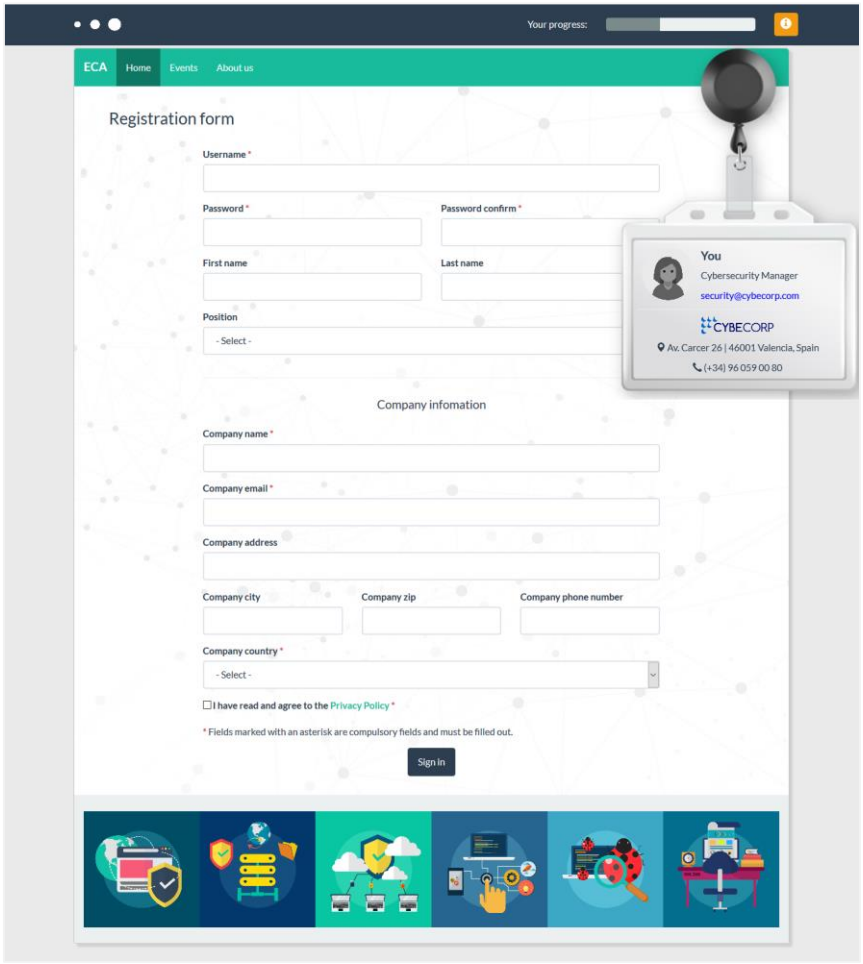




CYBECO
Lorentz center
Co-funded by the European Union

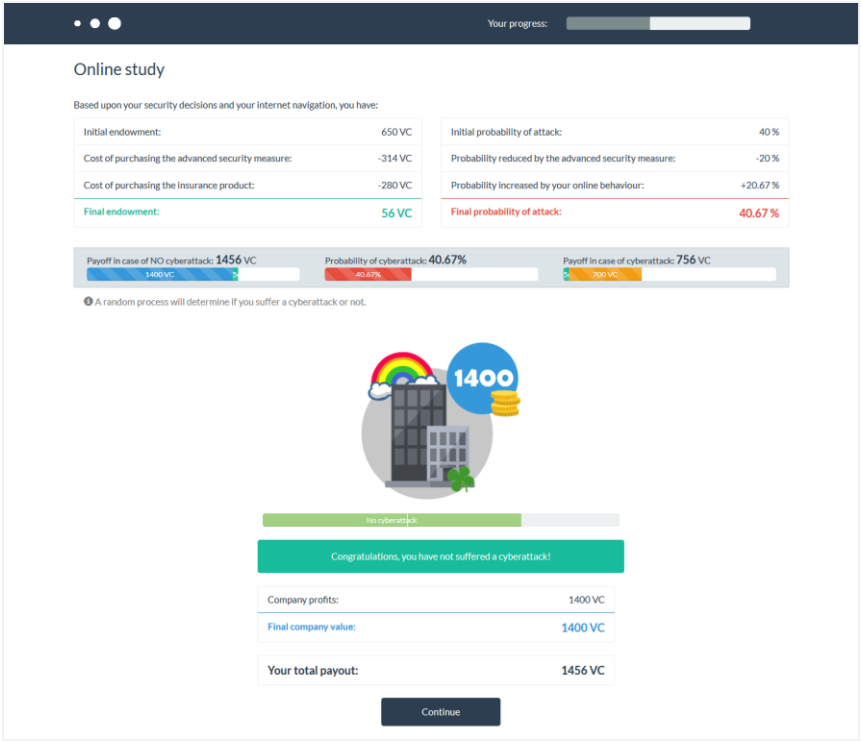
Experiment 1: online surfing

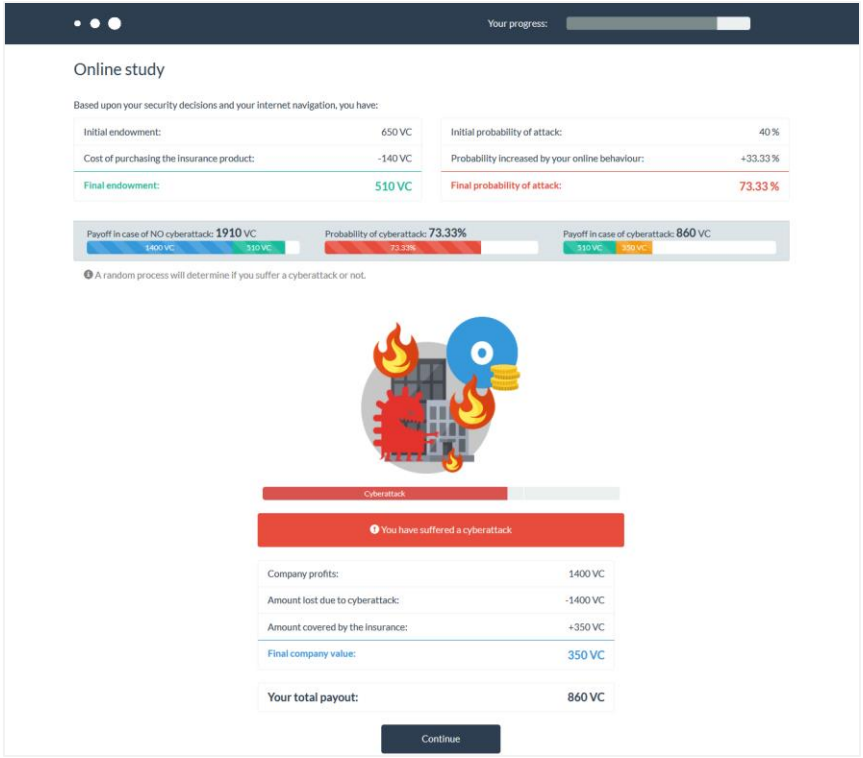




CYBECO
Lorentz center
Co-funded by the European Union

Experiment 1: to be or not to be… attacked

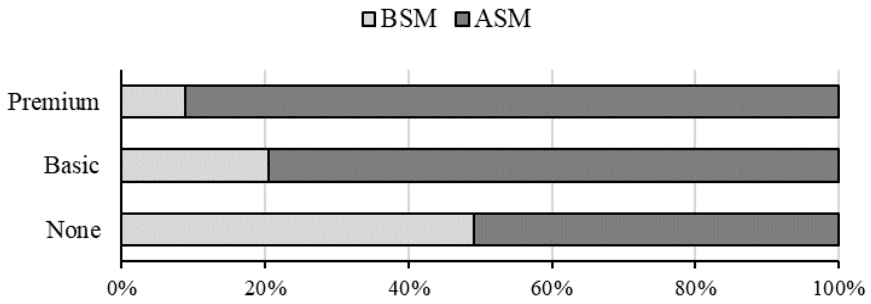




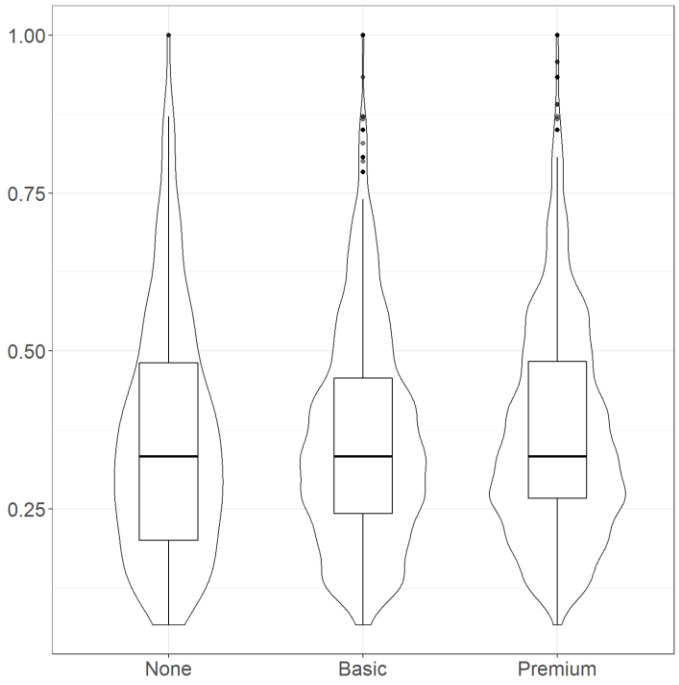
CYBECO
Lorentz center
Co-funded by the European Union

Moral hazard

- Protection and insurance are complementary

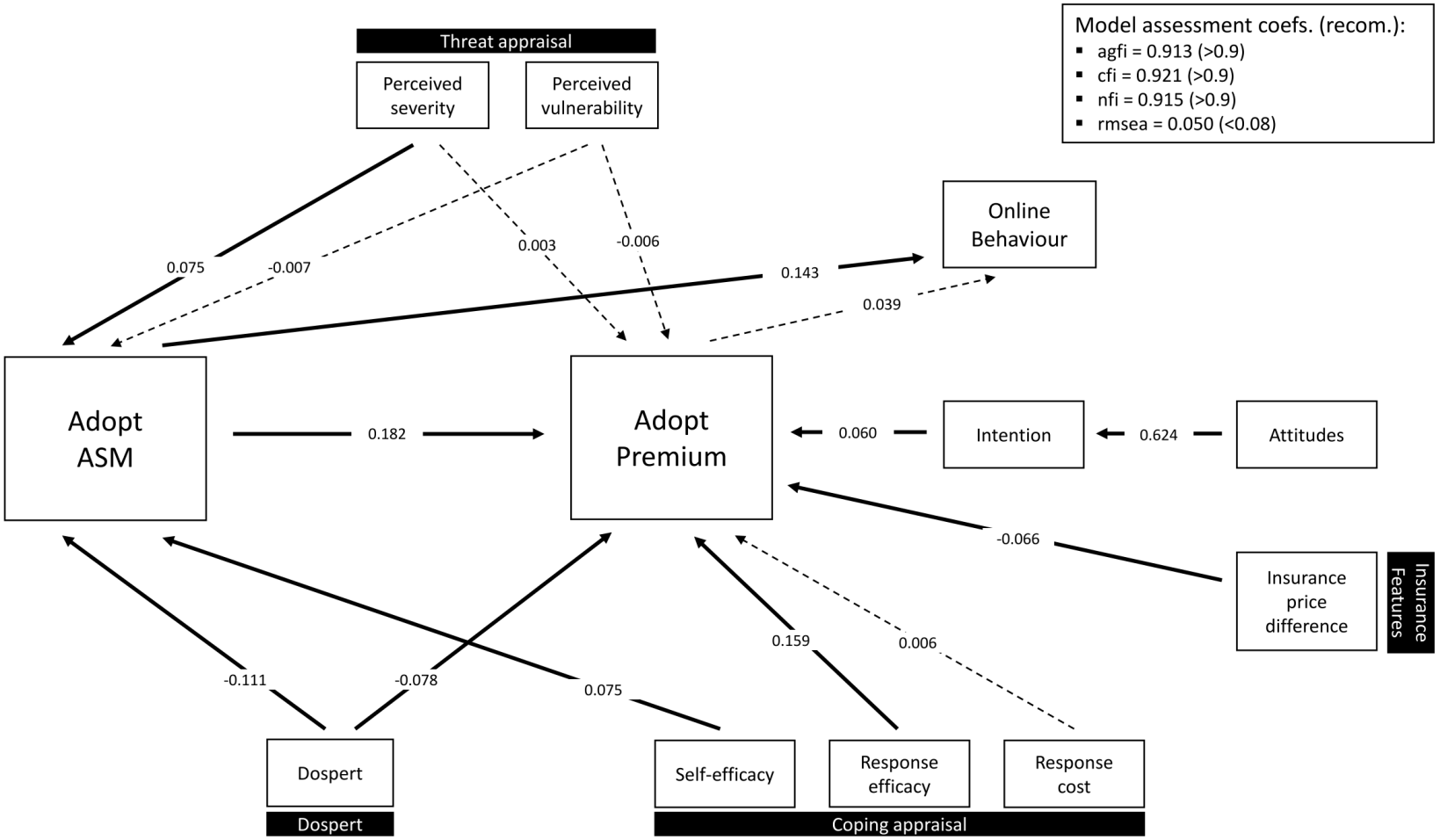


- Insurance level does not affect online behaviour



CYBECO
Lorentz center
Co-funded by the European Union

ASM and Insurance Adoption



CYBECO

Lorentz center

Co-funded by the European Union

THANK YOU

Co-funded by
the European Union