www.cybeco.eu

APRIL 2019 ISSUE 4

Introduction

Welcome to the fourth CYBECO Newsletter!

The CYBECO project is a collaboration between seven European institutions and it is funded by the EU's H2020 RIA programme with two million Euros for two years.

During the last six months of the CYBECO project, the CYBECO team has managed to make significant progress in the implementation of the project activities and to achieve all project objectives.

More specifically, the modelling framework for cybersecurity risk management has been enhanced and finalized.

The second version of the CYBECO Toolbox was developed and has been updated on the basis of expert reviews and two focus groups (experimental evaluations) that took place in London and Valencia within October. Through the expert reviews and the focus groups the usability and the end-user relevance of the Toolbox have been assessed and will be improved.

Furthermore, following the conduction of two behavioural experiments in the previous semester, a third experiment has been designed and implemented. This experiment provided relevant information about the mechanisms of creation of beliefs of defenders when exposed to intentional attackers in an adversarial context.

Also, policy recommendations have been produced on the basis of the following studies:

- An empirical study of policy usability focusing on identifying key roles and influential drivers within companies;

- A qualitative study of the decision-making process followed by SMEs for cyber insurance adoption;

- An agent-based model was developed and the effects of different cyber insurance policy options on the ecosystem were studied.

Finally, the CYBECO partnership designed and co-organized the Lorentz Cyberinsurance workshop in Leiden, Netherlands, on March 25-30, 2019.

Inside this issue:

CYBECO analyzes cybersecurity risks to advise major organizations in the selection of security countermeasures and cyber insurance.

CYBECO Results

Modelling Framework for Cybersecurity Risk Management

One of the main outputs of the CYBECO project is the Modelling Framework for Cybersecurity Risk Management.

The framework provides a comprehensive modeling of the cyber risk analysis problem, including the presence of adversarial threats and standard cyber and physical threats, as well as the use of insurance (cyber and traditional) as part of the security portfolio. Additionally, basic catalogues for assets and threats were identified to feed the CYBECO Toolbox.

A draft algorithm in R was developed and evolved, that fully simulates a problem modeled under the previous framework, to obtain the probabilities of the different events and find the optimal security investments.

The above framework and algorithm allow for the incorporation of multiple types of uncertainty and preference modeling, as they can model discrete, continuous and mixed variables. Last but not least, preference models incorporating cyber security behavioural findings were also

Cyberinsurance Ecosystem and Policy Recommendations

A model of the cybersecurity ecosystem was developed as a basis for a comparative framework to analyze key cyber security directives and regulations. The model was validated with cyber insurance professionals. Interviews were conducted with representatives of policymakers, insurance brokers, cyber insurance providers, and companies to validate the model regarding the goals of the corresponding actors and investigating possible barriers for the cyber insurance adoption from different perspectives. The discussion with stakeholders confirmed the correctness of the developed ecosystem model and provided insights on the goals of the actors present in the ecosystem.

11 in-depth interviews were conducted focusing upon unpacking the role of the company as an actor in the wider ecosystem. The findings of the study suggested that the decision-making process involves a complex ecosystem which varies across businesses. Understanding organisational structures and the various roles and responsibilities within cyber insurance ecosystem were helpful for the development of the ecosystem. The results also advised that standardisation of insurance policy coverage and implementation of best practices could be beneficial to help address mistrust in insurers from companies, and/or boost cyber insurance adoption.

In a second study, the focus was on Dutch SMEs and the decision-making process that they use to purchase cyber insurance. Based on the results of qualitative analysis of the interview transcripts and Protection-Motivation Theory a conceptual model was proposed explaining different aspects impacting a company's decision regarding the purchase of cyber insurance.

Another study focused on the development of an agent-based model simulating the effects of different cyber insurance policy options on the ecosystem. The outcomes of this study suggested that the various insurance policy options had positive but rather small influences. The combination of several policy options into a synergetic design provided results with more observable effects on the ecosystem level.

A set of policy measures supporting the cyber insurance ecosystem was also proposed based on the results of policy, empirical and modeling research studies.

Lorentz Cyberinsurance Workshop

CYBECO Workshop at Lorentz Center

The CYBECO partnership initiated and organized the workshop “Cyber Insurance and its Contribution to Cyber Risk Mitigation” at the Lorentz center in Leiden, Netherlands.

The workshop proposed built upon and reached beyond the research of the CYBECO project, bringing together perspectives from cybersecurity, risk management, psychology and mathematical modelling.

The workshop took place at the Lorentz Center in Leiden, Netherlands, March 25-29, 2019.

March 27 was an open day with participants from the cyberinsurance industry and a special session dedicated to CYBECO.

The idea of the open day event, was to share the experience of the workshop participants and exchange ideas with a broader audience regarding opportunities and challenges in cyber insurance.

Regarding the organization of the workshop, the following seminars were included in it, delivered by the noted keynote speakers:

* Cyber Insurance Market: Challenges and Trends (by Maarten van Wieren, AON);
* How do Attacks Come to Be? Empirical Insights from - Attacker Economics and Attacker Artefacts (by Luca Allodi, Eindhoven University);
* Cyber Security and Cyber Insurance (by Rainer Boehme, Inssbruck University);
* Modelling Cyber Catastrophes (by Gordon Woo, RMS);
* Responsibility and Behavioural Aspects in Cyber Security (by Lynne Coventry, University of Northumbria at Newcastle);
* Silent Cyber: Present and Future (by Eric Dallal, AIR);

* Vulnerability does not equal loss (by Eireann Leverett, Cambridge University);
* Cyber accumulation risk - Swiss Re's view on Cyber catastrophes (by Philipp Hurni, Swiss Re);
* CYBECO Project Open Day session, delivering presentations on the CYBECO approach; the results of the controlled experiment on cyber insurance decision making and demonstrating the CYBECO toolbox. (CYBECO consortium partners).

The rest of the time was spent in formulated working groups to progress around open questions relevant to the CYBECO themes that are currently attracting the interest of both research and industry, and requiring a multidisciplinary approach, starting from the following seed thematic descriptions:

* Cyber insurance market;
* Data supply for cyber insurance;
* Refined threat modelling;
* Cyber resilience and responsibilities;
* Policy Making in the Cyber insurance field.

CYBECO Workshop Outputs

CYBECO Workshop Outputs

The core outputs of the formulated working groups were the following:

1. Cyber insurance market

· The CYBECO cyber insurance ecosystem was validated;

· The group focused on the role of the broker in the cyber insurance ecosystem;

· Valuable input and feedback from the industry representatives (cyber insurers and brokers) has been provided on the group research problem;

· The group agreed to complete a report on the outcomes of the 5 days of work in Lorentz and publish it in a relevant academic journal.

2. Data supply for cyber insurance

· A compiled list of cyber data sources was made available;

· Proposals to improve the availability of cyber security data were made.

3. Refined threat modelling

· The group outlined a white paper on research needs in cyber threat modelling;

· Core issues discussed were modeling of targeted threats, models for different segments of organizations, the role of expert judgement when little data is available, dealing with social engineering attacks, the need for multiple impact models, the need to combine cyber security and cyber safety aspects.

4. Cyber resilience and responsibilities

· The group outlined a white paper on research needs in cyber resilience and its measurement;

· Specifically, further research has to be conducted on those factors affecting cyber-resilience at the individual, organizational, sector, national and global level to allow subsequently the assessment of cyber-resilience maturity;

· A better evidence base is required to understand the role of cyberinsurance in enhancing or undermining cyber resilience at these different levels;

· Enhanced scenario planning is recommended where resilience (specifically the ability to recover from cyber attacks) is highlighted.

5. Policy group

· A list of relevant policy options to promote the adoption of cyber insurance was completed;

Based on the multiple discussions, especially those held in relation to the CYBECO session and the working sessions with cyber insurance providers and brokers, the following issues were raised:

- There is still a lot of uncertainty around the cyber insurance product design, especially in relation to pricing, which is mainly driven by the market process with little modelling efforts;

- The lack of data available so far may be countered through expert judgement, which needs to be taken into account properly;

- Targeted threats are increasingly important. Game theoretic models are still not much in use, mainly because they are unstable;

- Besides attacks, we should recall that cyber insurers also refer to reliability issues. Cyber insurance is about cyber safety and cyber security, which need to be integrated into the models;

- The CYBECO cyber insurance model was deemed largely relevant;

- The CYBECO toolbox was considered relevant by several of the members of the cyber insurance sector present.

The results of the workshop suggest that the approach undertaken by the CYBECO project is relevant and timely.

Materials from the workshop are available at https://svn.tbm.tudelft.nl/TREsPASS/CYBECO/Lorentz.

CYBECO Partners

The project is a collaboration between seven European institutions, namely TREK Development S.A. from Greece, Instituto de Ciencias Matemáticas (ICMAT – CSIC) from Spain, Intrasoft International S.A. (INTRASOFT) from Luxembourg, Devstat Servicios de Consultoría Estadística S.L. (DEVSTAT) from Spain, AXA Technology Services (AXA) from France, Technische Universiteit Delft (TU DELFT) from Netherlands and the University of Northumbria at Newcastle (UNN) from the United Kingdom.

CYBECO partners combine different types of expertise in the fields of mathematics, risk management, behavioural sciences, software engineering and technology policy.

TREK DEVELOPMENT SA, Greece

AGENCIA ESTATAL CONSEJO SUPERIOR DEINVESTIGACIONES CIENTIFICAS - INSTITUTO DE CIENCIAS MATEMATICAS, Spain

INTRASOFT International SA, Luxembourg

DEVSTAT SERVICIOS DE CONSULTORIA ESTADISTICA SL, Spain

AXA TECHNOLOGY SERVICES, France

TECHNISCHE UNIVERSITEIT DELFT, Netherlands

UNIVERSITY OF NORTHUMBRIA AT NEWCASTLE, United Kingdom

This eNewsletter has been developed with the financial assistance of the European Union under the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement 740920. The contents of this eNewsletter are the sole responsibility of the CYBECO project partners and can under no circumstances be regarded as reflecting the position of the European Union or of the Programme's management structures.