CYBECO

Supporting Cyberinsurance from a Behavioural Choice Perspective

D8.5: Organization of final event

Due date: M24

Abstract:
This deliverable describes the rationale and output of the organization of the final CYBECO event. It was held as a Lorentz workshop entitled *Cyber Insurance and Its Contribution to the Mitigation of Cyber Risk.*

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)	

Document Status

Document Title	Organization of final event
Version	2.0
Work Package	8
Deliverable #	8.5
Prepared by	D. Rios Insua, A. Couce Vieira (CSIC)
Contributors	Wolter Pieters, Kate Labunets (TUDELFT), Pam Briggs, Dawn Branley-Bell (UNN), José Vila (DEVSTAT), Nikos Vassileiadis (TREK), Vassilis Chatzigiannakis, Sofia Tsekeridou (INTRASOFT), Deepak Subramanian (AXA)
Checked by	TREK, INTRASOFT
Approved by	TREK
Date	25/4/2019
Confidentiality	PU

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	1.0	April 5, 2019
Second draft after peer-review	2.0	April 23, 2019
Final version after quality check	3.0	April 25, 2019

Table of Contents

1 Introduction 5
2 Workshop rationale 6
3 Background 7
4 Event schedule and logistics 11
5 Event output 14
6 Discussion 16
Appendix A. Event Program 17
Appendix B. Event Photos 19

1 Introduction

The rise in both the scale and severity of recent cyberattacks demands new thinking about cybersecurity risk and the mitigation and transfer of that risk as the CYBECO project promotes. Cyber insurance is one potential way to manage risk by transferring damage liability, but the cyber insurance market is immature and the understanding and actuarial knowledge of cyber-risk is currently underdeveloped. Because of its adversarial nature and worldwide reach, cyber risk is different from risks in other domains, meaning that a sustainable solution requires new ways of analysing those risks and offering insurance products that provide incentives to improve security within the ecosystem. These innovations can only be achieved by the collaboration of mathematicians, computer scientists, economists, behavioural scientists, the insurance and cyber security industry, and policy experts.

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 project focuses mainly on choice behaviour, by developing a framework for analysing adversarial risks, identifying insurance selection behaviour, and building a tool for supporting cyber insurance offering and purchase decisions. The broader central question was under which conditions a healthy cyber insurance market can contribute to the reduction of the impact of cyber threats. We aimed at developing an interdisciplinary perspective further by building a new community of individuals, well beyond the scope of CYBECO, who can help us understand the highly complex interplay of social, economic, information sharing and technical factors that underpin a sustainable model of cyber insurance. To this end, we facilitated talks on key topics as well as workshop discussions on the cyber insurance market, data supply, refined threat modelling and cyber resilience. The integration of perspectives and extended community would provide a basis for new research projects as well as practical impact. The scientific organizers were:
Pamela Briggs (Newcastle, UK)
Katsiaryna Labunets (Delft, Netherlands)
Wolter Pieters (Delft, Netherlands)
David Rios Insua (Madrid, Spain)
Maarten van Wieren (Rotterdam, Netherlands)
whereas the workshop coordinator was Maria Krebbers (Lorentz Center, Netherlands). The workshop took place at the Lorentz Center in Leiden, Netherlands, March 25th-29th, 2019. March 27th was an open day with participants from the cyberinsurance industry and a special session dedicated to CYBECO. The webpage was
http://www.lorentzcenter.nl/lc/web/2019/1096/info.php3?wsid=1096&venue=Oort

2 Workshop rationale

Major cyber-attacks make the news several times a year. In addition, many smaller companies and individuals suffer losses because of cyber incidents. As digitization pervades more and more of society, an increase in the scale and impact of cyber-attacks is also observed, indicating that systemic risk is also growing. Nations around the globe understand the importance of engaging in this problem. Both privately as well as publicly, collaboration in cyber risk research, security, management, policy and transfer are aimed at keeping society secure. In this, economic aspects play a major role, since investments in mitigating cyber risk require careful balancing against opportunity losses to create value while improving efficient risk mitigation against a background of rapidly changing technological reality is far from easy.

Historically, risk gets transferred along value chains through contractual agreements, mostly leading to accumulation of the risk with the smaller parties unable to actually bear the risk, contributing to its systemicity. Under such conditions, insurance can lead to explicit, rational and therefore a sustainable transfer of risk to capable parties, typically reducing systemic risk. In addition, through their accumulation of knowledge, insurers coax markets into reducing risks where economically viable. However, for cyber risk, the role of insurance is only still developing, due to lack of historical experience, tremendously complex systems, associated risks and seemingly ever-changing characteristics of cyber risk, as well as poorly understood systemic risk components. This means that there is a lack of clear guidelines on how cyber insurance should be implemented to contribute to social welfare by improving the overall security. In this regard, the main goal of our workshop is to promote the study of conditions under which cyber insurance can be effectively used for cyber security risk management.

The complexity of cyber risk combined with that of the insurance value chain implies that overcoming the above challenges requires a multidisciplinary approach. On the one hand, there are disciplines like information technology and cyber security that need to be combined with legal, psychological and business management perspectives. On the other hand, there is the dynamics of capital, regulations, actuarial sciences, analytics, underwriting and marketing that need to be combined to make cyber insurance work to its full potential. Our Lorentz Center workshop also aimed at creating a community of academics and industry experts capable of overcoming the multidisciplinary challenges in understanding cyber risk, its transfer and the relation to systemic risk serving as seed for future interdisciplinary projects in the field. In this way, we aim at contributing to the sustainable transfer of cyber risk.

3 Background

We present now the relevant disciplinary viewpoints that we aimed at integrating into our workshop.

The risk management perspective

As with any other type of risk, organizations can deal with cyber risk in four ways: (1) avoidance, (2) mitigation (i.e. cyber security), (3) transfer (including insurance) or (4) acceptance (implying the requirement of provisional capital buffers). As with other types of risk, the exact mix of these four treatments can determine the success or failure of organizations. Because cyber risk is complex and multifaceted, economic considerations determine only in part how is it treated, with psychological, organizational as well as governance factors typically being dominant factors.

Most organizations with a sense of urgency around managing cyber risk initially focus on mitigation through cyber security. Only as it becomes apparent that perfect security is unattainable will most organizations realise the importance of wider measures including third-party cyber risk management, cyber insurance and strategically avoiding new risks by delaying business innovation. For the purpose of economically balancing the above, some form of cyber risk quantification is indispensable. From a scientific point of view, the main challenge lays in identifying optimal investment allocations. For large organizations, cyber risk transfer often includes internal forms of insurance, e.g. through a captive, increasing the need for an economic perspective.

The cyber security perspective

Quantifying the impact of cyber security is notoriously hard. Standard statistical approaches do not work because of lacking (breach) data, foremost due to unknown breaches. More sophisticated approaches that observe the behaviour of various risk drivers typically require making assumptions combined with Bayesian methods. The fact that various cyber security controls are far from independent in their effectiveness further complicates this. In many cases, people responsible for these controls do not see the added value in obtaining metrics and choose to focus their efforts on keeping cyber abuse at bay.

Cyber insurance can play an important role in this. Based on the marketplace overview that insurers and brokers have, they can more easily challenge the larger insurance prospects. For large organizations, obtaining insurance will likely entail interaction between relevant stakeholders, leading to a more comprehensive perspective on cyber risk for all parties involved. This leads to better understanding of non-technical cyber security measures as well as the value of cyber risk measurement and management. For smaller organizations, the insurance industry increasingly tends to include cyber security services as precaution benefitting both the insurer and the insured.

However, there is also the possibility that due to competitive forces and insufficient regulatory oversight, insurers compete on price and selection risk in a race to gain market share. Although this may appear as irrational, there is some logic in it, as the value of obtaining data through underwriting and claims is of strategic importance for insurers to thrive in this market in the long run. Consequently, we see the emergence of professional data and analytics firms that specialize in the collection and analysis of cyber risk related data.

The human factors and psychology perspective

There are a number of human and behavioural factors that are likely to influence the uptake and appropriate governance of cyber insurance. Firstly, we know that risk perceptions around cyber threats are not always accurate and that systematic biases are at play wherein many individuals with responsibility for sensitive company assets underestimate the likelihood of a cyber-attack. The situation is compounded by a general lack of expertise, particularly in smaller companies, where they may not fully appreciate the risk to their business as a result of not having secured their data.

Even where the risks are fully understood, companies may underinvest in cyber insurance for a range of reasons. The policies may not be 'usable' and may require the disclosure of sensitive information around previous breaches and suspect incidents; or organisations may simply not have the time and resources available to understand their particular vulnerabilities and so they may struggle to understand the best insurance coverage for their enterprise.

Such attitudes and behaviours tap into an extensive psychological literature around systematic biases in the judgement of risk (see for a summary of these) and the ways and individual threats are weighed against protective measures (e.g. protection-motivation theory). We know that there are ways to influence decision-making so that people become more or less risk-averse and some of these ‘nudging’ techniques will be considered in the seminar.

The mathematical modelling perspective

Numerous frameworks have been developed to screen cyber security risks and support cyber risk management resource allocation, including CRAMM, ISO 27005, MAGERIT or SP 800-30. Similarly, several compliance and control assessment frameworks, like ISO 27001, Common Criteria, or CCM provide guidance on the implementation of cyber security best practices. These frameworks cover detailed security controls suggested for protecting an organisation's assets against the risks to which they are exposed. They have virtues, particularly their extensive catalogues of threats, assets and controls providing detailed guidelines for the protection of digital assets. Even though, much remains to be done regarding cyber security risk analysis from a mathematical point of view. Indeed, a detailed study of the main methodologies for cyber security risk management reveals that they often rely on risk matrices, which present well documented shortcomings. Compared to more stringent methods, the qualitative ratings in risk matrices (likelihood, severity, and risk) are more prone to ambiguity and subjective interpretation. Moreover, with counted exceptions like ISI-HMG, these methodologies do not explicitly take into account the intentionality of some threats. The likelihood of a threat or attack is often elicited analysing its frequency over a certain period. However, the intentionality and strategic behaviour of some cyber threats is a key component when it comes to analyse whether a threat would target the system and, if so, how often, a fact frequently forgotten. Thus, ICT owners may obtain unsatisfactory results about risk prioritization and the measures they should implement. In this context, cyber insurance, as mentioned above, is emerging as a complementary way for dealing with cyber risks through risk transfer.

Numerous mathematical modelling challenges await concerning cyber risk and cyber insurance especially if we take into account the availability of limited amounts of data. Some of them include the development of more solid risk quantification models beyond risk matrices. These models should incorporate:

- multiple impacts;
- likelihood models that combine limited data with expert judgement and consider that some threats may be intentional;
- the development of generic preference and likelihood models in cyber risk;
- the development of methods that facilitate optimal security resource allocation (countermeasures and cyber insurance);
- the development of parametric cyber insurance products that facilitate their design and market segmentation;
- the inclusion of cyber re-insurance issues.

The economic perspective

The impact of cyber risk on society is huge. Some estimates point in the direction of 0.7% of global GDP with the impact of a single, large-scale attack with systemic fallout exceeding that of natural disasters or (conventional) terrorist attacks. It is therefore no surprise that cyber risk structurally reappears in top-10 lists and that about 0.1% of global GDP is annually spent on cyber security. This means that the cyber security spend is actually quite close already to its expected impact, implying that we are getting close to levels beyond which cyber security investments exceed their benefits. And yet, only about 2% of total cyber security spend is used for insurance, implying that there is significant room for economic improvement through such instruments.

On the other hand, constraints in the market on the limits available for cyber insurance coverage (currently around $200mn only for the largest companies) indicate that insurance companies are perhaps not yet entirely comfortable with the risk levels they currently underwrite. And this makes perfect sense. Details of business operations and cyber security controls matter tremendously and yet it is simply too costly as well as undesirable from the insured’s perspective to let the insurer perform a full risk assessment. It implies that better standards and regulations might be needed not only for the insurers but also for other organizations.

Another viable approach may be to develop wholly new business models around risk management. It might, for instance, be conceivable that insurance companies will provide attractively priced cover for all clients of a cyber security supplier closely monitored to deliver services against high standards. Another example is that large firms will require third parties to work on the cyberspace they provide, follow training and consequently become part of the cyber insurance cover for that large firm. Similarly, emerging cyber communities, such as smart cities and smart harbors, may turn out also to create rational structures for sharing and managing cyber risk within that community.

4 Event schedule and logistics

The program is available at http://www.lorentzcenter.nl/lc/web/2019/1096/program.php3?wsid=1096&venue=Oort with the open day information available at http://homepage.tudelft.nl/6d93v/CI-open-day/index.html. There were 51 participants during the whole workshop to whom 13 participants from the cyberinsurance industry joined during the open day, totalling 64 participants.

The following seminars were included in the workshop, 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:

1. **Cyber insurance market**

The cyber insurance market involves different players (insurers, brokers, insured companies, regulators, third-party vendors, security services providers...) who create a complex ecosystem. All these parties have their perspectives and goals which must be taken into account for the effective operation of cyber insurance. Therefore, we need to study a model for the cyber insurance ecosystem including existing relationships between parties and their goals from various perspectives (economic, law, ethical, risk management).

Another open problem in relation with the cyber insurance market is the lack of trust between insurers and insured companies, which results in a limited understanding of companies' level of risk leading to an inadequate level of coverage provided by insurers. This issue demands better standards and regulation to help establish transparent and efficient relations within the cyber insurance ecosystem. An alternative approach could be the development of new business models where, for example, a cyber insurer collaborates with a cyber security service provider by selling insurance coverage together with security services.

It is also relevant to determine what is the 'correct' behaviour for the ecosystem and how cyber insurance affects the behaviour of insured companies and the ecosystem in general. Then, we could consider relevant behaviour techniques for cyber insurance to nudge or incentivize ecosystem players towards the correct decision-making.

The cyber insurance market is a complex topic and could benefit from the contribution of different perspectives like security certification approaches from cyber security, new business models from business development, financial models from economics, behavioural theories from psychology, etc. The clear understanding of the cyber insurance ecosystem and best behaviour for its participants could reveal the central conditions for the use of cyber insurance. Also overcoming such barrier as the lack of trust between cyber insurance players, could provide a green light to the adoption of cyber insurance.

2. Data supply for cyber insurance

A well-known problem for cyber insurance is the lack of (historical) data about security incidents. Having those data is one of the critical conditions for the successful operation of cyber insurance. In May 2018, the new General Data Protection Regulation (GDPR) came into force. GDPR requires that all companies that work with personal data of EU citizens have to report about any data breach affecting these data. Therefore, data protection authorities will be collecting a significant amount of information about security incidents. There is an ongoing discussion within the cybersecurity community about providing access to these data for interested parties. With these data, cyber insurers could build better actuarial models of cyber risks or use different techniques like predictive models or machine learning classification. However, such access mechanism is an open problem which requires a contribution from different perspectives as it involves the interests of various parties (like government, companies, individuals). The behavioural and economic perspectives feed into the willingness to share the data. To enable meaningful interpretation, contributing to better insurance and reduction of systemic risk, knowledge from cyber security (what data to look for), risk management (linking data to risk), and modelling (correlating data) needs to be combined.

3. Refined threat modelling

Existing approaches like STRIDE, CORAS, attack trees, etc. — help to identify threats and describe how cyber-attacks may develop. The benefit of these methods is that they can be used to model different types of attackers and some behavioural aspects in terms of likelihood. However, they poorly incorporate the dynamic behaviour of parties and the economic perspective, i.e. cyber security and cyber insurance investments and their effect. In this regard, several research works have proposed economic and financial models to determine the optimal amount of investment in information systems security. Moreover, there is a significant inconsistency between existing models concerning how they address the main obstacles:

interdependent security, correlated risk, and information asymmetries. The primary challenge in addressing these obstacles is to develop a holistic representation of cyber threat agents and their behaviour, which requires a careful combination of economic and mathematical modelling approaches while accounting for behavioural aspects. Such a threat modelling approach is a key condition for understanding how cyber insurance contributes to cyber security risk management, as attackers play a crucial role in the threat events that we are protecting against.

4. Cyber resilience and responsibilities

With increasing digital connectivity we become more interdependent on one another, increasing the scale and effect of cyber-attacks. Therefore, a significant challenge for cyber society is to address the growing systemic risk by improving cyber resilience and defining the responsibilities of the participants in the ecosystem. An open question in this respect is to investigate how cyber insurance can contribute to the realization of cyber resilience and fulfilment of responsibilities, and what kind of implications it creates for the ecosystem. Therefore, we need to have a contribution from 1) cyber security on what cyber resilience means and what kind of responsibilities are vital, 2) the economic and behavioural models of a cyber catastrophe and scenarios for resilience, as well as 3) the risk management vision on the balance between investments in security controls and cyber insurance. This topic adds to the understanding how cyber insurance supports the cyber ecosystem beyond the limits of cyber security risk management and contributes to cyber resilience, i.e. helps to withstand cyber 'hurricanes'.

5. Policy Making in the Cyber insurance field

This final group was formed the last day to compile policy issues discussed at various groups.

5 Event output

These were the core outputs of the formulated working groups after consecutive working group sessions and insightful discussions within and across working groups:

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.
   - During the open day event, 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 identified include:
     - modeling of targeted threats,
     - models for different segments of organisations,
     - 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, organisational, 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
   - We would recommend enhanced scenario planning 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, we would list the following most important raised issues:

- 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.

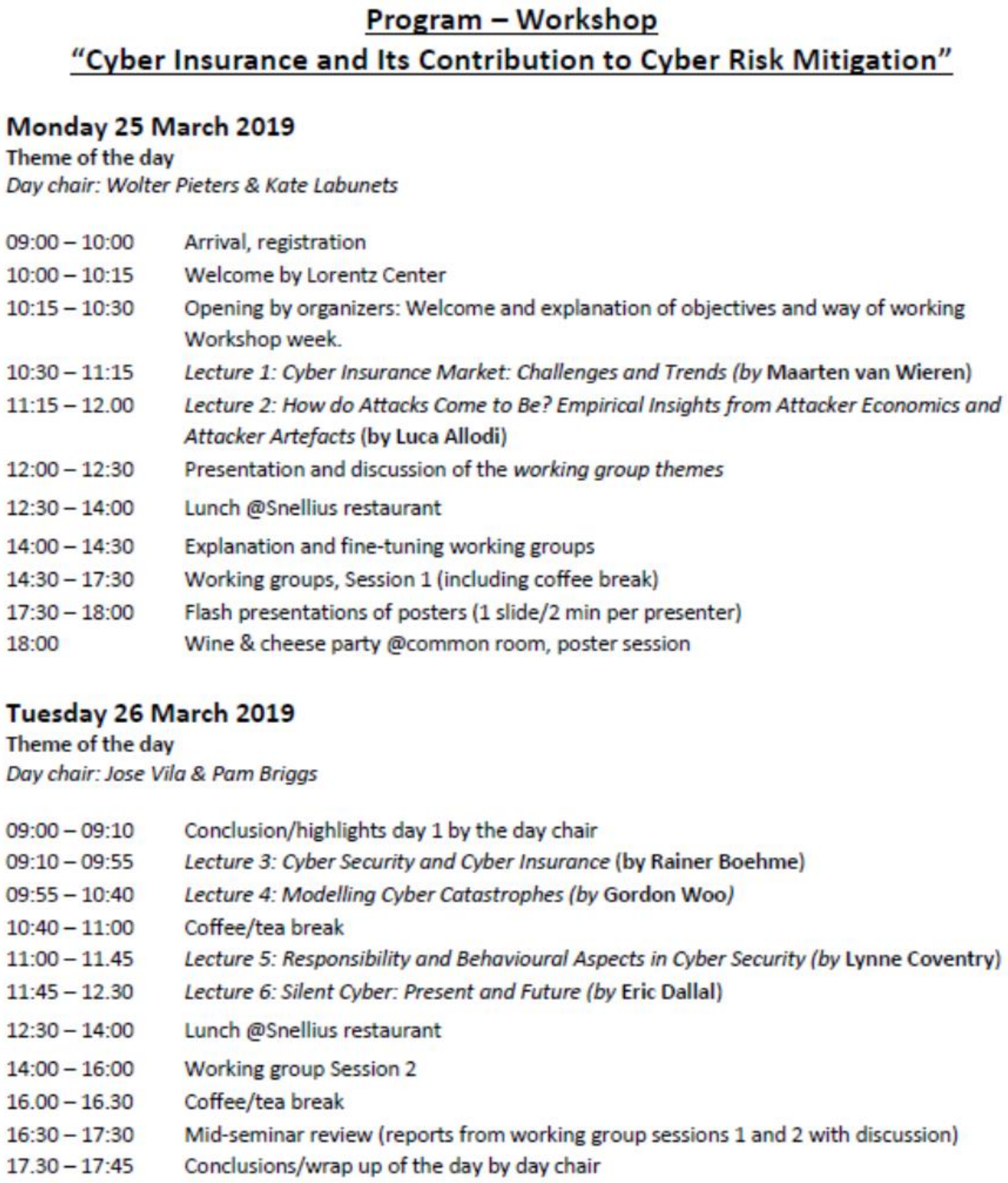
Materials from the workshop are available at https://svn.tbm.tudelft.nl/TREsPASS/CYBECO/Lorentz

Overall, the event received positive feedback both from the participants of the main week-long event as well as from the industry representatives who participated on the open day session on March 27, 2019. The CYBECO consortium further received a solid feedback of the market needs in this field and realized that the products in this market are now being developed. We believe that this workshop created a significant contribution to the development of the cyber insurance community and brought together researchers from different background and cyber insurance practitioners.

6 Discussion

The CYBECO event was held at the Lorentz center in Leiden and included a specific CYBECO project session which allowed us to interact with other cyber insurance researchers and practitioners. The overall impression about the CYBECO toolbox was very positive. There were discussions about possible continuations of the CYBECO project. Contacts with projects like SECONDO and CYBERSURE were reinforced.

Appendix A. Event Program



Program – Workshop
"Cyber Insurance and Its Contribution to Cyber Risk Mitigation"

Monday 25 March 2019

Theme of the day

Day chair: Wolter Pieters & Kate Labunets

09:00 – 10:00	Arrival, registration
10:00 – 10:15	Welcome by Lorentz Center
10:15 – 10:30	Opening by organizers: Welcome and explanation of objectives and way of working Workshop week.
10:30 – 11:15	*Lecture 1: Cyber Insurance Market: Challenges and Trends (by* **Maarten van Wieren**)
11:15 – 12.00	*Lecture 2: How do Attacks Come to Be? Empirical Insights from Attacker Economics and Attacker Artefacts* **(by Luca Allodi)**
12:00 – 12:30	Presentation and discussion of the *working group themes*
12:30 – 14:00	Lunch @Snellius restaurant
14:00 – 14:30	Explanation and fine-tuning working groups
14:30 – 17:30	Working groups, Session 1 (including coffee break)
17:30 – 18:00	Flash presentations of posters (1 slide/2 min per presenter)
18:00	Wine & cheese party @common room, poster session

Tuesday 26 March 2019

Theme of the day

Day chair: Jose Vila & Pam Briggs

09:00 – 09:10	Conclusion/highlights day 1 by the day chair
09:10 – 09:55	*Lecture 3: Cyber Security and Cyber Insurance* **(by Rainer Boehme)**
09:55 – 10:40	*Lecture 4: Modelling Cyber Catastrophes (by* **Gordon Woo***)*
10:40 – 11:00	Coffee/tea break
11:00 – 11.45	*Lecture 5: Responsibility and Behavioural Aspects in Cyber Security (by* **Lynne Coventry**)
11:45 – 12.30	*Lecture 6: Silent Cyber: Present and Future (by* **Eric Dallal**)
12:30 – 14:00	Lunch @Snellius restaurant
14:00 – 16:00	Working group Session 2
16.00 – 16.30	Coffee/tea break
16:30 – 17:30	Mid-seminar review (reports from working group sessions 1 and 2 with discussion)
17.30 – 17:45	Conclusions/wrap up of the day by day chair

Wednesday 27 March 2019 [Open day]

Theme of the day

Day chair: David Rios Insua

Detailed program is available at https://bit.ly/2SQO4Ag.

08:30 – 09:00	Walk-in
09:00 – 09:15	Introduction and explanation of objectives and way of working for the open day
09:15 – 10:00	Keynote 1 – "Vulnerability does not equal loss" by Eireann Leverett, Centre for Risk Studies at the University of Cambridge & Concinnity Risks.
10:00 – 10:15	Presentation of the roundtable themes
10:15 – 11:15	Session 1: 4 roundtables based on the topics of the workshop (see next page).
11:15 – 11:45	Coffee/tea break
11:45 – 13:00	Session 2: 4 roundtables based on the topics of the workshop.
13:00 – 14:00	Networking break and lunch
14:00 – 14:40	Keynote 2 – "Cyber accumulation risk - Swiss Re's view on Cyber catastrophes" by Philipp Hurni, Swiss Re.
14:40 – 16:00	Keynote 3 – CYBECO session (approach description; results of controlled experiment on cyber insurance decision making; toolbox demo)
16:00 – 16:30	Coffee/tea break
16:30 – 17.30	Results of the roundtables and discussion
17:30 – 17:45	Closing of event
18:00	Networking and workshop dinner at Belgisch Biercafe Olivier (Leiden)

Thursday 28 March 2019

Theme of the day

Day chair: Jeroen van der Ham

09:00 – 10:30	Plenary session (updates on the results of the open day). Create policy group.
10:30 – 11:00	Coffee/tea break
11:00 – 12:30	Working group Session 4 / Research and policy group Session 1 (Research and policy impact agenda)
12:30 – 14:00	Lunch @Snellius restaurant
14:00 – 15:30	Workgroup Session 5 / Research and policy group Session 2 (including coffee/tea)
15:30 – ...	Free afternoon

Friday 29 March 2019

Theme of the day

Day chair: Michel van Eeten

09:00– 10.30	Preparation to the final presentations: Working groups and research and policy group
10:30 – 11:00	Coffee/tea break
11:00 – 12:00	Working groups results: Final presentations (CI market & Cyber resilience and responsibilities)
12:00 – 13.30	Lunch @Snellius restaurant
13:30 – 14:30	Working groups results: Final presentations (Data supply for CI & Refined threat modelling)
14:30 – 15.30	Presentation of the results from the research and policy group + discussion
15:30 – 15:45	Closing of workshop

Appendix B. Event Photos

CYBECO
CYBECO: "Supporting Cyberinsurance from a Behavioural Choice Perspective"

CYBECO Toolbox scope