CYBECO

Supporting cyber-insurance from a behavioural choice perspective

Vassileiadis, Nikos; Vieira, Aitor Couce; Insua, David Ríos; Chatzigiannakis, Vassilis; Tsekeridou, Sofia; Gómez, Yolanda; Vila, José; Labunets, Katsiaryna; Pieters, Wolter; Briggs, Pamela

Publication date
2019

Document Version
Final published version

Published in
Challenges in Cybersecurity and Privacy

Citation (APA)
Vassileiadis, N., Vieira, A. C., Insua, D. R., Chatzigiannakis, V., Tsekeridou, S., Gómez, Y., Vila, J., Labunets, K., Pieters, W., Briggs, P., & Branley-Bell, D. (2019). CYBECO: Supporting cyber-insurance from a behavioural choice perspective. In *Challenges in Cybersecurity and Privacy: the European Research Landscape* (pp. 103-115). River Publishers.

5

CYBECO: Supporting Cyber-Insurance from a Behavioural Choice Perspective

Nikos Vassileiadis[1], Aitor Couce Vieira[2], David Ríos Insua[2], Vassilis Chatzigiannakis[3], Sofia Tsekeridou[3], Yolanda Gómez[4], José Vila[4], Katsiaryna Labunets[5], Wolter Pieters[5], Pamela Briggs[6] and Dawn Branley-Bell[6]

[1]Trek Consulting, Greece
[2]Institute of Mathematical Sciences (ICMAT), Spanish National Research Council (CSIC), Spain
[3]Intrasoft International, Greece
[4]Devstat, Spain
[5]Faculty of Technology, Policy and Management, Delft University of Technology, the Netherlands
[6]Psychology, University of Northumbria at Newcastle, United Kingdom
E-mail: n.vasileiadis@trek-development.eu; aitor.couce@icmat.es; david.rios@icmat.es; Vassilis.Chatzigiannakis@intrasoft-intl.com; Sofia.Tsekeridou@intrasoft-intl.com; ygomez@devstat.com; jvila@devstat.com; K.Labunets@tudelft.nl; W.Pieters@tudelft.nl; p.briggs@northumbria.ac.uk; dawn.branley-bell@northumbria.ac.uk

Cyber-insurance can fulfil a key role in improving cybersecurity within companies by providing incentives for them to improve their security, requiring certain minimum protection standards. Unfortunately, so far, cyber-insurance has not been widely adopted. CYBECO focuses on two aspects to fill this gap: (1) including cyber threat behaviour through adversarial risk analysis to

support insurance companies in estimating risks and setting premiums and (2) using behavioural experiments to improve IT owners' cybersecurity decisions. We thus facilitate risk-based cybersecurity investments supporting insurers in their cyber offerings through a risk management modelling framework and tool.

5.1 Introduction

Cyber security is increasingly perceived as a major global problem as reflected by the World Economic Forum [1] and is becoming even more important as companies, administrations and individuals get more and more interconnected, facilitating the spread of cyberthreats. Famous examples include the Target 2014 data breach, in which a cyber attack to that company through one of its suppliers caused the loss of 70 million credit card details, entailing major reputational damage, and the NotPetya malware, which affected thousands of organisations worldwide with an estimated cost of more than 8 billion EUR.

Given the importance of this problem, numerous frameworks have been developed to support cybersecurity risk management, including ISO 27005 [2] or CORAS [3], among several others. Similarly, several compliance and control assessment frameworks, like ISO 27001 [4] or Common Criteria [5], provide guidance on the implementation of cybersecurity best practices. Their extensive catalogues of assets, controls and threats and their detailed guidelines for the implementation of countermeasures to protect digital assets facilitate cyber security engineering. However, a detailed study of the main approaches to cybersecurity risk management reveals that they often rely on risk matrices for risk analysis purposes, with shortcomings documented in e.g. Thomas et al. [6].

Moreover, with few exceptions like IS1 [7], such methodologies do not explicitly take into account the intentionality of certain threats, in contrast with the relevance that organisations like the Information Security Forum (ISF) [8] start to give to such threats. As a consequence, ICT owners may obtain unsatisfactory results in relation with the prioritisation of cyber risks and the measures they should implement, even more in the case of an increasing variety of threats as well as the increasing complexity of countermeasures for risk management available, including the recent emergence of cyber-insurance products [9].

The CYBECO project aims at providing a framework and a tool to facilitate cyber security resource allocation processes, including the provision

of cyber insurance and, consequently, contribute to a more cyber secure environment.

5.2 An Ecosystem for Cybersecurity and Cyber-Insurance

CYBECO includes a detailed analysis of the cyber-insurance (and cyber-security) ecosystem. This is aimed at facilitating the use of the toolbox for specific stakeholder scenarios, as well as providing policy recommendations that, together with the toolbox, help achieve key goals. We identified several primary and secondary actors participating in the cyber-insurance ecosystem and relationships that exist between them.

The main parties that we identified are:

- *insurance providers* who "assume risks of another parties in exchange for payment" [9];
- *insurance brokers* who provide an advice to the companies on the available insurance products matching their needs;
- *companies* that are interested in transferring part of their cyber-related risks with cyber-insurance. The reasons for purchasing cyber-insurance may differ depending on the company size.

Secondary actors include *consumers* using services or products provided by companies; *experts* that provide professional services to the insurance companies (e.g., risk assessment, forensics, cyber incident counsel, legal and PR services); *regulators* managing corresponding business sectors; and other parties.

Based on the discussions with the representatives of different actor types and existing literature, we identified their motivation and goals, which guide their behaviour in the ecosystem. An insurance provider is interested in increasing its market share, having better actuarial data to improve risk assessment and run a profitable business. Similarly, an insurance broker aims at making a profit, but also at providing its clients with high-quality advice about cyber risks. The companies try to get advice on security investments, cover possible losses related to cyber risks and, in case of an incident, get help with incident handling. At a higher level, we have a regulator or government actor whose primary interests are to increase the overall level of security and create a resilient ecosystem [10].

The current cybersecurity regulations and standards are poor concerning policy measures that are related to cyber-insurance. Therefore, we adopted a framework proposed by Woods and Simpson [10] to identify possible policy

measures that can be considered by the government for improving the cyber-insurance market. The framework provides six main themes for possible policy measures:

1. *Wider adoption* covers measures like assigning financial costs to cyber events (i.e., regulatory fines), raising awareness that traditional insurance policies do not cover cyber risk, supporting market development via governmental procurement capability, and making cyber-insurance mandatory for specific business sectors.
2. *Defining coverage* includes standardisation of the language used in cyber-insurance policies, promotion of cyber exclusion clauses in non-cyber policies, and providing certification for acts of cyber war or terrorism.
3. *Data collection* includes policy measures such as the introduction of standard data formats for risk assessment and claim processes, requirements for risk assessment data collection, and collecting high-level data on the cyber-insurance market.
4. *Information sharing* consists of measures like making available data collected by government (related to GDPR or NIS regulations), open access to sector-specific information-sharing initiatives (sector ISACs), creating a state- or EU-level cyber incident data repository and mandating other organisations to share data.
5. *Best practice* includes defining cybersecurity best practices that cyber-insurers should check with their clients or even demand and, at the same time, implementing regulations that clarify what the liability of insurers giving security advice is.
6. *Catastrophic loss* comprises policy measures related to the role of government as insurer of last resort, including different models for insuring catastrophic events (e.g. terrorism).

To better understand which policy measures have more influence on the ecosystem, we mapped the goals of the actors to Wood and Simpsons' framework. Wider adoption of cyber-insurance implies growth of the market and, therefore, supports goals like increasing market share for insurers, making a profit for insurers and brokers. At the same time, wider adoption means that more companies insured their cyber risks, implying that the resilience of the ecosystem is also increasing. Policy measures related to coverage definition help brokers to better advice companies about relevant insurance products meaning that companies get an appropriate policy to cover their cyber risks. Wider use of cyber exclusions in non-cyber policies could lead to improving

the level of sales of cyber-insurance products contributing to the profitability of insurers and brokers.

Data collection policy measures impact insurers' goal related to having better actuarial data. Information sharing measures also supply insurers with actuarial data and help brokers to provide clients with high-quality advice about cyber risks as brokers can have real information about current cyber incidents. Security best practices help brokers to advise their clients on cyber risks and countermeasures, meaning that companies get advice about what security investments to make. By using security standards in cyber-insurance risk assessment and even including security best practices as required in cyber-insurance policy, the government could affect the overall level of security in the ecosystem. Finally, catastrophic loss measures contribute to increasing ecosystem resilience, which is the goal of the governmental actor.

The only goal that is not covered by this policy measures framework is related to company actors who need assistance in incident handling. However, the existing practice shows that most insurers offer their clients crisis management services as a part of cyber-insurance products. Such services are mostly provided by partnering organisation and its cost is included in the policy coverage [11, 12].

Details on the cyber-insurance ecosystem, the associated policy recommendations, and their connection with the CYBECO toolbox are described in the associated deliverable [14].

5.3 The Basic Cybeco Model: Choosing the Optimal Cybersecurity and Cyber-Insurance Portfolio

CYBECO provides several cyber-insurance related decisions. The main model aims at providing support to an organisation that needs to allocate its cybersecurity resources, including the adoption of cyber-insurance. In it, we distinguish between a Defender, to which our methodology will support in her allocation, and an Attacker, who will try to perpetrate attacks to the Defender in pursue of certain goals.

We represent the problem as a bi-agent influence diagram (BAID) in Figure 5.1, with the terminology used in [14]. Therefore, the diagram includes oval nodes that represent uncertainties modelled with probability distributions; hexagonal utility nodes that represent preferences modelled with a utility function; rectangle nodes, which represent decisions modelled through

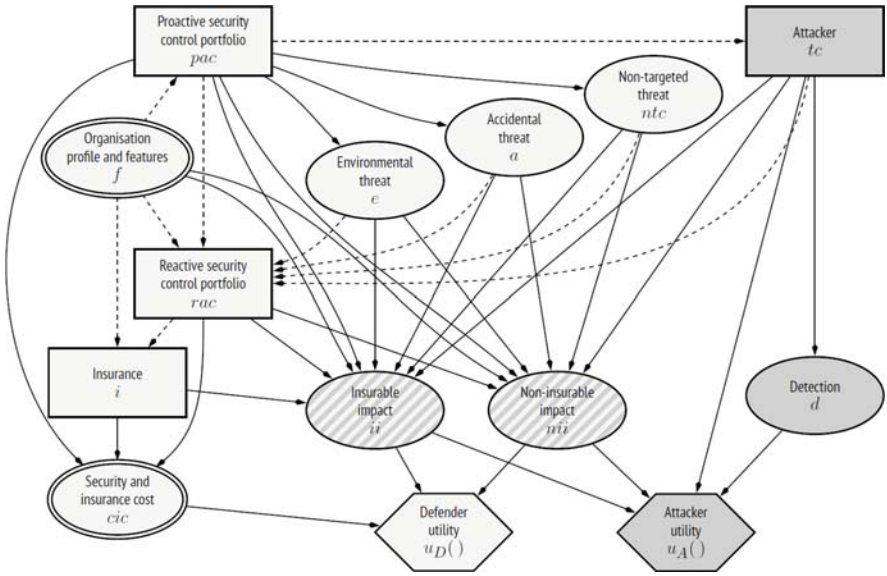

Figure 5.1 BAID describing the cybersecurity resource allocation problem.

the set of relevant alternatives at such point; and, finally, double oval nodes that represent deterministic nodes modelled through a function evaluating the antecessors of the corresponding node. The diagram also includes arrows to be interpreted as in standard influence diagrams [15]. Light nodes designate nodes belonging just to the Defender problem; dark ones to the Attacker; and, finally, striped ones are relevant to both agents.

We outline the BAID. First, we include a description of the organization profile and features, including its assets. We then identify the threats relevant to the organisation; following the ISF classification, we distinguish between environmental, accidental and non-targeted cyber threats, which we model through uncertain nodes. Besides, we also consider targeted cyber threats, modelled as decisions, but associated with a different agent, the Attacker. Having determined the threats and relevant assets, we may identify the impacts that we separate between insurable and non-insurable ones.

Once with the relevant threats and impacts for the organisation at hand, we may identify the actions that may be undertaken to mitigate the likelihood and/or impact of the threats. We distinguish three types of instruments: proactive security controls, reactive security controls and insurance. The above instruments may have to satisfy certain constraints (financial, technical, compliance, etc.). Besides, they will have security and insurance costs, which

will typically be deterministic. With all the relevant attributes in place, we may then prepare the preference model for the Defender through her utility.

We turn now to the remaining elements of the Attacker problem, mainly his detection and identification. Finally, with all his relevant elements in place, we may then build a preference model for the Attacker through the utility of the attacker through a value node.

Based on such model, we build the so-called Defender problem. This facilitates the quantitative modelling of the problem using conditional probability distributions at uncertain nodes and a utility function for modelling the preferences and risk attitudes of the Defender. All those models are standard in decision analysis except those referring to the likely threats performed by the attacker(s) that entail strategic thinking.

To facilitate their assessment, we consider the so-called Attacker problem. As we do not have full access to the attackers to elicit their beliefs and preferences, we use random probabilities and utilities to model our uncertainty about them. We then simulate from such problem to find the corresponding random optimal alternatives that help us to find the required attack forecasts. This feeds back the Defender problem that is finally solved to provide the optimal proactive portfolio, reactive portfolio and insurance that should be implemented by supported organisation.

This and other models for other cyber-insurance related decisions are fully described in [17].

5.4 Validating CYBECO

The findings of the CYBECO project have been validated in several ways:

1. A set of use cases and scenarios were developed to verify whether the proposed models were robust in all situations. They are available in [18]. They have confirmed the validity of our approach, although some fine tuning, specification and further modelling has been required.
2. A workshop in which we presented the CYBECO toolbox wireframes to a number of cybersecurity professionals and solicited their feedback. This was essential for the fine-tuning of the project findings.
3. The last validation approach focused on the application of behavioural-experimental methods to test the assumptions of the CYBECO models on purchase behaviour of cyber-protection measures and cyber-insurance, as well as on the belief formation of cyber-risk and vulnerability levels. To this end, the project has designed and run a large-scale

online behavioural economic experiment with a total sample of 4.800 subjects from Germany, Poland, Spain and UK. Beyond the validation of the model, the experiment has provided behavioural insights relevant for the development of the cyber-insurance market in the EU.

The structure of the experiment was as follows. In a controlled gamified environment, subjects were meant to design the protection and cyber-insurance strategy for an SME and were required to carry out certain tasks online (see Figure 5.2). After that, each subject may receive a random attack

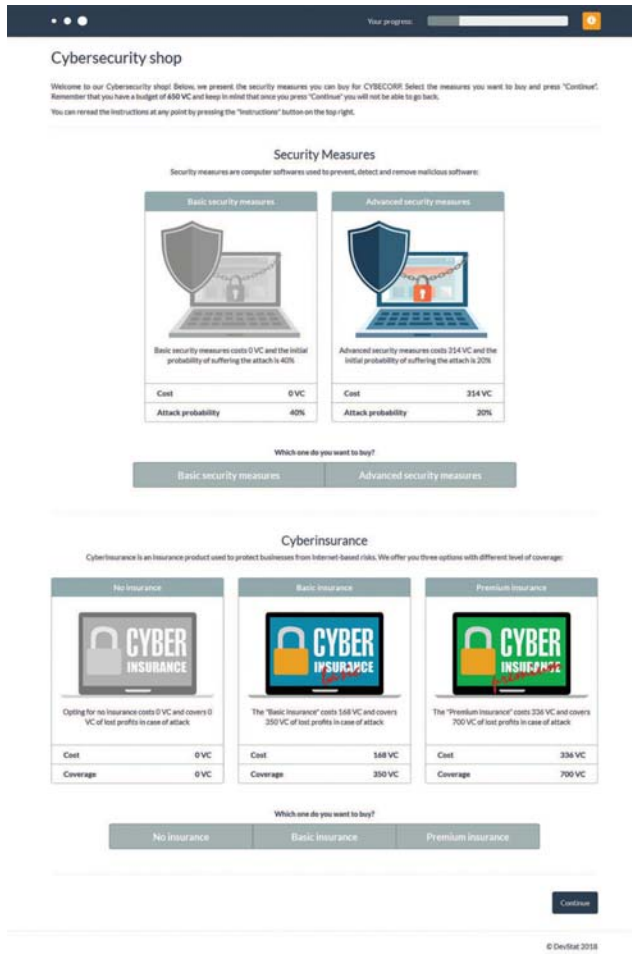

Figure 5.2 Screenshot of the online cybersecurity shop in the experiment.

with success probability depending on the purchased protection measures and level of security of her online behaviour. According to the methodology of behavioural economics, the decisions of the participants and the random events in the experiment (the attack) have an actual impact in their economic incentives, to be received after completing the experiment. To check belief formation, the process is repeated twice. The experiment also included a questionnaire to measure risk attitude and the Protection-Motivation psychological variables.

The economic experiment validated the underlying assumptions of the model and provided other relevant insights. Experimental results showed that belief formation is dependent on the context of the attack, the participants selecting higher protection and insurance levels under the menace of intentional attacks (cybercrime) than of random (random virus) ones. The experiment also analysed the impact of the experience of suffering a cyberattack in the updating of beliefs and protection-insurance strategies. The results show the presence of two opposite reactions: although an attack does in general motivate participants to increase their protection levels, suffering the attack reduced confidence level in the effectivity of the protection measure for 15.1% of the participants who reduced their protection level after the attack. As insurance behaviour regards, experimental subjects seem to purchase insurance levels over the optimal level. Moreover, the experiment excluded moral hazard in cyber-insurance: purchasing a cyber-insurance policy does not reduce the security level of online behaviour and is positively correlated with the acquisition of stronger cybersecurity protection measures. An additional relevant result of the experiment is the existence of vulnerable segments of population (elder citizens, for instance) that, although being risk averse and concerned with cybersecurity, behave insecurely online. The likely reason for this lack of security is that they do not know how to behave in a safer way.

5.5 The CYBECO Decision Support Tool

When compared with standard approaches in cybersecurity, the CYBECO paradigm provides a more comprehensive method leading to a more detailed modelling of cyber risk problems, yet, no doubt, more demanding in terms of analysis. We believe though that in many organizations, especially, in critical infrastructure sectors, the stakes at play are so high that this additional work should be worth the effort.

To facilitate implementation, we are converting our generic actionable model into a decision support system (DSS), the CYBECO tool, for cybersecurity risk management at a strategic level. The objective of such DSS would be to provide the best portfolio of security controls and insurance products, given a predefined relevant budget and other technical and legal constraints for a certain planning period.

The toolbox adopts the form of an online calculator (see Figure 5.3) to guide the user into analysing their current cybersecurity risk level and the optimal cybersecurity strategy for their specific needs. The calculator is viewed as a multi-step online visually-enriched form, which asks the pertinent

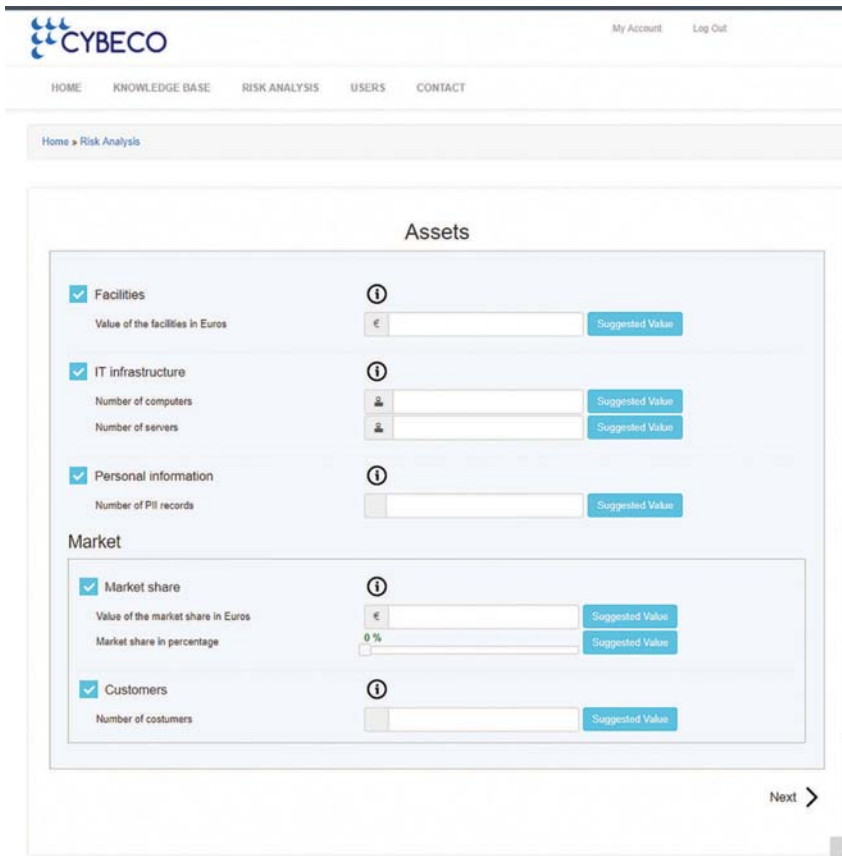

Figure 5.3 A snapshot of the CYBECO tool, gathering inputs on assets to feed the cyber risk analysis tool.

questions (e.g., company size, characteristics, relevant threats, relevant security measures and insurance products, relevant impacts, etc.) and offers the best option for the stakeholder (SME, large industry) based on the outcomes of the CYBECO cyber risk management models.

To enhance the usability, visual appearance of outputs, and general user-friendliness of the calculator, three types of user-oriented validations have been undertaken to collect relevant feedback. First, we have designed and implemented a behavioural economic experiment with a sample of 2,000 potential users of the calculator (workers in SMEs in managerial or cyber-security related positions) in Germany, Poland, Spain and UK. In a gamified controlled environment, the participants were asked to define the cyber-protection and cyber-insurance strategies of an SME using five different framings of the output of the CYBECO calculator. The experiment showed that the potential users of the CYBECO toolbox tend to use it more as an information source to make such a decision in a better informed manner rather than an expert tool able to guide them to the best option and provide relevant recommendations (only 30% of the users declared to have purchased the strategy recommended by the tool). It must be highlighted that this result is not attributable to a lack of understanding of the ranking criteria but it results from the fact that users do consciously prefer a different protection approach, coverage or price level than the one dynamically recommended by the toolbox. Another evaluation target has been the user navigation paths, offered by the toolbox, which were evaluated by two focus groups with about 50 actual users, which helped in improving the visual aspect of the toolbox. Finally, a rich set of uses cases has been developed and applied as usage patterns on the toolbox to crosscheck the correct implementation of the cyber risk analysis algorithms.

5.6 Conclusion

We have provided a brief summary of some of the ongoing and expected achievements of the CYBECO project. On the supply side, we expect that the end-users would benefit from better founded and designed cyber-insurance products and cyber risk management frameworks. On the demand side, we expect that the end-users would benefit from a well-founded tool that allows them to determine their optimal cyber security investments, including the appropriate cyber-insurance product. Globally, the society as a whole would benefit as CYBECO helps in creating a more secure environment.

In a nutshell, by properly modelling and combining decision-making behaviour surrounding cyber threats (risk generation), the decision-making behaviour of insurance companies (risk assessment) and the decision-making behaviour of IT owners (which includes cyber-insurance), we hope to help mitigate cyber risks at the global level.

Acknowledgements

CYBECO: Supporting cyberinsurance from a behavioural choice perspective is a project funded by the H2020 programme through grant agreement no. 740920.

References

[1] World Economic Forum, "The Global Risks Report 2019," 2019.
[2] International Organization for Standardization, ISO/IEC 27005 – Information Security Risk Management, 2013.
[3] M. S. Lund, B. Solhaug and K. Stølen, Model-driven Risk Analysis: The CORAS Approach, Springer, 2010.
[4] International Organization for Standardization, ISO/IEC 27001 – Information Security Management Systems – Requirements, 2013.
[5] The Common Criteria Recognition Agreement Members., Common Criteria for Information Technology Security Evaluation, Version 3.1 Release 4, 2009.
[6] P. Thomas, R. B. Bratvold and J. E. Bickel, "The risk of using risk matrices," in *SPE Annual Technical Conference and Exhibition 2013.*, 2013.
[7] National Technical Authority for Information Assurance (UK), HMG IA Standard Number 1., 2012.
[8] Information Security Forum, Information Risk Assessment Methodology 2, 2016.
[9] A. Marota, F. Martinelli, S. Nanni, A. Orlando and A. Yautsiukhin, "Cyber-insurance survey," *Computer Science Review,* 2017.
[10] PricewaterhouseCoopers, "The Global State of Information Security Survey 2018," 2017.
[11] D. Woods and A. Simpson, "Policy measures and cyber insurance: a framework," *Journal of Cyber Policy,* vol. 2, no. 2, pp. 209–226.

[12] S. Romanosky, L. Ablon, A. Kuehn and T. Jones, "Content analysis of cyber insurance policies: how do carriers write policies and price cyber risk?," in *Workshop on Economics of Information Security*, 2017.
[13] B. Nieuwesteeg, L. Visscher and B. de Waard, "The law and economics of cyber insurance contracts: a case study," *European Review of Private Law,* vol. 26, no. 3, pp. 371–420, 2018.
[14] The CYBECO Consortium, "D7.1 – CYBECO Policy Recommendations," 2019.
[15] D. Banks, J. Rıos and D. Rıos Insua, Adversarial Risk Analysis, Francis and Taylor, 2015.
[16] R. D. Shachter, "Evaluating Influence Diagrams," *Operations Research,* vol. 34, no. 6, pp. 871–882, 1986.
[17] The CYBECO Consortium, "D3.1 – Modelling framework for cyber risk," 2018.
[18] The CYBECO Consortium, "D4.1 – Cyber-Insurance Use-Cases and Scenarios," 2018.