CSP FORUM

Risk Assessment and Cyber Insurance Workshop – Report

Satellite Event of the CSP Innovation Forum 2015

CSP Forum (www.cspforum.eu)
Funded by SecCord CSA (www.seccord.eu)
Unit H4, European commission, DG CONNECT
Consortium Partners: WIT, UNITN, HP, SAP ATOS

Table of contents

Table of figures

1. Introduction

Business companies and individual users can resort to cyber-insurances to protect themselves from risks related to cyber-attacks, basically the very same way they purchase insurance for physical goods. While the market is rapidly growing for cyber-insurance (especially in the US soil), showing that there is a strong interest, the adoption is still low and the maturity of the offer pretty at early-stage. Two main reasons emerge. First of all, the lack of historical data related to cyber-attacks makes it extremely difficult to derive models of "what is good" and "what is bad", so that insurance companies have hard-time to determine premiums and standardized cyber-insurance offers. Second, because computer systems are interdependent and standardized, insurance companies fear a major cyber-space accident, so-called “cyber-hurricane,” resulting in an unaffordable number of claims. While these are two well-known reasons that cover the viewpoint of the insurers, what is the role and viewpoint of the other stakeholders such as business companies, policy-makers, etc. ?

The CSP Forum event “Risk Assessment and Cyber Insurance”, organized on April 27th 2015 in Brussels, discussed around this topic, with special focus on its fundamental challenges and possible solutions.

After a welcome speech by the organizers, five prominent experts in the field shared their findings and opinions, challenged by the audience during Q/A sessions and a closing panel.

The five speakers were carefully selected to present the point of view of key stakeholders for Risk Assessment and Cyber Insurance:

- EU Commission: what is the point of view of the EU commission and which initiatives have been run and will be running at EU level on this topic
- Industry sectors: why and when industry may want to resort to cyber insurance instruments
- Cyber Insurance Brokers: cyber insurance challenges and opportunities from a broker perspective
- Business Universities: academic scientific view on cyber insurance and public policy
- Auditors: auditors point of view on viable models for cyber-risks

This CSP Forum event was a satellite event of the “CSP Innovation Forum 2015” (https://www.cspforum.eu/2015), organized by the European Commission, DG CNECT (Unit H4 Trust & Security) and the CSP Forum. Overall, more than 60 people registered for the seminar with a good mixture of industry (large companies, but also SMEs), research institutions, and academia as well as EU and national level institutions.

2. Agenda

Figure 1 shows the agenda of the CSP Forum event "Risk Assessment and Cyber Insurance".

Oganisers:

Luca Compagna (SAP)
Fabio Massacci (University of Trento)

Agenda

14:00 - 14:15: **Welcome**

14:15 - 16:45: **Invited speaker session,** Chair: Fabio Massacci (University of Trento)

- **Cyber insurance and the NIS directive**
  Ann-Sofie Ronnlund (European Commission)
- **The need for and the making of cyber insurance**
  Stefano Nanni (UNIPOL)
- **Cyber-insurance from a brokers perspective**
  Mr. Stephen Wares (Cyber Risk Practice Leader for Marsh EMEA)
- **Cyber-insurance and public policy**
  Prof. Julian Williams (Durham Business School)
- **Models for Cyber-risk**
  Maarten van Wieren (Deloitte)

17:00 - 17:30: **Panel and wrap-up**, Chair: Fabio Martinelli (CNR, NIS WG3 Chair)

- Prof. Christian Probst (DTU, TRESPASS Project)
- Massimo Felici (HP)
- *All invited speakers*

Figure 1- Agenda and organisers

3. Outcomes

This section presents the outcomes of the CSP Forum event "Risk Assessment and Cyber Insurance". The slides of each presentation are available here.

- ***Cyber-insurance and the NIS[1] directive***, Ann-Sofie Ronnlund (European Commission). Risk assessment as part of the NIS Platform guidance and the NIS Directive: will it foster also cyber insurance? This is the main question the presentation elaborated on. One of the assumptions is that the proposed incident notification requirement of the NIS Directive will improve the situation with regard to collection of historical data, which may be of use for cyber insurance. In addition, the best practice guidance on risk assessment and management---of the NIS Platform---will help in determining organisations that are performing well. Indeed 30-40% of the overall cyber insurance companies states that they award the companies that invest on security and risk assessment, e.g., by lowering insurance costs. The speaker made also clear that NIS will not interfere with "liabilities".

[1] Network and Information Security (NIS), https://resilience.enisa.europa.eu/nis-platform

- ***The need for and the making of cyber insurance***, Stefano Nanni (UNIPOL). This talk outlined the perspective of a generic financial conglomerate with banking and insurance operations. While both businesses deal with cyber risk and current related regulatory requirements, the bank is likely to become a critical infrastructure under the NIS Directive and the insurance segment deals with challenges to meet increasing demand in cyber insurance from a variety of industries. If there is a strong appetite for cyber insurance (industries from many sectors are asking for it, even from sectors that were not expected), the barriers for wider and systematic adoption are still standing up. Initiatives run by NIS and ENISA are contributing to lower these barriers, but more will be necessary and mainly outside the technical realm. There is a need for legal certainty, in particular on liability, and standardization, but also a necessary shift in the mentality from a threat avoidance model to a more risk management driven one. The latter is evangelized since long time (cf. Bruce Schneider talk at BlackHat 2001), but is it fully established? All this together could make insurance driving security in the digital world as it does in the real one.

- ***Cyber-insurance from a broker perspective***, Stephen Wares, (Cyber Risk Practice Leader for Marsh EMEA). This presentation discussed the challenges for organisations in transferring their cyber exposures to the insurance market both under a dedicated cyber policy and within their existing insurance programme. Among these challenges the insurance communication gap (see the European 2015 Cyber Survey Report by Marsh[2] for more detail): many chief officers of large companies believe they have insurance that would cover them in the event of a cyber-breach while they do not. Pricing immaturity (due to lack of data) and high-degree of outsourcing within the ICT business are two additional key challenges. The latter is particularly tricky as it makes difficult to establish (i) what or who is insured and (ii) how much cyber-hurricane damage could be in such a distributed and strictly connected network of companies (elephant in the room?). The talk also restated the insurance market's appetite and explained the capability to take on cyber peril based exposures and the process for designing and placing a suitable insurance programme. Among the closing recommendations: companies should ensure that their cyber risk is fully investigated and understood; insurance coverage with respect to cyber risks should be investigated and accurately communicated within the company; better modelling tools are required by the insurance industry to ensure that insurers are underwriting within capacity constraints; and because insuring cyber exposures is complex and fractured across many policies, companies need to make full use of the expertise that exists within their broker to get the right outcomes.

- ***Cyber-insurance and public policy***, Prof. Julian Williams (Durham Business School). *The only way that insurance markets provide a global benefit to targets (e.g., companies) is when security investment is separately mandated by a social planner (usually government) whose sole objective is to maximise the targets global utility.* This is, in essence, the key message that this talk outlined as a result of a careful modelling and analysis of the cyber-insurance economic aspects (including the attacker component). If insurance is provided without a social planner (e.g., by a monopolist insurance), then the effects almost unambiguously indicate an aggregate drop in security investment. Indeed, security investment does not increase when there is a fully competitive cyber-insurance market, in fact it may well decrease as targets shift to making risk neutral security investment decisions. This does not mean that cyber insurance is `bad', but that it cannot be used in place of public policy coordination of security.

[2] http://uk.marsh.com/NewsInsights/Articles/ID/45277/European-2015-Cyber-Survey-Report.aspx

- ***Models for Cyber-risk***, Maarten van Wieren (Deloitte). The quantification model developed by Deloitte under the World Economic Forum was presented. It includes a probability model to determine breach rates per hacker-company pair. Company attractiveness and resilience determine breach probability distribution. The quantification model allows for reasoning on different perspectives: company, insurance and society. By filling in the data required by the quantification model (e.g., risk vision and appetite, risk controls and incident data), the company gets a measure of its cyber security status helping to understand which risks are managed and which are not. Via the same data and outcomes is possible to define best fitting cyber insurance contracts. Progressing on the already discussed cyber insurance challenges (e.g., lack of data) will make these contracts and the cyber insurance market more precise, effective and attractive. All in all, it will have a positive impact on society for what concerns "total benefit of digital access" versus "total cost for security assurance". Among the needs to pursue this vision: further development of cyber resilience approaches (especially privacy controls to counter-balance European market friction toward cyber

The workshop ended with a Panel & Wrap-up discussion chaired by Fabio Martinelli (CRN, NIS, WG3 Chair). Besides the speakers, Prof Christian Probst (DTU, TRESPASS Project) and Massimo Felici (HP) joined the panel as representatives of the TREsPASS and SECCORD projects, respectively. TREsPASS develops approaches toward Continuous Risk Assessment for Cyber Insurances. SECCORD performed research reviews and consultations with stakeholders on these subjects and reported about some findings. For instance, it has emerged a limited understanding of *economics* of cyber security and privacy research. The panel discussion with the audience focused on the role of cyber insurance. Panelists shared their opinions. Hereafter some of the statements:

- Cyber insurance can help toward wellness, but it should not be left only to the insurance players.
- Cyber insurance may just be a product closing a gap. As such it needs to be very well defined. It could well be that in a few years cyber risks will be incorporated within classis insurance contracts.
- Residual risk is a very important element. EU is doing the right job here, putting together the right actors. Total cost for society should be lowered, if cyber insurance is one of the means great.
- Internet of Things and big data could open insurance opportunities/incentives. Similar to profile car drivers and therefore personalize insurances, those driving well will pay less.

4. Sum-up

Summing up the event was very interesting and well received. Below we summarize the main key points that emerged, including challenges that were not so well-known, on-going initiatives that could also foster cyber insurance, and white spots.

- *What or who is insured?* Answering this question turns out to be not so easy. Various studies indicate a communication gap between insurances and companies (see above what reported for *Cyber-insurance from a broker perspective*, by Stephen Wares and the European 2015 Cyber Survey Report by Marsh[3]). If organisations should better inspect their insurance coverage with respect to cyber risks and accurately communicate the findings within the company, it is also clear that the high-degree of outsourcing within the ICT business makes more difficult to answer that question.
- *Liability*: outsourcing also points to the liability challenge, one of the white spot that is undermining the legal certainty necessary to establishing a cyber-insurance market.

[3] http://uk.marsh.com/NewsInsights/Articles/ID/45277/European-2015-Cyber-Survey-Report.aspx

- *NIS and ENISA*: both initiatives are strongly supporting incident information sharing (cf. incident notification requirement of the NIS Directive). This will improve the situation with regard to collection of historical data, which may also foster cyber insurance.
- *The role of public policy*: Cyber insurance is not a two-party environment between insurances and companies. Academic study in the field argues that "The only way that insurance markets provide a global benefit to targets is when security investment is separately mandated by a social planner (usually government) whose sole objective is to maximise the targets global utility". The same study indicates that the overall security investment will almost unambiguously drop if insurance is provided without a social planner. In more detail, without a social planner, the interdependency would cause unexpected consequences (e.g., companies buy less insurance coverage or invest less in security), and it would result in a failure in a cyber-insurance market. All in all, cyber-insurance should not be used as a mere substitute of public policy coordination of security.