



EUROPEAN COMMISSION
Information Society and Media Directorate-General
Emerging Technologies and Infrastructures
Trust and Security

WORKSHOP ON "SOCIO-ECONOMICS IN TRUSTWORTHY ICT"

WORKSHOP REPORT

22nd June 2011 - BRUSSELS



TABLE OF CONTENTS

1. INTRODUCTION.....	1
2. SCOPE, MOTIVATION AND GOALS.....	1
3. AGENDA.....	2
4. SOCIO-ECONOMICS IN TRUSTWORTHY ICT.....	3
4.1. Work programme 2011.....	3
4.2. Economics of Cyber Security	4
4.3. Innovation potential and barriers of security products and services.....	7
4.4. Privacy balance of power/Trust Measurement.....	10
4.5. Security information and data for research, industrial and strategic decision-making	13
ANNEX I. ATTENDANCE LIST.....	15

1. INTRODUCTION

The Trust and Security Unit of DG INFSO organised a workshop on "**Socio-economics in Trustworthy ICT**" on 22nd June 2011 in Brussels.

The aim of the workshop was to discuss socio-economic and legal aspects with the objective of jointly identifying current research trends and discussing future research perspectives in the thematic field of socio-economics in Trustworthy ICT.

The importance of the subject was highlighted in terms of the need to properly ensure strong interplay of trust and security dimensions with legal, societal and economic research in view of development of a techno-legal system that should be usable, socially accepted and economically viable.

2. SCOPE, MOTIVATION AND GOALS

The workshop was aimed at sharing and discussing issues related with socio-economics in trustworthy ICT, a rather novel dimension of security and trust, under a very informal and open approach intended to explore key topics and research aspects that should be taken into consideration for current and future activities.

The key areas for discussion at the workshop were defined as:

- Economics of Cyber Security
- Innovation potential and barriers of security products and services
- Privacy balance of power/Trust Measurement: Internet users have very low access to change the conditions that are imposed to them
- Security information and data for research, industrial and strategic decision making: more and better information to make right decisions, how to define policies, reliable data is needed.

3. AGENDA

9:30-9:40	Introduction
9:40-10:00	EC presentation WP 2011 and key topics
10:00-11:15	Individual presentations and Q&A <i>Economics of Cyber Security</i> Lothar Fritsch, David Pym, Mark Felegyhazi, Sebastien Meissner, <u>Ernesto Damiani</u>
11:15-11:30	Coffee break
11:30-13:00	Individual presentations and Q&A <i>Innovation potential and barriers of security products and services</i> Rigo Wenning, Heiko Rossnagel, Ulrich Seldeslachts, Steven Maisel, <u>Fabio Massacci</u> ,
13:00-14:00	Lunch break
14:00-15:30	Individual presentations and Q&A <i>Privacy balance of power/Trust Measurement</i> Andreas Albers, Claudia Diaz, Antonio Liroy, Reijo Savola, <u>Roger Torrenti</u>
15:30-15:45	Coffee break
15:45-16:45	Individual presentations including Q&A: <i>Security information and data for research, industrial and strategic decision making</i> Julian Williams, <u>Michel Van Eeten</u>
16:45-17.00	Summary of the workshop

4. SOCIO-ECONOMICS IN TRUSTWORTHY ICT

4.1. Work programme 2011

The workshop started by the introduction of the specific strategic objective in FP7 Work programme 2011 related with Trustworthy ICT. This strategic objective will be part of the coming call for proposals (FP7 Call 8).

The objective is a trustworthy Information Society based on an ecosystem of digital communications, data processing and service provisioning infrastructures, with trustworthiness in its design, as well as respect for human and societal values and cultures.

The overall presentation highlighted the key role played by security, privacy and trust in the Information Society. References were made to current changes, transition towards a digital society, massive change trends, new services, radical changes in security and the need to better understand what's going on. The core role of Digital Agenda for Europe was emphasized in support of Policies and Regulation for the Digital Age, where Trust & Security is considered as one of the key areas.

4.2. Economics of Cyber Security

The session, chaired by Ernesto Damiani, was supported by the following presentations:

- *Economics of Cybersecurity - Economic perspectives on Information Security*
Lothar Fritsch - Norwegian Computing Center (Oslo)
- *Systems Security Economics*
David Pym - University of Aberdeen
- *Cyber Insurance for Data Breaches*
Mark Felegyhazi - Crysyst Lab, BME-HIT
- *EUROPRISE – European Privacy Seal*
Sebastien Meissner - Datenschutzzentrum
- *Toward Risk-Aware Business Processes*
Ernesto Damiani - Università degli Studi di Milano, Italy

The presentation on *Economics of Cybersecurity - Economic perspectives on Information Security* introduced a number of considerations (from micro and macroeconomics aspects) with respect to privacy risk dimensions, like the duality between the differences in perception from business versus citizens/users or the attempts to “economize” privacy risks. This perception is not only different but also changing over time. From a business perspective, the concept of “Return on Privacy Investment” (ROPI) was introduced, together with a number of issues based upon the value of privacy or the cost of reinstalling privacy. From a macroeconomic perspective, it was highlighted the uneven access to information from sellers with respect to buyers, this having implications in functional aspects of transactional processes. Some ideas were proposed, like enhancing a more participatory design of security mechanisms with users or securing better transparency or research on societal norms versus security economics. In summary, needed research and practice was suggested in the following topics: a) Participatory design of security mechanisms, b) Task-fit of security procedures, c) Tension between societal norms, market practice, regulation, supervision and economic principles should be researched, d) The “societal” security model beyond perimeter security, including economics, social norms, behavioural psychology, and multilateral interests and e) Clearer understanding of cost-benefit distribution of security technology and procedures.

The presentation on “*Systems Security Economics*” focused on a systems-based perspective based upon the use of mathematical models in economics for cyber security, highlighting the relevance of stewardship processes to secure the use of the information. Consideration of trade-offs as opposed to micro-macro alternative was suggested, both at declarative and operational levels (choices to implement, objectives achievement). A broader “life cycle” approach to be considered, raising the question on how to measure policy-infrastructure-assurance. A number of ideas on security modelling has already been published in WEIS¹ related with understanding dynamics and investment cycle.

¹ *Workshop on Economics of Information Security* (George Mason University, USA, June 14–15, 2011)

Currently most of the economic & security models are rather handcrafted, this emphasizing the need for further availability of modelling tools. The key message was on a more scientific and rigorous use of mathematics for systems security modelling.

The presentation on *Cyber Insurance for Data Breaches* introduced a number of examples of history on data breaches whereas it was clear that the role of CISO² did not formally exist before these attacks and data breaches. Many companies did not even realize data breaches when they happened, this justifying the urgent need to make insurance policies into force when data breaches happen. The key topic in this respect was on security versus insurance issues. In terms of security audits the need for both static and dynamic audits was highlighted (particularly relevant for data and processes on the cloud). The eventual outsourcing of audits to third parties was considered as a realistic and interesting option. Reference was made to the ENISA³ *Data Breach Notification Report*, in response to the implementation of data breach notifications requirement, set up by the Article 4 of the reviewed ePrivacy Directive. However, no standard for adequate monitoring systems has been consolidated yet. The question on whether to invest in insurance or in security was proposed to the session, more in particular about the limits/balance between the two approaches. The key points were, in summary, targeted towards: a) data value assessment, b) design a clear data flow in system, c) monitor data flows, and e) establish security.

The presentation on *EUOPRISE – European Privacy Seal* focused on the contribution to socio-economics in trustworthy ICT of the security certification of IT products and IT-based services in Europe, USA and South America, as carried out by EuroPriSe. Importance was given to the fact that the certification criteria are publicly available (Internet), whereas privacy evolves in becoming a marketing advantage in some market areas. Personal information was highlighted as a valuable market resource, whilst data protection is not yet part of data security. A number of ideas were proposed for discussion: a) privacy protection goals (extended), b) privacy by design (specific criteria needed, some already existing in Canada, requirements for implementation, studies on economic impact, ROI, privacy breach, studies on impact of regulatory approaches), c) privacy preferences (are users willing to pay for that?). A suggestion for future research was made with respect to developing a methodology of data protection and privacy, and to exploring the interdependence of data security and data protection in network infrastructure.

The presentation *Toward Risk-Aware Business Processes* outlined the need of economics-based models for the value of information, introducing a discussion on how to differentiate between what is valuable versus what is not that valuable. Inter-organisational business processes were presented as an example, suggesting the alternative of “secure orchestrations” of processes, in order to minimize the risks of attacks by shaping information flows according to information value. It was noted that what is most valuable at the beginning could be less valuable at the end of the product life cycle, and that this can be quantified (although further research is still needed). Importance was given to the consequences of the heterogeneity of exchanged information. Disclosure risk was discussed in terms of the need to quantify and predict

² Chief Information Security Officer

³ European Network and Information Security Agency

the combination of dysfunctional behaviour, probability and impact. The final proposal was to explore modelling business processes as games.

The discussion following the different presentations lead the group to identify some research trends related to the need of models for evaluation of value of data and to recognize that in macroeconomics the role of actors could play a fundamental role in R&D. Importance should be given to analysing the effects and consequences of security of data and services in the cloud, as it could become the best way to implement the modelling of the control and the analysis of the systems. It was recognized that the challenge is in the cloud.

The discussion on the balance between security and insurance was considered interesting, although it was recognized that the effect of the lack of statistics on data security, where an additional difficulty derives from the fact that the system evolves over time constantly, is not static, and statistics are not yet available (use cases could be an alternative approach). As far as data security is concerned, many levels that have been managed independently should be integrated / coordinated.

Concerning implementing privacy-by-design, a first attempt and better understanding are still needed, before considering using application scenarios.

According to the workshop participants, there is a need to explore and better understand the users' willingness to pay, particularly taking into consideration that related costs don't happen at the same time (the cost of privacy breaches come later, willingness to pay for securing that particular risk will have to take this aspect into account). Research is needed in progressing on the consequences of implementation of privacy-by-design in open environments (cloud and multi-tenancy are examples of new sets of problems).

Discussion was also held on Intellectual Property Rights as a fundamental and important issue (where the EU is in some disadvantage versus USA, e.g. in IPR versus time validity of patents).

Probability and impact of security breaches could be considered as components, whereas a predictive analysis of system behaviour is possible and could be explored systematically. In terms of information made available, reverse engineering is a breach strategy that can be linked to the kind and type of data format (a CAD file does not open the same kind of possibilities and risk that a raster drawing).

The prediction of economic value was identified as a key topic, whilst the existence of an economic toolkit for services in the cloud was seen as viable.

4.3. Innovation potential and barriers of security products and services

The session, chaired by Fabio Massacci, was supported by the following presentations:

- *Challenges of distributed Security*
Rigo Wenning - W3C Legal counsel & Privacy Activity Lead
- *Towards Viable Security Solutions – A Pragmatic Approach*
Heiko Rossnagel - Fraunhofer IAO
- *Innovation potential and barriers of security products and services - A perspective on Security Innovations (in Europe)*
Ulrich Seldeslachts - LSEC
- *Science-Business presentation*
Steven Maisel – Science Business
- *Why Johnny can't afford Security Technologies*
Fabio Massacci – University of Trento

The presentation on *Challenges of distributed Security* highlighted the advent of new, distributed challenges. Devices turning into generic machines and web apps are in fact the front-end for the cloud system. The challenge is on maintaining security in open systems (as people will not anymore accept locked systems). Suggestions were made along the line of: a) accepting that security is not a goal in itself, b) selecting a “field of technology” and help improving security and privacy (by generating additional code), and c) security and privacy must be done in an “open process” that allows the world to contribute and scrutinize. The example of the FP7 project PrimeLife⁴ was mentioned in relation to security considerations on social networking.

The presentation *Towards Viable Security Solutions – A Pragmatic Approach* suggested that the economics of security and privacy should be considered as a new discipline that is highly fragmented but provides great opportunities for future research. Most of the work concerns single case studies, focusing on specific technologies or particular user requirements, whilst researchers belonging to certain discipline often seem to have poor awareness of the contributions made by researchers from different disciplines. As a consequence, what is missing is a holistic approach to the topic by integrating interdisciplinary researchers to develop a clear and well-structured research agenda that provides a framework to integrate the different research streams. The presentation was targeted towards a “viable security” approach, based upon considering the combined dimensions of effectiveness and market demands compliance. A security solution would only be viable when it has already succeeded on the market, and has been adopted. A number of methods for assessing market compliance was proposed, namely: a) ex-ante evaluations grounded in diffusions of innovations and technology acceptance theory (to predict market performance of security solutions), b) stakeholder analysis (to elicit preferences of all stakeholders involved in a structured and complete form), and c) conjoint analysis (to measure consumer preferences and willingness to pay for product features). In summary, the presentation emphasized security to be considered as a

⁴ Sustainable privacy and identity management to future networks and services. <http://www.primelife.eu>

multidisciplinary issue that must be addressed in a multidisciplinary way, where much more research is necessary.

The presentation on *Innovation potential and barriers of security products and services - A perspective on Security Innovations (in Europe)* took innovation in security as a starting point, emphasizing not only the scientific and technological breakthroughs but in particular the importance of the budgets devoted to that purpose (in comparison with those allocated in the US, for instance). Security was defined as reactive by nature, but not in all cases responsive. An extensive list of barriers was provided, namely on barriers to entry to the market, challenges similar to ICT-industry, barriers to growth and barriers to exit. The presentation outlined a number of innovations in Information Security at European level. . The *European Security European Innovation Network* was referenced in terms of their aim to expand the existing security sector cluster infrastructure within North-West Europe to increase opportunities for small and medium-sized businesses for new innovations, and to improve their competitive advantage in the global security market. The network is composed of a number of participating clusters: SITC (Security Innovation and Technology Consortium), Systematic Paris Region, LSEC, TeleTrust Deutschland and Cluster Seguridad, among others. The network already represents over 1350 companies, reaching over 10.000 security professionals in Europe, collectively representing over 10 billion € market and having more than 10 leading universities and research centres involved.

The *Science-Business presentation* introduced the *Science|Business* organization as a team of experts in communications, innovation and European R&D, where academia, industry and policy makers are broadly represented. The organization has been designed to act as a platform, able to activate and involve experts throughout top-level networking events and many other activities. *Science|Business* proposed to use its growing network to facilitate efforts to promote standards, certification and best practice in trustworthy ICT, stimulate and organise interplay between technology development and research, whilst pushing for open innovation and investor-driven innovation.

The presentation on *Why Johnny can't afford Security Technologies* introduced a number of considerations based on the economic consequences of introducing a "sensible expressive security policy" in a specific organization. At the end the associated investments and operational cost could be expressed in a so-called "user value unit" (e.g. instead of applying such expressive security policy the organization could have opted to hiring 20 new associate professors). As a consequence, multiplication (of costs and investments) hurts innovation, whereas vendors' models are based upon correlation between the number of users and what is managed, rather than the number and type of product components installed. Recommendation was made on the need to know the reality before starting selling a product (as many costs only materialize when those products are tried or operationally implemented) and the need for user trials, benchmarks and data sharing, whereas a significant difficulty comes from the lack of sufficient information on security setting and incidents (that are kept confidential as they can lead to significant reputation damages). A reference was made to considering applying legislative solutions similar to those applied in avionics, where in case security incidents are identified, it is mandatory to investigate them and provide public conclusions and recommendations.

The overall discussion started on whether there is sufficient action on innovation. The workshop participants agreed on the fact that there should be proportionality between functionality and security, as security-related running costs are probably even higher than what was expressed. The fact that innovation is more a supply than demand-driven issue was highlighted, and subsequently a discussion started on how the demand in security could be increased in terms of innovation. A distinction was made between innovation at the firms' level and at the societal level, this leading to the existence of different roles depending on the nature of the involved stakeholders. It was mentioned that the effect of regulation on the mandatory need to implement firewalls and antivirus resulted in its broadest implementation. Whether this should be expanded to broader security aspects was subject of a number of speculations.

In terms of the demand side, many of the arguments are based upon business/companies considerations, whilst users/citizens dimensions are still relatively unknown. There is a need to explore service typologies that are able to match their security expectations without compromising functional or business aspects. Considerations were made about the significant difference between the costs of physical security versus cost of information security (10%).

The participants agreed on the fact that security is a deferred cost, and new business models should be developed accordingly. The role regulation should play was discussed in terms of catalysing effects (an example was made on the regulation of safety belts in cars, and the consequences of its implementation by the car industry).

In terms of identified topics, the outcomes were: a) the security space is very fragmented, b) there is room for improving demand-driven innovation complementing supply-driven innovation, this resulting in opportunities for further revision of the role of users representing the demand side (market driven business, policy driven for citizens), c) the need to investigate ways of making security to become a revenue stream rather than a replacement of a cost.

There was also consensus that public sector is an important player in the demand for security (20% of the current market), and that solutions have to be thought of in terms of functionalities for the future (mature by 5-10 years) rather than restricted to the current situation, needs and technologies. Demand will change radically over time, and it is reasonable to assume that technology will automatically incorporate security, although it is not totally clear how the technology will evolve (technologists and economists should therefore start working together with policy makers). The role of the public sector is multi-faceted, as it can regulate, procure, and use security-based solutions. There is a need to specifically transfer to the political level what should be considered in terms of regulation or policy aspects, together with substantial and well-developed justifications.

4.4. Privacy balance of power/Trust Measurement

The session, chaired by Roger Torrenti, was supported by the following presentations:

- *Interplay between Online Privacy and Data-centric Business Models*
Andreas Albers - Goethe University Frankfurt
- *COSIC: COmputer Security and Industrial Cryptography Presentation*
Claudia Diaz – KU Leuven
- *Trust measurement*
Antonio Lioy - Politecnico di Torino
- *Trust, Security and Privacy (TSP) Measurement*
Reijo Savola - VTT Technical Research Centre of Finland
- *Research status and suggestions for FP8*
Roger Torrenti - Sigma Orionis / PARADISO project coordinator

The presentation *Interplay between Online Privacy and Data-centric Business Models* started by making a number of considerations on Online Business Models versus User Privacy. Although users are increasingly becoming aware of privacy threats and have already started demanding to be protected while using Online Services, many business models are based upon somewhat limited user privacy. A number of research questions were raised, namely on the interplay between user privacy and data-centric business models, where there is a need to better understand how online businesses will respond to potential negative impacts of increased user privacy, and on how users will respond to the potential changes of Online Services offerings due to their lack of user data. The final suggestion was on developing further research a) to better understand the interplay between user privacy and online business models, and b) to explore enabling fair data-related interactions between users and online business.

The presentation *COSIC: COmputer Security and Industrial Cryptography Presentation* focused on the current activities and areas of interest of COSIC, the privacy subgroup of the KU Leuven Dept. of Electrical Engineering-ESAT. The activities on formalization, modelling and quantification of privacy properties were presented, and specific attention was given to the importance and significance of traffic analysis in security. A lot of sensitive information can be inferred just throughout analysing the submenus dynamics in the user interactions, thereby compromising privacy dimensions. Social networks dynamics are another source of potential security breaches (as an example, the observation of a number of changes in liaisons in LinkedIn in a specific time frame could allow to predict a potential merger of companies). The cloud is also opening new spaces and challenges as far as traffic analysis is concerned. In any case, it was recognized that social networks contributed to security user awareness much more than ever before. The COSIC subgroup expressed their interest in progressing in research on traffic analysis in relation to location privacy, social networks and anonymous communications.

The presentation on *Trust measurement* referred to a number of finalized and ongoing R&D projects involving TORSEC, the group on security of University of Torino. The

presentation introduced the concept of complete binary measurement of a system security. This is possible and has already been tried, although with trust as a subjective measurement or measure against (subjective) relevant issues. Accordingly, specific requirements and expectations versus contract-manifest (as provided by suppliers) should be expressed, defining for instance the balance among confidentiality, integrity and availability. Importance was given to ex-ante versus ex-post measurement, together with the role to be played by trusted, robust and dependable logging. The importance of this role becomes evident in the cloud, as forensic interventions (typically made by taking out the hard disks for detailed investigations) will no longer be possible without getting logging information on what the data was, where the data was stored and which changes were made over time.

The presentation on *Trust, Security and Privacy (TSP) Measurement* introduced references to a number of trust factors as identified in one of the biggest national projects over cloud services in Finland⁵, differentiating between non-functional and functional trust factors. In terms of main security and privacy measurement objectives, effectiveness was found as the main objective (together with correctness, due to the relationship with software intensive systems). A trade-off between security and efficiency has been identified, whereas TSP visualization techniques (colour codes, details) were found to be of significant importance. Further research is needed in a widely accepted “trust, security and privacy metrology” framework, for which realistic cases and data are still needed.

The presentation on *Research status and suggestions for FP8* introduced the perspectives from the PARADISO FP7 project⁶. The project was launched at the initiative of the Club of Rome, and it is a forward-looking analysis to better understand Internet-societies interactions and to identify new innovation paths. Their key outputs will include a document with recommendations to the EC (a call for action from the PARADISO high-level expert panel) and a conference to be organized on Sept. 7-9 2011 including the launch of the “*Platforms for collective awareness and action*” initiative.

The overall discussion recognized the importance and significance of all presentations’ contributions. The need for revising the interplay between user privacy and online business models was acknowledged, together with the interest of enabling fair data-related interactions between users and online businesses. The discussion confirmed that some empirical work has already been done (e.g. study of the impacts on advertising industry, depending the kind of ad).

The ideas in traffic analysis were broadly discussed, progressing in a number of interesting issues like the perception that “trust” is somewhat related to “blind trust” on companies, as an indirect effect of branding (people tend to trust companies). Further research is still needed to better understand the consequences of changes of privacy, which could also result in changes in efficiency. A potential topic was the investigation on applying security SLAs, which could become a new research area in itself. The

⁵ Cloud Service Expert interview Study. * Uusitalo, I., Karppinen, K., Juhola, A. and Savola R. Trust and Cloud Services – An Interview Study. 2nd IEEE Int. Conf. on Cloud Computing Technology and Science. Finland (2010)

⁶ www.paradiso-fp7.eu

concept of “protection by default” was also proposed as an alternative. In any case, the linkage of free services with access to user information to target services offerings needs further investigation, in particular on whether this could eventually result in cutting down incomes for online services offerings.

The idea of exploring security-related business models was welcomed, with the reservations that an approach based on “protecting the users against the service provider” could result in unexpected consequences. This would need further research (as for example providers could find ways of bypassing any attempt in this respect).

4.5. Security information and data for research, industrial and strategic decision-making

The session, chaired by Michel Van Eeten, was supported by the following presentations:

- *Socio-economics in Trustworthy ICT*
Julian Williams - University of Aberdeen
- *Economic Incentives to Enhance Trustworthy ICT: The Role of Intermediaries*
Michel Van Eeten, Hadi Asghari - Delft University of Technology

The presentation on *Socio-economics in Trustworthy ICT* outlined that at present there are a great number of risk management models available to assist security practitioners in decision making. Most of these models rely on some form of measurement of the risk environment. However, at present there are only a few public datasets available to undertake this type of measurement exercise:

- NIST-CVSS database (crude scoring system, not enough variation without integration with a company specific systems model)
- OWASP DREAD Classification system (massively incomplete)

The information commonly stored in these dataset is useful, but it is classified in such a way that mapping to simple models of policy maker preferences is impossible. Third party vendors also have extensive datasets but at present appear unwilling to make these available for public use. The presentation suggested considering two opportunities to start correcting the referenced situation: a) case study research for medium-large organizations on the interactions of threat contained within the various datasets and a manual on how to integrate them with the state-of-the-art in dynamic optimization models, and b) Large scale agglomeration of the various datasets into a coherent “threat index”, with known volatilities, skews and clustering. An important remark was made on the fact that data at present is fragmented and difficult to use without extensive cleaning, this severely affecting models (that are as good as the data used to parameterize them). It was also considered important to point out a pressing need for consolidation and agglomeration of disparate sources into a time index (with daily or weekly variations) maintained by experienced index providers.

The presentation on *Economic Incentives to Enhance Trustworthy ICT: The Role of Intermediaries* focussed the discussion on the believe that Trustworthy ICT is increasingly dependent on efforts of Internet intermediaries such as ISPs, financial service providers, search engines, e-commerce, and m-commerce. As a consequence, the key research question was: what economic incentives (including regulatory) shape the security decisions of Internet intermediaries? The presentation gave an overview of the lessons learnt from recent research on the situation of infected machines in wider OECD located in ISP networks. The applied methodology used different data sources to locate infected machines, whilst for each IP address the study looked up the country and ASN⁷, mapped ASNs to ISPs (and non-IPs) in 40 countries, connected data on

⁷ Autonomous System Number

infected machines with economic data (e.g. # subscribers of ISP) and compensated for known measurement issues. The research found that 31 ISPs were in the top 50 in all four examined years, meaning that only resolving the security issues with those 31 ISPs would have a relevant incidence in solving the issue. The research showed that regulatory incentives improve security of ISPs (for example, countries where regulators participate in the London Action Plan⁸ have lower infection rates, this highlighting an indirect effect). A number of key topics for further research and knowledge were proposed: a) Economic factors driving security performance of intermediaries; including the spread of malware in access networks, security in clouds, social networks, and mobile networks, b) Market signals and transparency (e.g., open source software tools to analyse security performance of intermediaries), and c) Interplay between security and other regulatory objectives (e.g., privacy, copyright protection, net neutrality, censorship including child porn filtering).

The overall discussions lead to verify the validity of the research suggestions made by the presentations. Although the lack of incentives for benchmarking was evident, its need was unanimously recognized. It is uncertain whether improvement in security could result in probability for lowering insurance costs. An unresolved problem is that models are based upon past data, and it is unclear how to make them adaptable for the future, as there is no sufficient information on security (insurance is a mature sector where historical information is already available). The potential of using national risks incidents logs was outlined, but they are poor and incomplete. As far as incentives for intermediaries go, the consideration of reputation metrics was seen as an opportunity, although the need for a trial and error approach was recognized in the earliest research stages. The discussion suggested other sources of risk index, like the FIRE (*F*inding *R*ogues *E*) Networks index⁹. The participants agreed on the interplay between security and other regulatory objectives, this being an interesting area for further research and progress.

⁸ The purpose of the London Action Plan is to promote international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses. <http://www.londonactionplan.com>

⁹ <http://maliciousnetworks.org>

ANNEX I. ATTENDANCE LIST

Family name	Name	Organisation
ALBERS	Andreas	Goethe University
ASGHARI	Hadi	Delft University of Technology
CALZAROSSA	Maria Carla	Universita' di Pavia
DAMIANI	Ernesto	University of Milan
DIAZ	Claudia	KU Leuven
ESTEBAN	David	Techforce
FELEGYHAZI	Mark	BME
FRITSCH	Lothar	Norwegian Computing Center
LIOY	Antonio	Politecnico di Torino
MAISEL	Steven	Science Business
MASSACCI	Fabio	DISI- Universita di Trento
MEISSNER	Sebastien	Datenschutzzentrum
PYM	David	University of Aberdeen
ROSSNAGEL	Heiko	Fraunhofer
SAVOLA	Reijo	VTT Research Center
SELDESLACHTS	Ulrich	LSEC, Belgium
STIRNAL	Andy	European Security Round Table
TORRENTI	Roger	Sigma Orions
VAN EETEN	Michel	Delft University of Technology
WENNING	Rigo	W3C
WILLIAMS	Julian	University of Aberdeen
ANTON GARCIA	Maria	DG INFSO
FORT GONZALEZ	Anna	DG INFSO
JUCEVICIENE	Vilija	DG INFSO
MUECHLECK	Martin	DG INFSO
NIELSEN	Oluf	DG INFSO
OLIMID	Cristian	DG INFSO
SCILLA	Mario	DG INFSO
VILLASANTE	Jesus	DG INFSO