enisa
European Network and Information Security Agency

Economics of Security: Facing the Challenges

A multidisciplinary assessment

Acknowledgements

This report is the outcome of a collective effort by all the participants in the working group that was established by ENISA with a view to study the priority topics relating to the Economics of Security. ENISA would like to thank (in alphabetical order) Eyal Adar, Fabio Bisogni, Rainer Böhme, Tilman Brück, Simona Cavallini, Nicolas Christin, Jens Grossklags, Christoph Janello, Johann Kranz, Thomas Nowey, Arnold Picot, David Pym, Michael Rath, Ralf Schneider, Rahul Telang and Jeremy Ward, who provided valuable input, material and prompt support for the preparation of this report. The working group experts have contributed to the addressed topics as follows:

Economics of resilience: By Professor David J. Pym, PhD, ScD, FIMA, FBCS, University of Aberdeen, Scotland and Ralf Schneider, TÜV Informationstechnik GmbH, Essen, Germany

Behavioural economics of Security: By Nicolas Christin, Carnegie Mellon University and Jens Grossklags, Pennsylvania State University

Economic Incentives for Security: The role of public goods: By Arnold Picot, Christoph Janello, and Johann Kranz (Ludwig-Maximilians University Munich, Munich School of Management, Institute for Information, Organization and Management, Ludwigstr. 28 VG/II, 80539 Munich, Germany

Economic Incentives for Security: The role of information asymmetry and lack of information: By Simona Cavallini and Fabio Bisogni, Fondazione FORMIT, via Giovanni Gemelli Careri 11, 00147 Rome, Italy

Economic impact of intervention policies: By Simona Cavallini and Fabio Bisogni, Fondazione FORMIT, via Giovanni Gemelli Careri 11, 00147 Rome, Italy

Collection of data on security incidences: By Dr Thomas Nowey, Krones AG, Neutraubling, Germany

Software liability: By Prof Dr Rainer Böhme, Westfälische Wilhelms-Universität Münster, Germany, Dr Michael Rath, Luther Rechtsanwaltsgesellschaft mbH, Cologne, Germany, Ralf Schneider, TÜV Informationstechnik GmbH, Essen, Germany and Prof Rahul Telang, Carnegie Mellon University, Pittsburgh, PA, USA

Return on Security Investment (ROSI): By Jeremy Ward, HP Enterprise Security Services

IT Security Risk Management of Business processes: By Eyal Adar, White Cyber Knight Inc., Bnei-Brak, Israel and Ralf Schneider, TÜV Informationstechnik GmbH, Essen, Germany

We would also like to thank Alessandro Acquisti, Richard Clayton, Michel van Eeten, Reinhard Hutter, Andrea Renda and Ingrid Schaumueller-Bichl who, in addition to the working group members, gave their valuable input to the online public consultation performed by ENISA.

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of expertise for the European Union (EU), its Member States (MS), the private sector and Europe's citizens. As an EU agency, ENISA's role is to work with these groups to develop advice and recommendations on good practice in information security. The agency assists MS in implementing relevant EU legislation, and works to improve the resilience of Europe's critical information infrastructure and networks. In carrying out its work programme, ENISA seeks to enhance existing expertise in MS by supporting the development of cross-border communities committed to improving network and information security throughout the EU.

Contact details

For contacting ENISA or for general enquiries on the Economics of Security, please use the following details:

Louis Marinos, Senior Expert Risk Analysis & Management

Email: louis.marinos@enisa.europa.eu

Aristidis Psarras, Awareness Raising Officer

Email: aristidis.psarras@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Legal notice

section 6

section 7

section 8

List of Tables

1. Executive summary

This ENISA report is part of the work conducted within ENISA's 2011 work programme. As part of this effort, ENISA has analysed economic drivers and barriers in a number of areas (including policy, research, technology and business) and has identified potential areas of improvement to boost security and resilience in public systems and networks and consequently in relevant products and services by taking into account the economic dimension. This effort contributes to the identification of topics in the area of Economics of Security in line with the efforts to boost Europe's economic performance and introduce measures to reinforce the benefits of the single market, as announced in the Digital Agenda for Europe.

Highlights of this work are:

- A comprehensive analysis of the broad area of Economics of Security and an analysis of open issues and pending activities in each area.
- Identification of the relevant stakeholders, their role and the activities they should contribute to.
- Identification of the policy impact of the identified topics relating to the Economics of Security, thus providing a good basis for dialogue not only at the European level, but also at the level of Member States and the international community.
- Identification of the effect of business challenges – emanating from international developments in the market – on the Economics of Security. Such challenges shed additional light on the extent to which decision-makers in both business and policy arenas take account of the identified topics.
- Priorities of the identified topics relating to Economics of Security from multiple perspectives such as policy, business, research and maturity level of underlying concepts.
- Last but not least, with this effort ENISA attracted contributions from various important multidisciplinary experts who have supported the agency in this work. These experts are an important source of knowledge and networking in the field of Economics of Security

These essential elements are discussed in detail in the body of the report.

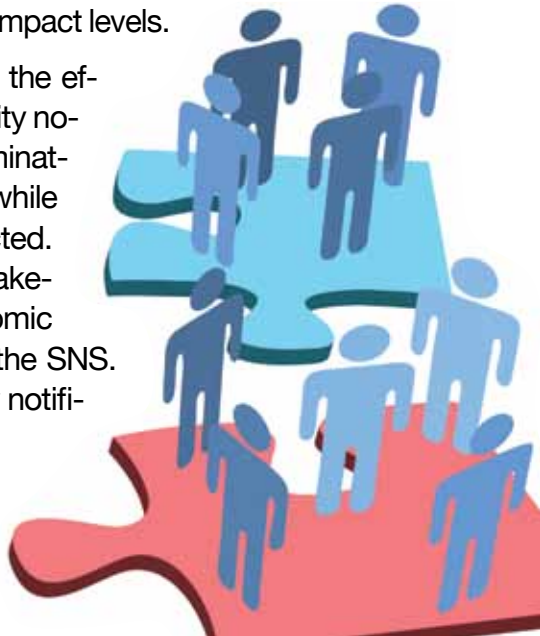
The task performed involved analysis as well as a synthesis of gathered knowledge. Once the analysis was completed, ENISA identified key issues that need to be addressed in the short term. As part of this work, ENISA identified particular stakeholders affected by this challenging environment, such as consumers, industry and the state. ENISA has established a working group to deepen discussion on the identified topics relating to the Economics of Security.

For each topic, the working group suggested several action points along with the stakeholders that seem to be best positioned to take action. Some of the most important action points that emerged through this work are:

1. To harmonise EU resilience legislation and to achieve effective enforcement of such legislation across Europe. This is primarily the re-

sponsibility of the European Commission and the legislators of the European Union, namely the European Parliament and the Council. The national authorities also have an important role to play in this effort.

2. With reference to behavioural economics, it seems that there is insufficient scientific material and empirical data. Research institutions and universities should study the economic relationships of the actors involved in fraudulent activities with a view to evaluating the efficiency of various intervention mechanisms (e.g. technical, social, organisational, etc.) to prevent such fraud.
3. Another action point would be for incentives (penalties or rewards) to be established both at EU and national level for ISPs that detect and clean up infected computers.
4. The sector regulators and authorities should conduct ex-post evaluation of the effects of current security policies. Such evaluations should have a short-term view but also some conclusions concerning the medium term, taking into account the specific sources of threats.
5. Collection of data on security incidents is another key topic of Economics of Security. The European Institutions should put in place common incident taxonomy and a common data pool of security incidents along with their impact. On the other hand, national authorities and sector regulators should establish benchmarking methods with a view to facilitating effectiveness and efficiency.
6. The European Institutions should issue a software liability programme to be introduced on a gradual basis, involving multidisciplinary stakeholder teams. Moreover, software developers and vendors should model realistic market scenarios related to software liability.
7. In order to achieve wider adoption of ROSI techniques, governmental agencies and private enterprise organisations need to cooperate with one another. Government suppliers should implement the ROSI certification with a view to providing assurance on the methods applied for public spending on IT Security.
8. Concerning IT security risk management of business processes, the key role is with the research institutions and universities. They should find methods to classify the economic value of IT assets, to identify the business impact of IT assets and to set the measurement parameters of business impact levels.
9. The national authorities should take the lead in enhancing the efficiency and effectiveness of information sharing and security notification schemes. They should adapt collected and disseminated information to the needs of participating organisations while maintaining statistics about all kinds of information collected. They should establish feedback loops with all types of stakeholders concerned and they should ensure that the economic perspective is duly taken into account when establishing the SNS. Finally, they should assess barriers and benefits of security notification schemes on an ongoing basis.



2. Introduction

As outlined in its 2011 work programme, ENISA analysed economic drivers and barriers in a number of areas (including legal, policy, technical and educational) and identified potential areas of improvement to boost security and resilience in public systems and networks and consequently in relevant products and services.

This effort also contributes to the identification of security requirements, particularly in public procurement for ICT products and services. This work also elaborates on economic issues (e.g. total cost of ownership, return on investment, etc.) arising from the fulfilment of such requirements. In this way, this work contributes to the points of the Digital Agenda for Europe, such as boosting Europe's economic performance and introducing measures to reinforce the benefits of the single market.

There is an ongoing debate at the international level on these issues, which has resulted in several studies and analyses. ENISA collected and analysed the existing knowledge available, to avoid duplication of work, and thus created a solid view of the complex issue of 'Economics of Security'. For this purpose, experts in this area were contacted and their views on open issues in the area of Economics of Security assessed.

The working group established for this study has acted as the main instrument to fulfil this task. To do this effectively ENISA adopted a multidisciplinary approach, with members combining a variety of skills pertinent to the area of Economics of Security (i.e. economists, legal experts, sociologists, representatives of consumer organisations and industry bodies). The working group has supported ENISA in the further analysis of the topics addressed by the expert community during the open consultation.

Among the most common topics that emerged in this open consultation were:

1. Information sharing and notification schemes
2. Economics of resilience
3. Behavioural economics of security
4. Economic incentives for security: The role of public goods
5. Economic incentives for security: The role of information asymmetry and lack of information
6. Economic impact of intervention policies
7. Collection of data on security incidents
8. Software liability
9. Return on security investment (ROSI)
10. IT security risk management of business processes

It is worth mentioning that the above priority topics of Economics of Security are not

listed in priority order. The list rather reflects the sequence of topics as they were identified and processed within the working group. Priorities have been assigned to these topics according to a multidimensional scheme (see Chapter 6).

Furthermore, it should be noted that this list is non-exhaustive and reflects the material assessed by our initial stock taking. The above topics have built the foundation for the work of the ENISA working group.

For the work conducted, previous ENISA deliverables have been taken into account; in particular the work on 'Security Economics and the Internal Market' (http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport).

The present document is a consolidation of the work of the working group and provides a short description of the identified topics, together with a stakeholder mapping. In this document, we assess existing business challenges affecting the Economics of Security, as well as the policy impact of the identified topics. The document lists the identified topics relating to Economics of Security by priority according to a multidimensional approach.

The contributions the members of the ENISA working group are presented in a separate document (named 'Economics of Security – Full Length Contributions') as they were submitted by the experts. This document contains detailed information on each topic relating to the Economics of Security, including open issues, future activities, stakeholders involved and references to relevant work at international level.

3. The big picture

This section presents an overview of the topics identified within the wider context of economic issues in line with the outcome of the deliberations within the relevant working group (see Figure 1).

It also considers the context of the topics identified, with regard to Policy, Social, Process/People, and Technical dimensions. Because this overview reveals only a small part of the details and interrelationships of the topics, we have developed it in order to help readers to see at glance the main topics relating to Economics of Security, as assessed from the survey carried out for this study and the discussions of the working group.The axes in Figure 1 represent the following information:

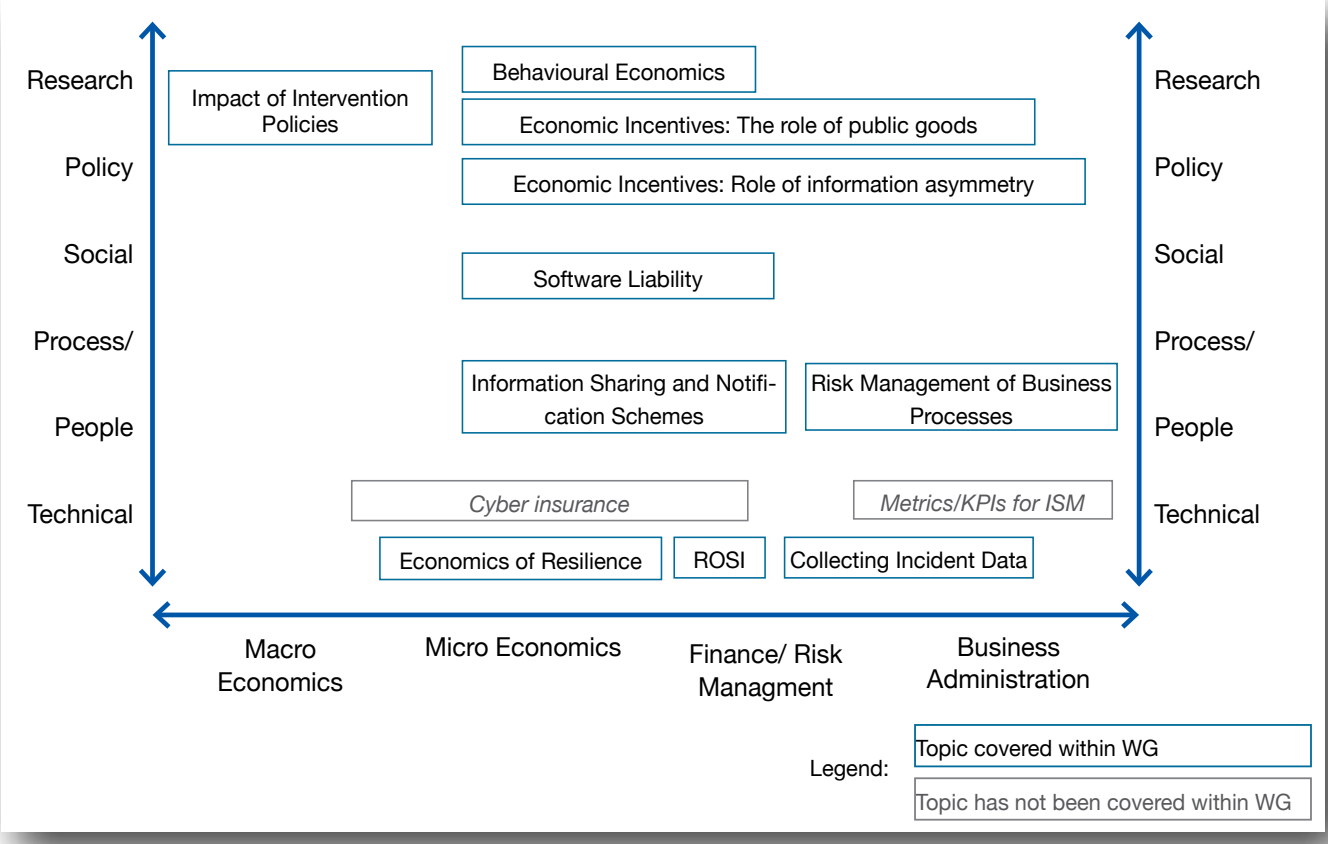


Figure 1: Overview of identified topics of Economics of Security

The horizontal axis shows various areas of economics, from 'macro-economics' to 'business administration'. The closer a topic to the macro-economics, the stronger is its relationship to economic theoretical issues. Example: 'economic incentives' is considered to be a topic that entails micro-economic issues but has macro-economic impact. The closer a topic to 'business administration', the stronger is its relationship to specialised applicability, e.g. within business practices. Example: 'risk management of business processes' is an activity that can be established within a company in order to identify risks connected to implemented processes.

The vertical axis reveals the context of the various topics. The closer a topic to policy, the greater is its relevance to political decision-making and political action. For example, 'impact of intervention policies' is a topic that needs to be part of political decision-making and be addressed at the level of policymaking. The closer a topic to technical issues, the more it can be addressed by using existing technical solutions. For example, the collection of incident data is an issue that can be addressed by using existing technological solutions from the area of intrusion, incident detection, IT audit, forensics, etc.

Another dimension that becomes apparent in Figure 1 is that of applicability and scope: it is obvious that topics closer to the corner 'technical – business administration' are easier to implement and find solutions to, because their applicability is more specialised and the scope is reduced. Topics close to the other end (i.e. 'micro-/macro-economics – policy') will be more difficult to develop/apply as they have a very broad applicability and scope, and they involve macro- and micro-economic relevance and national/international scope.

Not all topics relating to the Economics of Security identified during the ENISA survey were addressed by the working group. 'Cyber insurance' and 'Metrics for information security management' have been left outside the current focus, as the available expertise led us to concentrate more on the other topics.

The following sections give a short overview of the 10 identified topics of Economics of Security. In each case the topic is described and a list of activities given. The activities comprise a roadmap for each topic. Furthermore, for every topic there is a stakeholder mapping, visualising the indicative role of involved stakeholders. A distinction is made between two roles for the involved stakeholders, namely responsibility and contribution. The stakeholder mappings show which stakeholders are involved in which activities of a topic, under which role.

The following material has been derived from the contributions of the members of the working group. The contributions are presented in full length in a separate document named 'Economics of Security – Full Length Contributions' that includes also tables with detailed stakeholder mapping.

Bibliographical references have been omitted in the present report but they can be found in the full-length contributions of the working group members as mentioned above. For the topic 'Information sharing and security notification schemes' no contribution exists by means of a paper detailing this topic.

3.1 Economics of resilience

Resilience is a vital requirement for the internal market of the EU. Setting an EU policy frame and homogeneous legislation with due enforceability for a resilient IT will support future wealth even in the case of serious distortions and hazards. In any event, decisions should be compatible with an incentives

regime. Realistic options should be based on state-of-the-art measures promising optimal resilience of identified critical infrastructures from a practical point of view. The balancing of utility (social wealth) and costs, while at the same time avoiding externalities, is crucial before decisions are made.

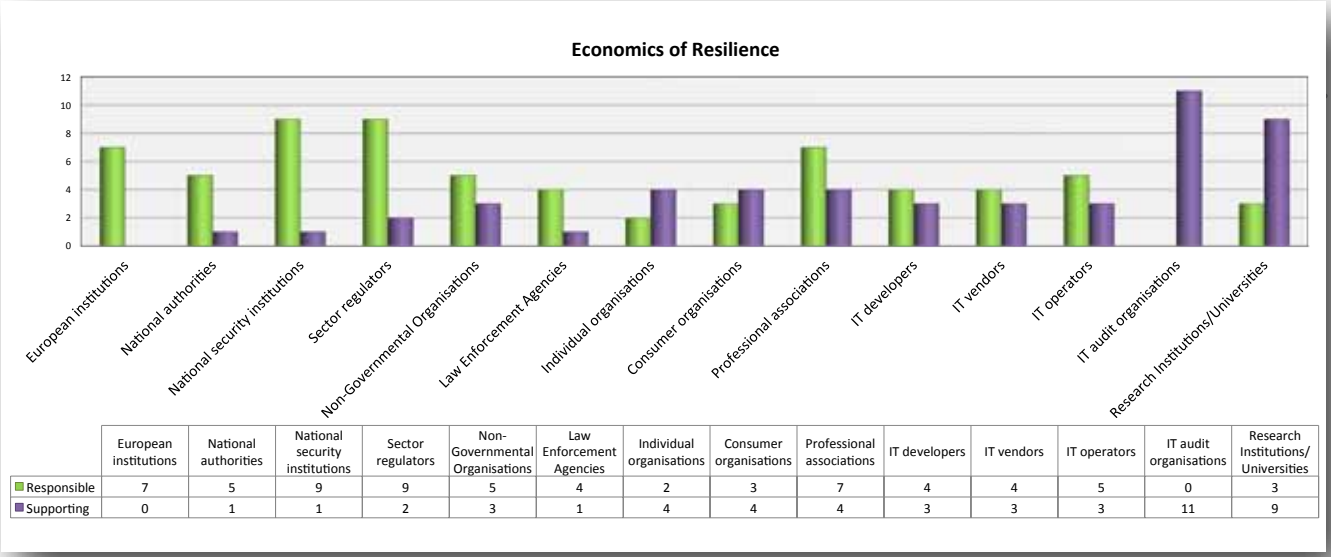
A dedicated multidisciplinary team of stakeholders might prepare bundles of course of actions for numerous realistic scenarios applicable to the EU internal market and identify the most promising sets based on thorough, in-depth analyses. The results will then be the resilience tools for the decision-makers in alignment with existing policies and directives. However, an appropriate blend between the technical competence of the multidisciplinary team and the policy/regulatory competence is a prerequisite in order to achieve the appropriate result.

The identified activities and stakeholder engagement for Economics of Resilience are as shown in Table 1.

Identified activities X: responsible (X): supporting	Stakeholders													
	European institutions	National authorities	National security institutions	Sector regulators	Non-governmental organisations	Law enforcement agencies	Individual organisations	Consumer organisations	Professional associations	IT developers	IT vendors	IT operators	IT audit organisations	Research institutions/universities
Set a policy on EU resilience expectations of information infrastructure compatible with an incentives regime	X	(X)	(X)	(X)										
Issue an EU resilience programme with resilience objectives and involving multidisciplinary stakeholder teams	X	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)
Gain a common understanding of information infrastructural resilience on national and international level	X	X	X	X	X	X	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)
Harmonise EU resilience legislation	X	X		X	(X)	X							(X)	(X)
Ensure enforcement by compulsory resilience regulations on multinational level	X	X	X	(X)		X			(X)				(X)	(X)
Identify critical information infrastructures	X	X	X	X	(X)	X		X	X			X	(X)	(X)

Identified activities X: responsible (X): supporting	Stakeholders													
	European institutions	National authorities	National security institutions	Sector regulators	Non-governmental organisations	Law enforcement agencies	Individual organisations	Consumer organisations	Professional associations	IT developers	IT vendors	IT operators	IT audit organisations	Research institutions/universities
Issue holistic incentives for a resilient information infrastructure	X	X							(X)	(X)	(X)	(X)	(X)	(X)
Model realistic scenarios of the internal market			X	X	X				X				(X)	X
Balance utility (social wealth) and costs, avoiding externalities in the model			X	X	X				X					X
Identify state-of-the-art measures promising optimal resilience			X	X	X		X	(X)	X	X	X	X	(X)	(X)
Identify most promising bundles of courses of action based on thorough in-depth analyses			X	X	X		X	(X)	X	X	X	X	(X)	X
Develop criteria for a resilient design and architecture of IT components, systems and networks			X	X			(X)	X	X	X	X	X	(X)	(X)
Develop criteria for organisational and procedural resilience			X	X			(X)	X	X	X	X	X	(X)	(X)

Table 1: Economics of resilience: Identified activities and stakeholder engagement



	European institutions	National authorities	National security institutions	Sector regulators	Non-Governmental Organisations	Law Enforcement Agencies	Individual organisations	Consumer organisations	Professional associations	IT developers	IT vendors	IT operators	IT audit organisations	Research Institutions/ Universities
Responsible	7	5	9	9	5	4	2	3	7	4	4	5	0	3
Supporting	0	1	1	2	3	1	4	4	4	3	3	3	11	9

Figure 2: Economics of resilience: Overview of stakeholder engagement

3.2 Behavioural economics of security

The behavioural economics of security aims to advance the understanding of the struggles between attackers and defenders by integrating lessons from behavioural research conducted in the lab and field. It is possible to draw from a wide range of psychology research, usability and human–computer interaction studies, as well as network security measurements, to formulate more realistic explanations of how economic incentives and human instincts interact.

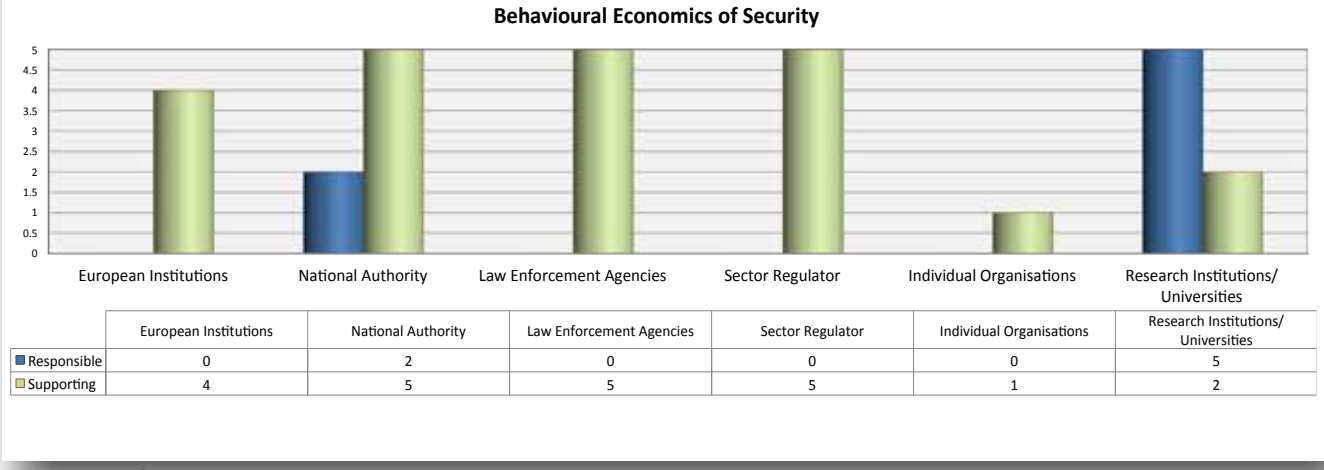
This complexity, as well as the frequency of situations with security relevance, is indicative of the significant cost of decision-making inflicted upon defenders and attackers. These costs are often unevenly distributed; for example because of strategic information advantages. As a result, making optimal security choices may be almost beyond the capacity of computers, let alone the human mind.

Several existing approaches in the behavioural economics of security need to be developed more fully and others, such as field trials, pilots, etc., need to be be applied more widely in order to shed more light on this important area.

The identified activities and stakeholder engagement for this topic are shown in Table 2.

Identified activities X: responsible (X): supporting	Stakeholders					
	European institutions	National authority	Law enforcement agencies	Sector regulator	Individual organisations	Research institutions /universities
Study economic relationships between actors behind current fraudulent activities. Objective is to evaluate efficiency of various intervention mechanisms (e.g. technical, social, organisational, etc.)		(X)	(X)	(X)	(X)	X
Investigate abuse patterns based on certain human behavioural traits of the victims to gain a better understanding of such aptterns. Develop ways to reduce relevant abuse		(X)	(X)			X
Collect and evaluate information (including qualitative measurements) on attacker success of various attack vectors		X	(X)	(X)		(X)
Develop security policies and controls, based on novel attack scenarios, to provide better protection. Evaluate and verify existing controls through exhaustive tests, including formal evaluation and verification methods	(X)	(X)	(X)	(X)		X
Elaborate on the formalisation of psychological insights in economic models (i.e. modelling of preferences, risk evaluation and behaviour, understanding of information and ambiguity, etc.)	(X)	(X)	(X)			X
Elaborate on incentives that emerge from interdependencies in interactions of multiple decision-makers (e.g. according to topological or other structural rules)	(X)	(X)		(X)		X
Develop intervention strategies in the area of behavioural economics (e.g. nudging)	(X)	X		(X)		(X)

Table 2: Behavioural economics: Identified activities and stakeholder engagement



	European Institutions	National Authority	Law Enforcement Agencies	Sector Regulator	Individual Organisations	Research Institutions/ Universities
Responsible	0	2	0	0	0	5
Supporting	4	5	5	5	1	2

Figure 3: Behavioural economics: Overview of stakeholder engagement

3.3 Economic incentives for security: The role of public goods

The fact that higher security comes at an increasing cost is becoming more and more obvious to many decision-makers; therefore tolerance of some level of insecurity is necessary for economic reasons. From an economic perspective, the key question is whether the costs and benefits perceived by market players are aligned with the social costs and benefits of an activity.

As the Internet itself can be seen as a public good, it is likely that ICT security shows public good characteristics as well. The consumption of public goods is not affected by rivalries in the domain or by excluding interested parties from involvement.

Total security is neither achievable nor desirable. Hence, each actor will carefully make a trade-off between costs and benefits associated with ICT security investments. Some level of ICT security is, however, a prerequisite for the globally interconnected economy to work. This is also true for the Internet's services to function. Basically a secure ICT infrastructure resembles a functioning banking sector, which is essential for doing business. Malevolent or careless users can cause harm to other users. Further incentives to invest in security are often misaligned as parties do not have to bear the costs of their behaviour entirely, if at all.

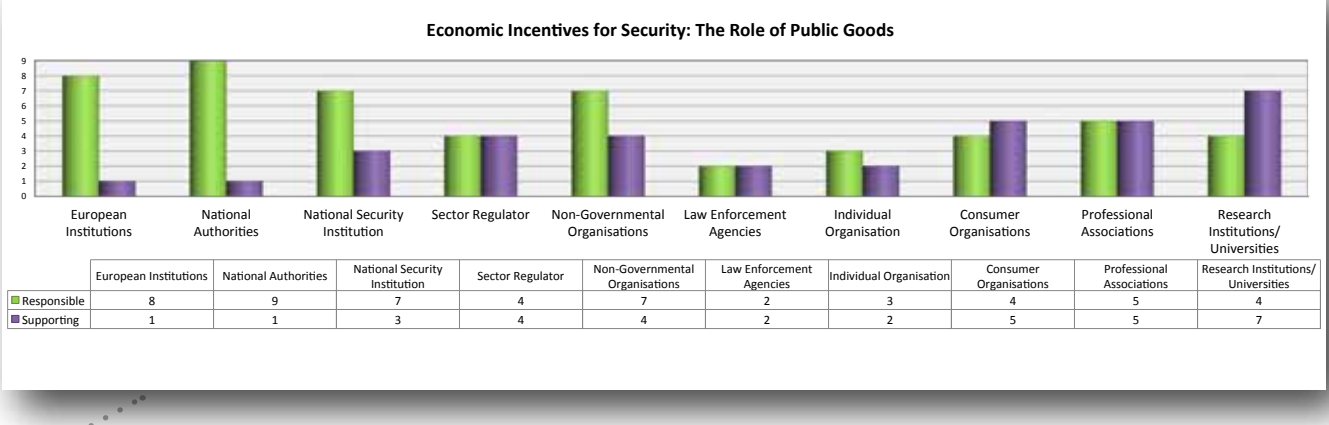
Due to these effects, ICT security can be regarded as a public good. If the existence of a public good is desired by society, its provision has to be safeguarded by means of regulatory intervention from some superseding level of governance. To these means pertain, e.g. legislation (such as liability laws), taxes, requirements, bans and rules and quotas, often designed to fight external effects.

The identified activities and stakeholder engagement for this topic are as shown in Table 3.

Identified activities X: responsible (X): supporting	Stakeholders									
	European institutions	National authorities	National security institution	Sector regulator	Non-governmental organisations	Law enforcement agencies	Individual organisation	Consumer organisations	Professional associations	Research institutions/ universities
More applied research on determining an appropriate level of IT security investments for firms (e.g. metrics)	X	X	X		X		X		X	X
Embedded instead of added security architectures for ICT systems		X	X	X	(X)		(X)	(X)	(X)	(X)
Investigating consumers' security-related behaviour and interventionist studies based on behavioural economics	X	X	X		X		X	X	X	X
Legal review of ISPs' rights to intervene in privacy to prevent malware attacks	X	X	X	(X)	X	(X)		(X)	X	X

Identified activities X: responsible (X): supporting	Stakeholders									
	European institutions	National authorities	National security institution	Sector regulator	Non-governmental organisations	Law enforcement agencies	Individual organisation	Consumer organisations	Professional associations	Research institutions/ universities
Define harmonised standards for security and resilience	(X)	(X)	(X)	(X)	(X)		(X)		(X)	(X)
Improving users' and firms' awareness and education	X	X	X		X			X	X	(X)
Establish third party certificates for stakeholders (ISPs, e-commerce, software vendors, etc.) when implementing state-of-the-art security measures			(X)	(X)	X		X	(X)	(X)	X
Incentives (penalties or rewards) for ISPs to detect and clean up infected computers (notify and quarantine infected users as done by Dutch ISPs or by means of a nationwide call centre (https://www.botfrei.de) as done in Germany)	X	X	X	X	X	X		X		(X)
Strengthen feedback loops by security breach disclosure laws	X	X	X	X	X	X		X	(X)	(X)
Security by law (such as replacing indexed TAN with mobile TANs)	X	X	(X)	X	(X)			(X)	X	(X)
Tightening of liability laws	X	X		(X)	(X)	(X)		(X)	(X)	(X)

Table 3: Economic incentives/public goods: Identified activities and stakeholder engagement



	European Institutions	National Authorities	National Security Institution	Sector Regulator	Non-Governmental Organisations	Law Enforcement Agencies	Individual Organisation	Consumer Organisations	Professional Associations	Research Institutions/ Universities
Responsible	8	9	7	4	7	2	3	4	5	4
Supporting	1	1	3	4	4	2	2	5	5	7

Figure 4: Economic incentives/public goods: Overview of stakeholder engagement

3.4 Economic incentives for security: the role of information asymmetry and lack of information

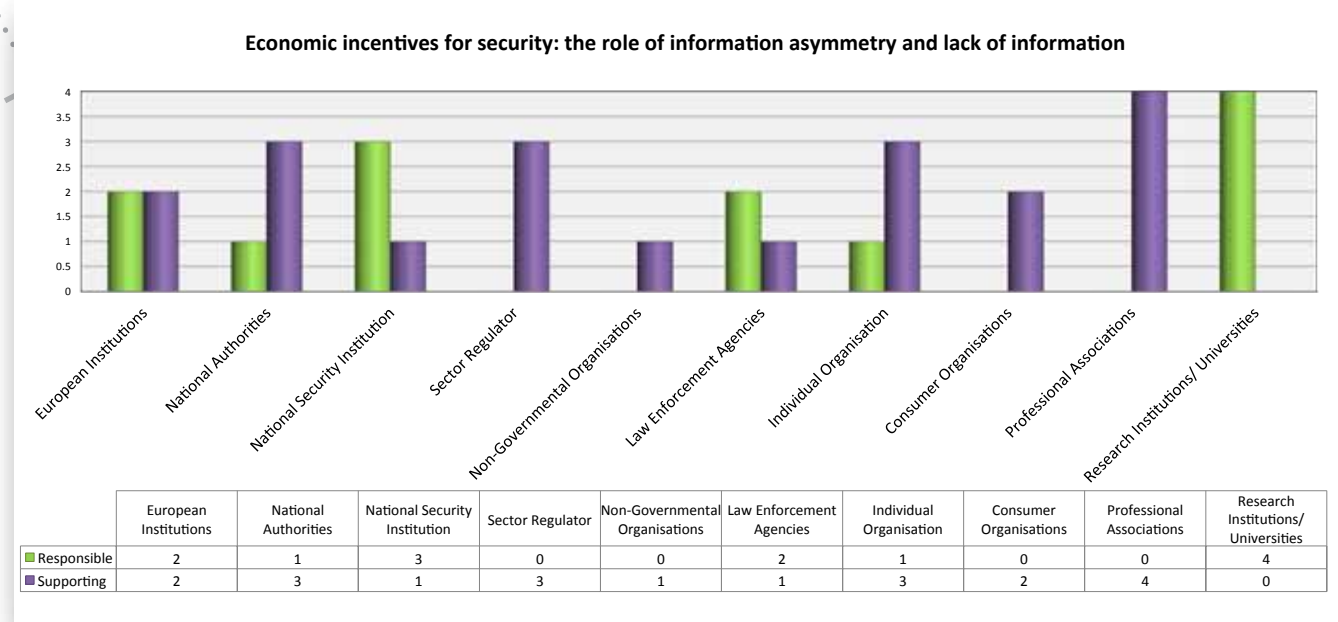
Each single type of stakeholder (e.g. citizens, NIS operator, infrastructure operator, public administrator) defines its security level according to potential damages suffered in case of a breakdown in security.

The current European policy debate and the most advanced studies on the economics of security have recently included the issue of responsibilities of protection and the attribution of the associated costs. In the separate document: 'Results Analytics of Stock Taking by Stakeholder Group', a number of references are presented in support of the analysis of this issue. To this effect different stakeholder types with specific roles in the security of information systems can be identified.

The identified activities and stakeholder engagement for this topic are as shown in Table 4.

Identified activities X: responsible (X): supporting	Stakeholders									
	European institutions	National authorities	National security institution	Sector regulator	Non-governmental organisations	Law enforcement agencies	Individual organisation	Consumer organisations	Professional associations	Research institutions/ universities
Define mechanisms to increase participation	(X)	(X)	X	(X)			(X)		(X)	X
Harmonise incident reporting procedures and define appropriate reporting schemes	(X)	(X)	X	(X)		X	X		(X)	X
Identify liability issues of the different types of stakeholders in case of failures (see section 3.7)	X	X	(X)	(X)		X	(X)	(X)	(X)	X
Define and adopt a long-term strategy for increasing awareness on security issues	X	(X)	X		(X)	(X)	(X)	(X)	(X)	X

Table 4: Economic incentives/asymmetry: Identified activities and stakeholder engagement



	European Institutions	National Authorities	National Security Institution	Sector Regulator	Non-Governmental Organisations	Law Enforcement Agencies	Individual Organisation	Consumer Organisations	Professional Associations	Research Institutions/ Universities
Responsible	2	1	3	0	0	2	1	0	0	4
Supporting	2	3	1	3	1	1	3	2	4	0

Figure 5: Economic incentives/asymmetry: Overview of stakeholder engagement

3.5 Impact assessment of intervention policies: Starting from the evaluation of socio-economic impacts due to security and resilience failures

Policy effectiveness in the NIS context should be evaluated taking full consideration of the potential effects of failures in security and resilience such as those affecting critical infrastructures. Policy effectiveness should be evaluated by competent bodies, depending on the origin of the policy and the purpose for which it was developed e.g. corporate policies, national policies, EU policies. According to the literature investigating impacts of security and resilience failures and also according to the most recent European policy debate, the evaluation of socio-economic damage due to disruptions of critical infrastructures (taking into account their interdependencies and cascading effects) has become one of the main areas of research in this area.

According to the analysis carried out above, the identified activities and stakeholder engagement for this topic are as shown in Table 5.

Identified activities X: responsible (X): supporting	Stakeholders									
	European institutions	National authorities	National security institution	Sector regulator	Law enforcement agencies	Non-governmental organisations	Professional associations	Research institutions/ universities	Individual organisation	Consumer organisations
Definition of methodologies able to make comparable assessment (at macro level) of socio-economic impacts due to security and resilience failures	X	(X)	X	(X)		X	(X)	X	(X)	
Refinement and harmonisation of indicators for assessing socio-economic effects of security and resilience failures (e.g. loss of turnover)	X	X	(X)	X		(X)	(X)	(X)	(X)	
Identification of categories of benefits related to security provisions for all the different types of actors	X	X	(X)	(X)	(X)		(X)		(X)	(X)
Specific methodologies and tools for impact assessment of security and resilience-related policies (including definition data and information to collect and use) (see also sections 3.1 and 3.6).	X	(X)	X	(X)				X		(X)
Ex-post evaluation of effects of current security policies in the medium term also according to the specific sources of threats	X	(X)	X	X	(X)	(X)	(X)	X	(X)	

Table 5: Intervention policies: Identified activities and stakeholder engagement

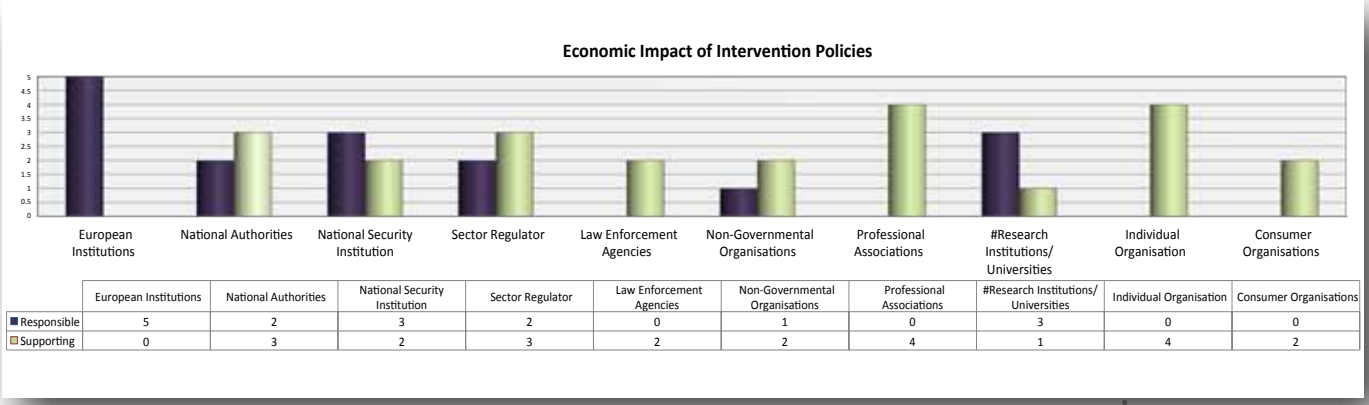


Figure 6: Intervention policies: Overview of stakeholder engagement

3.6 Collection of data on security incidents

Precise quantitative data relating to information security incidents, such as frequency, impact, type, timeline or the effectiveness of countermeasures, would be a valuable source of information for business as well as for academia and information-sharing initiatives. Although already helpful on the level of single incidents, such information can uncover its full potential when available for a multitude of incidents from various organisations and individuals in a standardised way.

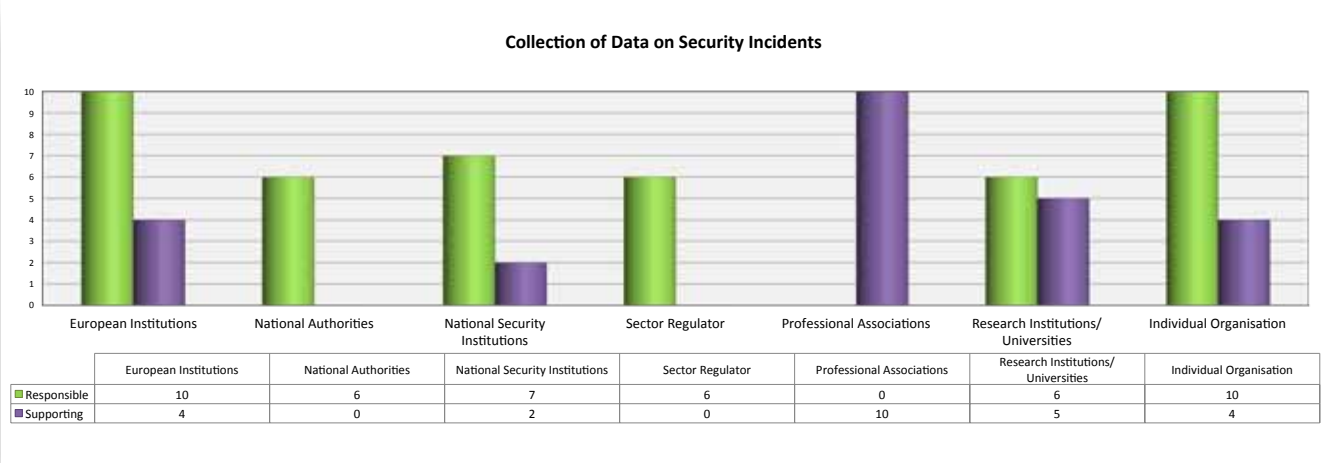
Individual organisations, especially SMEs, need information on security incidents to accurately estimate risks and to make cost–benefit-based decisions from the investment in information security as well as for the ex-post evaluation of security investments and for benchmarking between organisations. Risk management depends on accurate estimations of impact and probability of events. One way to determine impact and probability is to derive them from the frequency and severity of past incidents. Especially for the estimation of important high impact/low frequency risks historical data beyond the own organisation is needed. Approaches like return on security investment (ROSI) are based on the assumption that sufficient data are available to estimate risks and annual loss expectancies correctly. It must be noted, though, that alternative schools of thought exist, supporting the view that past data have not been very useful in predicting future events[1].

The identified activities and stakeholder engagement for this topic are as shown in Table 6.

Identified activities X: responsible (X): supporting	Stakeholders						
	European institutions	National authorities	National security institutions	Sector regulator	Professional associations	Research institutions/ universities	Individual organisation
Establish a common incident taxonomy	X		X		(X)	(X)	(X)
Build a data pool of security incidents and their consequences (e.g. security breaches, impact, etc.)	X	X	(X)	X	(X)	(X)	X
Integrate existing data sources	X		X			X	
Facilitate recording of incident data	X		X				X
Establish benchmarking	(X)	X		X	(X)	(X)	(X)
Develop economic models for cyber insurance						X	X

Table 6: Collection of data: Identified activities and stakeholder engagement

[1] Ian Angell, 'Information Systems Management Opportunities and Risks', http://paul-hadrien.info/backup/LSE/IS%20472/AngellSmithson%20book.pdf



	European Institutions	National Authorities	National Security Institutions	Sector Regulator	Professional Associations	Research Institutions/ Universities	Individual Organisation
Responsible	10	6	7	6	0	6	10
Supporting	4	0	2	0	10	5	4

Figure 7: Collection of data: Overview of stakeholder engagement

3.7 Software liability

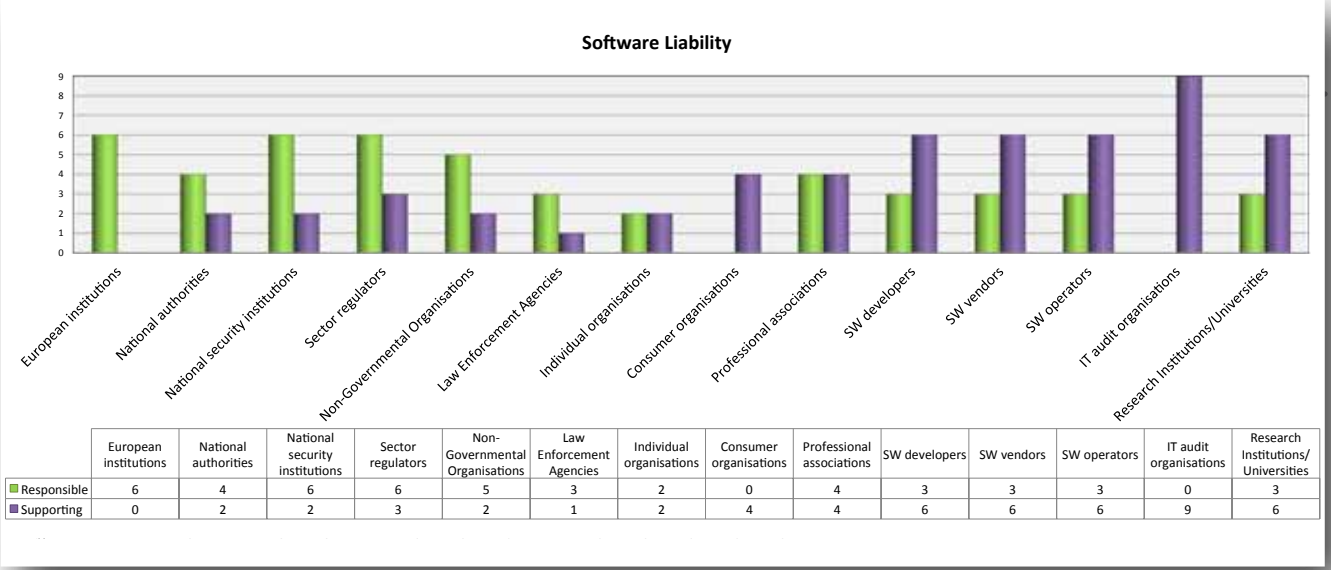
Economic aspects of liability are related to the impact (e.g. damage) experienced by users in the event of a breach or failure which presumably has its origin in the software itself. This argument is further supported by the ongoing discussions on the robustness of software. The question is how software liability, for instance in the case of writing a bug that might open up the vendor to legal action, could affect the computing industry[2]. Compared to other conventional products, for example the motor car, software liability is considered to be an immaterial/intangible good with the relevant limitations. In particular this implies a limited enforceability of national liability regulations, which are based on conventional products. In many economic systems a culture of impunity is manifest for software. A major challenge to assigning liability to vendors is the interdependence of today's IT systems. Given the complexity of these systems, software behaviour cannot readily be predicted. As a result, imperfections of the software cannot be fully foreseen, avoided, or assigned as a reason for malfunction. Additionally, in the case of an incident it is difficult to attribute damages to the software and to quantify actual losses. Therefore the ability to identify and attribute software liabilities could involve considerable effort. Software liability in particular can cause significant obstacles to open and free software distribution. It also raises market entry barriers to innovative competitors. Although software liability is not purely a (IT) security issue, security controls (both technical and organisational) may enhance fault tolerance of software and protect against maliciously caused breaches and drastically reduce the impact of failure. Moreover, security techniques can be used in assessing the risk related to a failure and also in identifying the causes of damage.

After decades of legal uncertainty and lack of ability to impose sanctions, which spurred innovation and productivity growth, society's dependence on its information infrastructure has grown to the point where it is time to rethink the balance between opportunity and responsibility. The identified activities and stakeholder engagement for this topic are as shown in Table 7.

[2] Richard Clayton

Identified activities X: responsible (X): supporting	Stakeholders													
	European institutions	National authorities	National security institutions	Sector regulators	Non-governmental organisations	Law enforcement agencies	Individual organisations	Consumer organisations	Professional associations	SW developers	SW vendors	SW operators	IT audit organisations	Research institutions/universities
Set a policy on EU liability expectations for software, compatible with an incentives regime	X	(X)	(X)	(X)										
Issue an EU software liability programme based on a gradual approach and involving multidisciplinary stakeholder teams	X	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)
Gain common understanding of software liability on national and international level	X	X	X	X	X	X	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)
Harmonise EU software liability legislation in line with international legislation	X	X		X	(X)	X				(X)	(X)	(X)	(X)	(X)
Ensure enforcement by inevitable software liability regulations on international level	X	X	X	(X)		X			(X)	(X)	(X)	(X)	(X)	(X)
Issue holistic incentives for an economically efficient software liability regime	X	X							(X)	(X)	(X)	(X)	(X)	(X)
Model realistic market scenarios related to software liability			X	X	X				X	X	X	X	(X)	X
Balance utility (social wealth) and costs, avoiding externalities in that models			X	X	X				X	(X)	(X)	(X)	(X)	X
Identify liability limiting market scenarios in line with the gradual approach			X	X	X		X	(X)	X	X	X	X	(X)	(X)
Identify most promising bundles of course of action based on thorough in-depth analyses (see also section 3.9).			X	X	X		X	(X)	X	X	X	X	(X)	X

Table 7: Software liability: Identified activities and stakeholder engagement



	European institutions	National authorities	National security institutions	Sector regulators	Non-Governmental Organisations	Law Enforcement Agencies	Individual organisations	Consumer organisations	Professional associations	SW developers	SW vendors	SW operators	IT audit organisations	Research Institutions/ Universities
Responsible	6	4	6	6	5	3	2	0	4	3	3	3	0	3
Supporting	0	2	2	3	2	1	2	4	4	6	6	6	9	6

Figure 8: Software liability: Overview of stakeholder engagement

3.8 Return on security investment (ROSI)

Return on security investment (ROSI) is a concept that links spending on information security controls to the management or mitigation of risk in order to demonstrate a quantifiable financial benefit to the organisation. Techniques to calculate ROSI have been in existence for more than 10 years. In times of increased economic stringency it is self-evidently important for organisations, in the public or private sector, to take account of the cost of ownership and improvement of their assets – including those connected with the management of their information security risk. Furthermore, as organisations have grown more reliant on IT systems connected through the Internet, reactive, tactical and technical approaches to information security are no longer adequate; information is central and is the primary target of attack.

As a consequence it makes sense to adopt a risk-based approach. As part of this it is necessary to involve stakeholders throughout the organisation in understanding and taking forward a more sophisticated cost/risk analysis, such as that provided by ROSI. Despite this, the use of techniques to calculate ROSI has not been extensive in either government or industry within the EU. ROSI techniques are, however, used by both the USA and Australian governments.

From available ROSI approaches and experience with their use, it seems that efficient use of ROSI techniques calls for:

- Identification of relevant security controls.
- Quantification of costs of relevant security controls.
- Determination of business asset value at risk (see also section 3.9).
- Identification of security incidents having the potential to impact business asset value (see also section 3.6).
- Quantification of frequency of security incidents potentially impacting asset value.

- Quantification of potential extent of impact of security incidents on asset value.
- Quantification of effectiveness of identified security controls.
- Calculation of ROSI based on the four quantified values above.

Following the calculation of ROSI, further activities should be undertaken to deliver value to the organisation:

- Identification and prioritisation of improvement areas for security controls.
- Planning for improvements, based on prioritisation.
- Implementation of improvements.

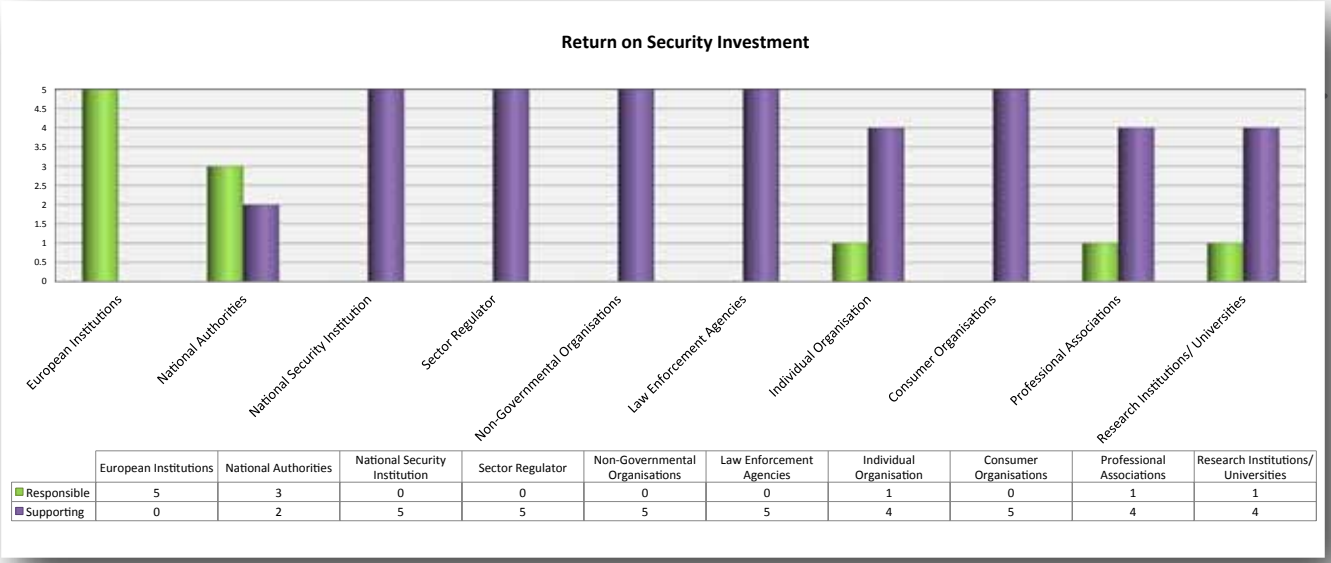
At the level of national government/EU decisions also have to be made regarding:

- ROSI to be just a non-mandatory instrument towards effective management of resources (i.e. Australian approach).
- Information security planning to be part of capital planning and investment control (i.e. US approach for federal government).
- Stakeholders which should be part of the followed ROSI approach.

In order to support the internal market, at the EU level the following activities are suggested:

Identified activities X: responsible (X): supporting	Stakeholders									
	European institutions	National authorities	National security institutions	Sector regulators	Law enforcement agencies	Non-government al organisations	Professional associations	Research institutions	Individual organisations	Consumer organisations
Definition of metrics associated with ROSI	(X)			(X)	(X)	(X)				
Definition of a ROSI standard	(X)			(X)	(X)	(X)				
Adoption of a ROSI standard by government agencies	(X)			(X)	(X)	(X)				
Implementation of ROSI certification for government suppliers				(X)	(X)	(X)				
Wider adoption of ROSI techniques by regulated private enterprise organisations				(X)	(X)	(X)				

Table 8: ROSI: Identified activities and stakeholder engagement



	European Institutions	National Authorities	National Security Institution	Sector Regulator	Non-Governmental Organisations	Law Enforcement Agencies	Individual Organisation	Consumer Organisations	Professional Associations	Research Institutions/ Universities
Responsible	5	3	0	0	0	0	1	0	1	1
Supporting	0	2	5	5	5	5	4	5	4	4

Figure 9: ROSI: Overview of stakeholder engagement

3.9 IT security risk management of business processes

Reliable and secure performance of business processes depends on their implementation by people, procedures, and technical systems such as IT (which are usually built by components). The business impact due to failure in availability or insecure operation as a result of manipulated data or disclosure can be observed in many variations. Hence, the question arises: what are the rules of interdependencies between business processes and implementing components, and how is it possible to control related risks in real life?

Business processes are the linking layer between business activities and the related information and communication technology (ICT) environment. In other words, business processes are dependent on IT systems and their components, such as applications, information, servers or networking devices. Analysing IT and security risks from a business processes perspectives is a generally accepted approach that enables us to link two worlds that currently use different languages: the business world and the ICT world. This link is an important contributor to the economics of security as it makes it possible to provide transparency of risk posture to the business management, to determine their needs and priorities, and to provide support for informed decisions.

Identified activities and stakeholder engagement for this topic are as shown in Table 9.

Identified activities X: responsible (X): supporting	Stakeholders										
	European institutions	National authorities	National security institutions	Sector regulators	Law enforcement agencies	Non-governmental organisations	Professional associations	Research institutions/universities	Individuals organisations	Consumer organisations	IT audit organisations
Identification of Key Business Processes for each sector and industry		(X)	(X)	X			(X)	(X)			(X)
Finding methods to classify the economic value of IT assets			(X)	(X)			(X)	X	(X)		(X)
Identifying business impact areas (or aspects) of IT assets			(X)	(X)			(X)	X	(X)		(X)
Setting parameters to measure the business impact levels			(X)	(X)			(X)	X	(X)		(X)
Selecting methods to assess the security levels of business processes			X	(X)			(X)	X	(X)		(X)

Table 9: Risk management of processes: Identified activities and stakeholder engagement

	European institutions	National authorities	National security institutions	Sector regulators	Non-Governmental Organisations	Law Enforcement Agencies	Individuals organisations	Consumer organisations	Professional associations	IT audit organisations	Research Institutions/ Universities
Responsible	0	0	1	1	0	0	0	0	0	0	4
Supporting	0	1	4	4	0	0	4	0	5	5	1

Figure 10: Risk management of processes: Overview of stakeholder engagement

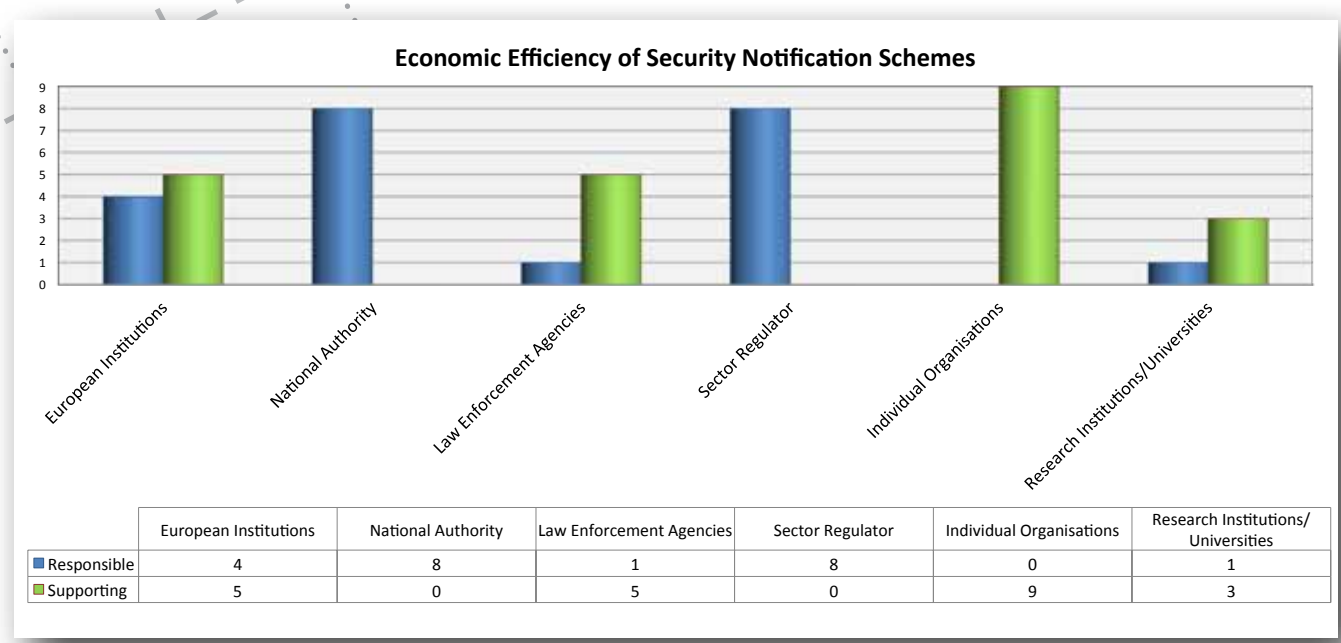
3.10 Information sharing and security notification schemes

When it comes to security notification schemes (SNS), economic efficiency aims to achieve the best possible level of security for the users of the service, while economising as much as possible on the resources employed and establish feedback loops. This balance should be established both at the level of SNS itself and at the level of connected/participating stakeholders. Cost efficiency should be the main concern with regard to interaction with the connected/participating stakeholders.

The activities identified for this topic are shown in Table 10.

Identified activities X: responsible (X): supporting	Stakeholders					
	European institutions	National authority	Law enforcement agencies	Sector regulator	Individual organisations	Research institutions /universities
Focus on support that covers both proactive and protective measures while achieving awareness at the level of participating organisations	(X)			X	(X)	X
Adapt collected and disseminated information to the needs of participating organisations; and help them to help themselves	(X)	X	X	X	(X)	
Use effective means of communication modalities and channels among participating organisations	(X)	X		X	(X)	
Maintain statistics about all kinds of information collected and disseminated, about costs, level of reduction of vulnerabilities among participating organisations, etc.	X	X	(X)	X	(X)	
Establish feedback loops with all types of stakeholders concerned (e.g. participating organisations, regulation authorities, government agencies, law enforcement agencies)	X	X	(X)	(X)	(X)	
Take into account the economic perspective when establishing the SNS	X	X		X	(X)	
Take into account the economic impact and economic return of offered services (for all types of participating organisations)	(X)	X	(X)	X	(X)	(X)
Establish feedback loops with related stakeholders to exchange information on the economic efficiency of the service (e.g. by means of cost oriented KPIs)	(X)	X	(X)	X	(X)	(X)
Assess barriers and benefits provided by SNS on a permanent basis, communicate them at national level and participate in the dialogue for permanent improvement of national preparedness	X	X	(X)	X	(X)	(X)

Table 10: Security notification schemes: Identified activities and stakeholder engagement



	European Institutions	National Authority	Law Enforcement Agencies	Sector Regulator	Individual Organisations	Research Institutions/ Universities
Responsible	4	8	1	8	0	1
Supporting	5	0	5	0	9	3

Figure 11: Security notification schemes: Overview of stakeholder engagement

4. The effect of the top market challenges to economics of security

One of the most interesting aspects of the Economics of Security, if not the most interesting, is the business perspective; in other words, the way that key decision-makers such as CEOs perceive this matter.

No matter what the engineers and the researchers say, at the end of the day it is up to the top management of the business world to go for more or less security.

In the present global financial crisis, where financial and human capital are scarce resources and companies are battling for survival, it is of paramount importance to identify the main drivers of the market, such as upcoming trends, challenges and risks that need to be addressed urgently. As with any investment, security investment will be determined by prevailing market trends and emerging challenges. This will definitely be the view of the majority of CEOs.

By relating these externalities to Economics of Security, we opt for an additional, yet extremely important element that will shed new light on the viewpoint of technological experts by including the perspective of business administrators.

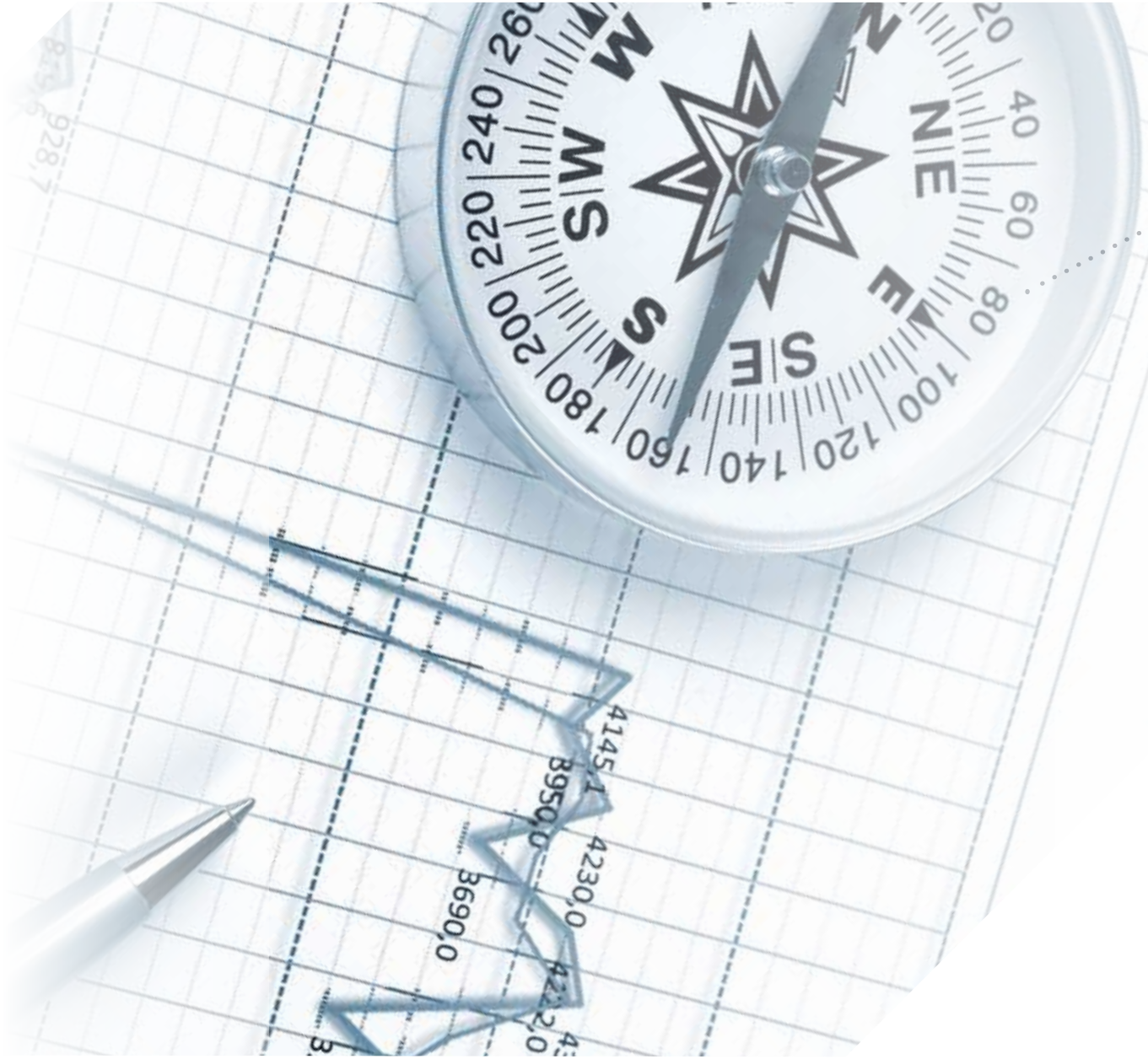
Every year, Ernst & Young carries out a study[3] that charts the global top 10 business risks and opportunities. They gather opinions from leading industry-based and academic commentators across seven global sector groups. The company conducted a survey of companies and governments in 15 countries to rank the risks and opportunities of 2011, with a view to obtaining forecasts on whether these challenges would be more or less important in the years to come. They also aimed to discover how leading organisations in each of the seven sectors surveyed are responding to these challenges.

Although similar studies are also being released continuously by other similarly reputable companies and organisations, at the time of this document was compiled the report cited was deemed to be the one mostly aligned with the researched topics and approach.

According to the findings of the survey, the top 10 business challenges identified are:

- **Regulation and compliance:** Compliance with applicable regulations is seen as the biggest challenge in the business world and particularly in the wider financial sector.
- **Cost cutting:** This is the challenge of controlling costs in order for the business to survive the strong competition.
- **Managing talent:** Many companies face big challenges not only in attracting but also retaining global talent.
- **Pricing pressure:** The global recession and the slow recovery have significantly increased the price pressure on companies and have dramatically reduced their profit margins.

[3] http://www.ey.com/GL/en/Services/Advisory/Turn-risks-and-opportunities-into-results – The-top-10-risks -and-opportunities-for-global-organizations



The effect of the top market challenges to economics of security

- **Emerging technologies:** This challenge mostly relates to the difficulties faced by companies in developing an innovation culture and the inherent uncertainty of using untested technologies.
- **Market risks:** This challenge is mainly related to stock market volatility and speculative financial attacks which have become particularly threatening to some sectors.
- **Expansion of government's role:** This challenge refers to the ever-growing dominance of governments, which is often detrimental to the flexibility of companies.
- **Slow recovery/double-dip recession:** The challenge that the current financial crisis will be succeeded by an escalated fiscal crisis of the national governments which may lead to a double-dip recession.
- **Social acceptance:** There is a new and increasing demand for companies to meet ethical standards created by public pressure.
- **Access to credit:** In the current conditions of financial crisis, access to credit is a vital requirement for many businesses.

If we look at the above challenges in conjunction with the 10 priority topics on Economics of Security identified in this survey, very interesting interrelationships emerge. By interrelationships we mean that a discrete challenge will have a strengthening or weakening effect on a particular topic of Economics of Security. As an example,the need for cost cutting will strengthen the role of return on security investment (ROSI). That is, the management of a business will need to be convinced about the effectiveness and efficiency of security investments undertaken. In this case, the provision of accurate figures about the expected return on investment will be central to decision-making.

The effects of the business challenges to the identified topics are presented in Table 11. Relationships are denoted by the symbols ↑ and ↓. While the symbol ↑ denotes a strengthening trend, symbol ↓ denotes a weakening trend for the relevant topic of Economics of Security in the context of a business challenge.

	Regulation and compliance	Cost cutting	Managing talent	Pricing pressure	Emerging technologies	Market risks	Expansion of government's role	Slow recovery /double-dip recession	Social acceptance	Access to credit
Information sharing and notification schemes		↑		↑	↑		↑	↑	↑	
Economics of resilience	↑	↑		↑		↑	↑	↑	↑	↑
Behavioural economics of security				↑	↑		↑	↓	↑	
Incentives: The role of public goods		↑		↑			↑		↑	↑
Incentives: The role of information asymmetry			↑	↑			↑	↓		
Intervention policies	↑	↑	↓	↑	↓	↑	↑	↑	↑	↑
Collection of data		↓	↑	↓			↑	↓	↓	↑
Software liability	↑	↑		↑	↓		↑	↓	↑	↑
Return on security investment	↑	↑		↑			↑	↑	↑	↑
IT security risk management	↑	↑	↑	↑	↑		↑	↓	↑	↑

Table 11: Effects of business challenges to topics of Economics of Security

Concluding this section, it can be noted that the assessed effects on the identified topics imply a certain priority. Chapter 6 presents these priorities according to various dimensions (see Challenges view in Table 12).

5. Policy impact

The link between the topics identified in this report and the current EU policy context should also be assessed by the stakeholders identified in the respective thematic areas to determine the impact that such interconnections may have.

Economics in the context of information security has to be seen as a crucial contributor to the establishment of effective and efficient policies with the aim of supporting the efforts of the European Union in fighting cybercrime.

An increasing number of documents underline the economic impact of possible ICT failures on a wide spectrum of stakeholders, highlighting the need for consistent, continuous, robust and objective monitoring of the economic factors from an information security perspective. Such an observatory scheme would greatly facilitate the ex-ante process for policymaking and the ex-post process for evaluating the impact of the relevant policy.

It emerges from this analysis that a significant number of policies, as presented below, refer to a number of economic dimensions relating to the benefits of robust information security or the liability of weak information security. However, no specific topics have been identified for further assessment. From the input of the experts from the ENISA working group and the analysis performed by ENISA it was possible to identify the links between most of the Economics of Security topics and the relevant EU policies.

Although it might appear that more topics could be linked to specific policies, it is important for the sake of clarity to illustrate the link with the most prominent topics in each policy area. Therefore, to preserve the consistency and coherence of ENISA's output the policy dimension assessed in this report is in line with the policy context referenced in ENISA's 2012 work programme. A synchronous and forward-looking perspective is being presented in order to provide adequate material for the decision-making process for policy creation.

A. 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' {SEC(2009) 399} {SEC(2009) 400}

- Economics of resilience (see section 3.1)
- Economic incentives for security: The role of public goods (see section 3.2)
- Impact assessment of intervention policies: Starting from the evaluation of socio-economic impacts due to security and resilience failures (see section 3.5)
- Collection of data on security incidents (see section 3.6)
- Return on security investment (ROSI) (see section 3.8)
- Information sharing and security notification schemes (see section 3.10)

B. Commission Communication on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'

- Economics of resilience (see section 3.1)

- Economic incentives for security: The role of public goods (see section 3.3)
- Economic incentives for security: The role of information asymmetry and lack of information (see section 3.4)
- Collection of data on security incidents (see section 3.6)
- information sharing and security notification schemes (see section 3.10)

C. The Electronic Communications Regulatory Framework

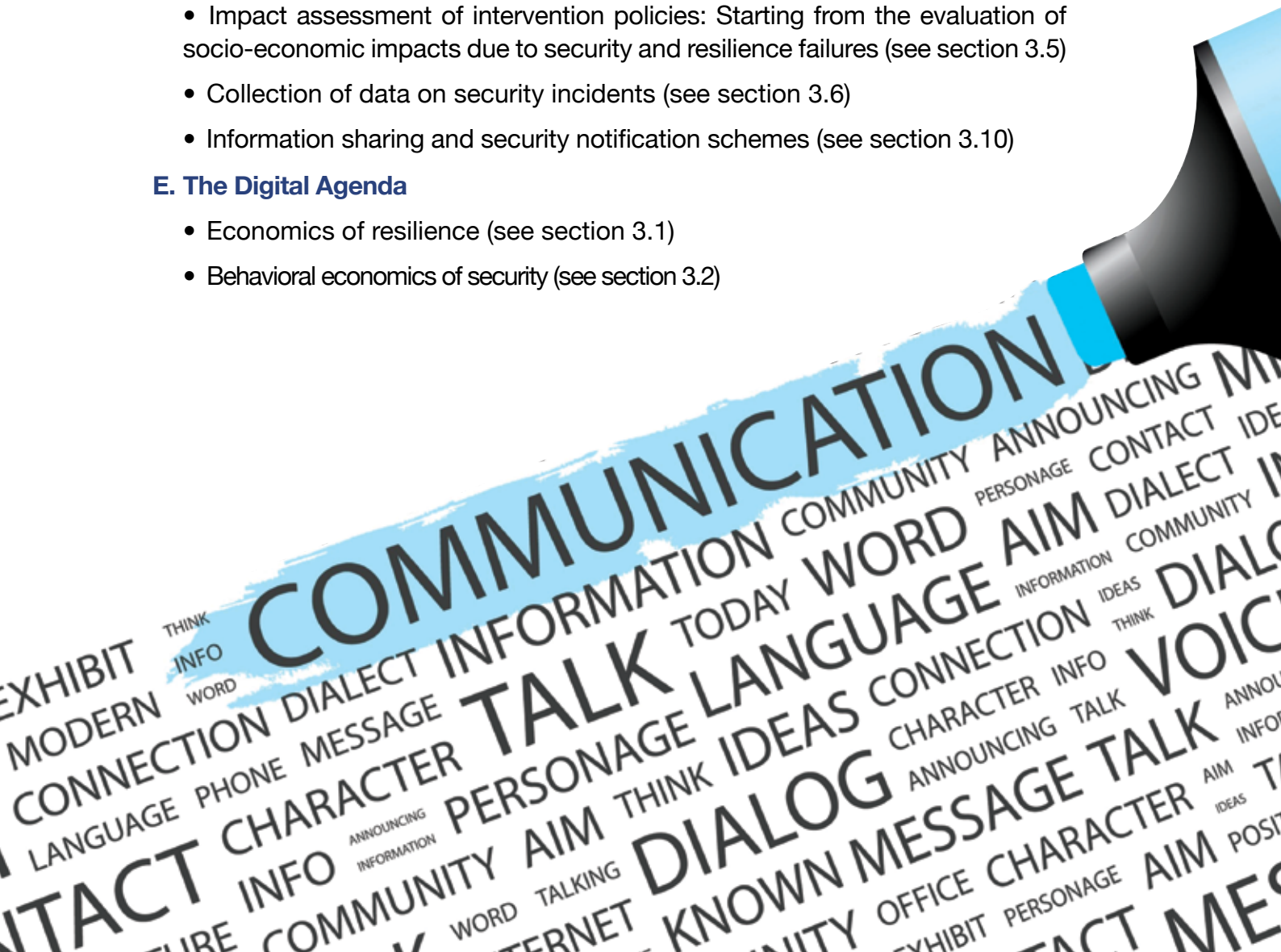
- Economic incentives for security: The role of public goods (see section 3.3)
- Economic incentives for security: the role of information asymmetry and lack of information (see section 3.4)
- Collection of data on security incidents (see section 3.6)
- IT security risk management of business processes (see section 3.9)
- Information sharing and security notification schemes (see section 3.10)

D. The Council Resolution of December 2009

- Behavioral economics of security (see section 3.2)
- Economic incentives for security: The role of public goods (see section 3.3)
- Impact assessment of intervention policies: Starting from the evaluation of socio-economic impacts due to security and resilience failures (see section 3.5)
- Collection of data on security incidents (see section 3.6)
- Information sharing and security notification schemes (see section 3.10)

E. The Digital Agenda

- Economics of resilience (see section 3.1)
- Behavioral economics of security (see section 3.2)



- Economic incentives for security: The role of public goods (see section 3.3)
- Economic incentives for security: The role of information asymmetry and lack of information (see section 3.4)
- Impact assessment of intervention policies: Starting from the evaluation of socio-economic impacts due to security and resilience failures (see section 3.5)
- Collection of data on security incidents (see section 3.6)
- Software liability (see section 3.7)
- IT security risk management of business processes (see section 3.9)
- Return on security investment (ROSI) (see section 3.8)
- Information sharing and security notification schemes (see section 3.10)

F. The Commission proposal on the future of ENISA

- Economics of resilience (see section 3.1)
- Economic incentives for security: The role of public goods (see section 3.3)
- Impact assessment of intervention policies: Starting from the evaluation of socio-economic impacts due to security and resilience failures (see section 3.5)
- Software liability (see section 3.7)
- IT security risk management of business processes (see section 3.9)
- Information sharing and security notification schemes (see section 3.10)

G. The Internal Security Strategy for the European Union

- Economics of resilience (see section 3.1)
- Economic incentives for security: The role of information asymmetry and lack of information (see section 3.4)
- Impact assessment of intervention policies: Starting from the evaluation of socio-economic impacts due to security and resilience failures (see section 3.5)
- Information sharing and security notification schemes (see section 3.10)

H. The Council conclusion on CIIP of May 2011

- Economics of resilience (see section 3.1)
- Software liability (see section 3.7)
- IT security risk management of business processes (see section 3.9)
- Return on security investment (ROSI) (see section 3.8)

I. The Communication on Personal Data Protection in the European Union

- Economic incentives for security: The role of information asymmetry and lack of information (see section 3.4)
- Collection of data on security incidents (see section 3.6)

- IT security risk management of business processes (see section 3.9)
- Information sharing and security notification schemes (see section 3.10)

J. The Single Market Act

- Behavioral economics of security (see section 3.2)
- Economic incentives for security: The role of public goods (see section 3.3)
- Economic incentives for security: The role of information asymmetry and lack of information (see section 3.4)
- Return on security investment (ROSI) (see section 3.8)

The above association of the prominent topics identified with the respective policies prepares the ground for a gradual integration of topics pertaining to the Economics of Security in the policy creation process. Should the above recommendations be embedded in the upcoming policies it is expected that they will generate a balancing effect to the supply and demand chain.

6. Priorities

One significant part of this work is to establish priorities for each of the identified topics of Economics of Security.

To do this, a multilevel approach was followed, so that multiple priority dimensions have been selected. These dimensions cover different viewpoints on the identified topics.

Some perspectives that have already been addressed in previous sections are definitely important for the prioritisation task. Hence, policy impact is an important aspect to consider for the prioritisation (see Chapter 5). Furthermore, business challenges are another dimension that is important for drawing up priorities, as they reflect the views of decision-makers (see Chapter 4). Another important dimension is the level of maturity: depending on the maturity of underlying technologies, methods and good practices, some of the identified topics are easier to develop than others where work on the relevant theoretical framework is still necessary (see Chapter 3).

Another important element in the prioritisation is the interdependencies among the identified topics. The work foreseen in some topics seems to be fundamental when addressing other topics of Economics of Security.

Finally, considering research as the engine of sustainable development, we have introduced a further dimension related to the necessity of mobilisation of research capabilities for the identified topics.

We thus end up with five different dimensions for the generation of priorities. These are:

- Priorities according to policy impact/relevance
- Priorities derived from business challenges
- Priorities according to the level of maturity of underlying concepts and methods
- Priorities according to cross-topic dependencies
- Research priorities

Table 12 depicts the identified priorities for the topics of Economics of Security according to these five dimensions. For the assigned priority values a range from 1 (high) to 5 (low) is used, depending on the importance of the topic under the context of each particular dimension. Different colouring is also used to visualise the prioritisation level.

	Policy Impact	Business Challenge	Level of Maturity	Cross-topicde-pendencies	Research
Information sharing and notification schemes	2	2	2	3	2
Economics of resilience	1	1	2	2	3
Behavioural economics of Security	4	5	4	3	1
Incentives: The role of public goods	2	4	3	2	2
Incentives: The role of information asymmetry	2	4	3	4	2
Intervention policies	3	2	5	4	1
Collection of data	2	2	1	1	5
Software liability	4	2	4	2	4
Return on security investment	4	1	1	1	4
IT security risk management	3	3	1	2	5

Table 12: Assessed priorities for the topics of Economics of Security

This multidimensional prioritisation approach allows for various perspectives to be taken into account and can support the derivation of priorities according to the weight an observer assigns to each of the aforementioned dimensions. It is worth noting that the priorities assessed above also reveal expected differences pertinent to the various perspectives.

Thus, using the table, varying conclusions regarding the priority of topics of Economics of Security can be derived.

7. Approach and results of stock taking

7.1 Approach

ENISA initiated this work by means of a public consultation in order to assess the most important topics on Economics of Security according to the IT community. For this purpose, experts in this area were contacted and their views on open issues in the area of Economics of Security assessed. After identifying the relevant expert community, ENISA invited over 90 experts to participate in the open stock taking exercise using an online tool. The objective was to:

- Collect information on available material in the area of Economics of Security
- Collect information on ongoing work in this area
- Deliver expert views on priorities, points of action and open issues for various kinds of stakeholders (e.g. Member States, industry, public administration, European bodies, etc.)
- Prioritise the issues that emerged from the above actitivies

After having collected and consolidated this information, ENISA generated a list reflecting priority topics and sectors. This material served as input for a working Group of Experts that has accompanied ENISA's work. The members of this Expert Group have been identified according to the assessed topics and priorities. The top 10 priorities have been compiled / consolidated from the received input and they are presented in the present report.

Besides the identified priorities, various open issues on Economics of Security were mentioned during the stock taking phase. It is important to mention this information here, as it demonstrates the depth achieved in the identification of the top 10 topics. Furthermore, although it is presented in the expert contributions, some of this information is worth reproducing here in order to avoid the risk of information loss through the consolidation steps performed as part of the synthesis of this work.

The stock taking input received is presented below. Naturally the collected information was not totally free of overlaps as many contributors have similar views on the existing priorities. In this document we present a summary of the identified priorities, after having eliminated eventual overlapping. However, in a separate document (see Analytical results of stock taking by the working group) we retained the degree of detail available as we think that it best demonstrates the views of the various stakeholder communities participating in the stock taking.

Moreover, the working group supported ENISA by providing suitable tools for optimisation of the decision-making process, as well as for making better use of the available knowledge for future ENISA work.

7.2 Results of stock taking by stakeholder group

The results of the stock taking exercise have been grouped by type of stakeholder, as each stakeholder group had different views and interests.

7.2.1 Industry

- An EU reference Security Ontology and data base for security planners and decision-makers.

- Methods for quantifying parameters of relevance for security measures and investments.
- A community/ network of security decision-makers.
- How to identify and measure the economic role of IT asset within the organisation.
- What should be the categories to identify the impact of the IT asset (for example: financial, brand, legal, productivity, safety).
- What are the parameters to measure the values in each area?
- How to find common language to communicate these aspects with business management.
- Building a data pool with quantitative data on information security incidents from organisations for the privacy preserving pan-European exchange and analysis of impact data.
- Benchmarking economic metrics on information security between organisations using multiparty computations.
- Development of common taxonomy for security incidents, it-assets (and their value), security measures and risk measures.
- The cost of regulatory failure.
- Spending on information security management.
- Cost-effectiveness of threat management.

7.2.2 Academia

- A serious effort for data collection on security incidences and breaches. Comprehensive and reliable data would be an excellent tool for both public policy and effective risk management.
- Behavioural economic modelling of security attack targets.
- Behavioural economics, remote risks and insurance.
- Botnet clean-up.
- Building trust in public–private partnerships.
- Countering cybercrime.
- Development of overall risk analysis method for organisations, based on business processes.
- Development of security measurement constructs.
- Economic effects and repercussions of lack of security.
- Economic impact of intervention policies.
- Economic modelling of online crime actors.
- Economic modelling and integration of field data.
- Experimental economics of security (human subjects experiments).
- Multivariate decision-making problems (e.g. mitigation and prevention).
- Economics of resilience.
- Effectiveness and efficiency of security measures.
- Aligning incentives for security of mobile devices and services (incl. mobile wallets).
- Applying soft paternalistic solutions (or 'nudges'), based on behavioural economics, to assist and improve security and privacy decision-making.
- Behavioural Economics approaches to understanding security and privacy decision-making.
- Cyber-insurance.
- Designing reliable market signals for security of information services.
- Efficiency of Security Investment (Security Productivity).
- Liability.
- Strengthening the incentives of ISPs to protect customers and mitigate infected machines.
- Improving the quality/security of Software.
- Micro-level empirical analysis of insecurity and terrorism and their actors.
- Resilient Enterprise: A framework for managing information security and surviving information security incidences at firm level.

- Software liability.
- Return on Information Security Investment (ROISI).

7.2.3 Other stakeholders (consumer organisations, associations, etc.)

- Adopt known standards and practices of areas closely related to security (like industrial safety, product and process quality or environmental protection).
- Incentives to secure CIs (from operators' and stakeholders' perspective) and the particular role of information sharing.
- Integration of economic models of systems security with mathematical models of systems architecture and performance.
- Investment in security and resilience
- Socio-economic impact due to failures of CIs and related domino effects.
- Specify a quality metric of effective security (as a basis for security auditing and e.g. SLAs).
- The concept of 'trust domain' from the perspective of information flow and its associated security issues (trade-offs, costs, etc.).
- The concept of information (information considered as a resource) stewardship in complex information ecosystems.
- Utilise organisational transparency (as a framework for balancing business profit / outcome and integrated security).

8. Stakeholders definition

European Institutions: European Council, European Parliament, European Commission, Council of the European Union, Court of Justice, Court of Auditors.

National authorities: National government and relevant organisations (i.e. parliament, ministries, etc.).

National security institution: Institutions concerned with the protection of the national (critical) information infrastructure (e.g. German BSI, UK CPNI, French ANSSI, etc.).

Sector regulator: A public authority or government agency responsible for exercising autonomous authority over some area of human activity in a regulatory or supervisory capacity (Wikipedia).

Law enforcement agencies: Law enforcement agency (LEA) is a government agency responsible for the enforcement of the laws (definition used mainly in US) (Wikipedia).

Non-governmental organisation (NGO): A legally constituted organisation created by natural or legal persons that operate independently from any government (Wikipedia) (e.g. European Agencies, international organisations such as UN, OECD, etc.).

Professional associations: (Also called a professional body, professional organisation, or professional society); usually a non-profit organisation seeking to further a particular profession, the interests of individuals engaged in that profession, and the public interest (Wikipedia).

Research institutions/universities

Individual organisation: Privately or publicly owned organisations of any size. This includes companies (service providers, vendors and SMEs) but also independent public organisations that are not part of national government (e.g. public services, public institutes, etc.).

Consumer organisations: Are advocacy groups that seek to protect people from corporate abuse like unsafe products, predatory lending, false advertising, astro turfing and pollution (Wikipedia).

European Network and Information Security Agency

Economics of Security : Facing the Challenges

Luxembourg: Publications Office of the European Union, 2012

ISBN: 978-92-9204-057-4

doi: 10.2824/23063

Catalogue Number: TP-32-12-064-EN-N

TP-32-12-064-EN-N

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu

doi: 10.2824/23063

Catalogue Number: TP-32-12-064-EN-N

ISBN 978-92-9204-057-4