Economics of Security: Facing the Challenges

Analytical Results of Stock Taking

19-12-2011

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 Economics of Security, please use the following details:

Louis Marinos, Senior Expert Risk Analysis & Management,
E-mail: louis.marinos@enisa.europa.eu

Aristidis Psarras, Awareness Raising Officer
E-mail: aristidis.psarras@enisa.europa.eu

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

Introduction

ENISA has initiated this work on Economics of Security by means of a public consultation in order to assess the most important topics in the field from the relevant community. For this purpose, experts in this area have been contacted and their views on open issues in the area of Economics of Security have been assessed. Subsequently, ENISA invited over 90 experts to participate to the open stock taking exercise over an online tool. The objective was to:

- Collect information on available material in the area of Economics of Security
- Collect information on on-going work in this area
- Deliver expert views in priorities, points of action and open issues for various kinds of stakeholders (e.g. Member States, Industry, Public Administration, European bodies, etc.).
- Prioritize the emerged issues

After having collected and consolidated this information, ENISA generated a list reflecting priority topics and sectors. This material served as input for an Expert Group that has accompanied ENISA's work.

This part of the work demonstrates the depth achieved in the identification of the top 10 topics that were further analysed in the report. Furthermore, with this document we would like to avoid the risk of information loss through the performed consolidation steps that were necessary within the synthetic part of preparing the main report. Hence, the complete input received by the experts as the stock taking exercise is presented below.

Analytical Results of Stock Taking by Stakeholder Group

Stakeholder's Group	Topics proposed	Justification for the proposed projects	References
Academia	Economics of resilience Behavioural economics, remote risks and insurance Building trust in public-private partnerships	Need to shift from an age of efficiency to an age of resilience Understanding the causes of the underdevelopment of insurance markets for critical infrastructure protection Need to foster efficient PPPs for resilience	http://www.ceps.eu/ceps/download/4061
Academia	Botnet clean-up Software liability Countering cybercrime	We have some competence at detecting botnets, but we have so far failed to come up with compelling arrangements for getting them cleaned up. The problem is economic rather than technical and so the correct mixture of incentives and regulation has to be identified We need to get a better understanding of how software liability (writing a bug gets you sued -- or, your insurance policy pays out) will affect the computing industry. Will it actually improve security? We need to find some way to counter cybercrime marrying the	http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/LessonsLearned http://www.enisa.europa.eu/act/sr/reports/econ-sec http://www.cl.cam.ac.uk/~rnc1/malware.pdf

		resources to hand that are either private actors, with limited powers, or public authorities with limited jurisdictions.	
Academia	Economic modelling of online crime actors Economic impact of intervention policies Behavioural economic modelling of security attack targets	Better understanding how online crime works will allow stakeholders to identify which policies are most likely to be effective in curbing the phenomena. Evaluating the impact of intervention policies is absolutely crucial to implement security policies that are viable, and that ultimately help victims. Users are vulnerable to a number of attacks that prey on human, rather than technical weaknesses. For instance, most social engineering scams prey on human flaws such as greed. A better formalization of our understanding of these flaws will help devising more efficient defence mechanisms.	http://www.andrew.cmu.edu/user/nicolasc/publications/CEVG-FC11.pdf http://www.andrew.cmu.edu/user/nicolasc/publications/CYK-CCS10.pdf http://www.andrew.cmu.edu/user/nicolasc/publications/MEC-NSPW10.pdf
Academia	Micro-level empirical analysis of insecurity and terrorism and their actors Economic effects and repercussions of insecurity	Most available empirical literature focuses largely on the macro-economic level, examining actual impacts at the expense of understanding the underlying processes that lead to these impacts. There is insufficient information on the structure and functioning of agents of insecurity and what factors create a conducive environment for their actions. We need to know more about how economic agents (individuals, the private sector and governments) respond to human-induced insecurity. Even though it has been shown that insecurity significantly	http://www.economics-of-security.eu/publications Llusa, F. and J. Tavares (2011) Economics of Terrorism: A (Simple) Taxonomy of the Literature. Defence and Peace Economics, Vol. 22, no.2.

	Effectiveness and efficiency of security measures	effects economic behaviour, there is little understanding on the underlying drivers of these changes. At macro-economic level, research focuses on the negative impacts caused by perpetrators at the relative expense to calculate impacts derived from responses to terrorism. More light should be shed on the negative economic repercussions and potential opportunities of security measures employed to thwart terrorism and organised crime.	Brück, T., Schneider F. and D. Meierrieks (2010) The Economics of Terrorism and Counter-Terrorism: A Survey. DIW Discussion Paper 1049 and 1050
Academia	A serious effort for data collection on security incidences and breaches. A good and reliable data would be an excellent tool for both public policy and doing effective risk management. Resilient Enterprise: A framework for managing information security and surviving information security incidences at firm level.	Information security decision making is heavily driven by uncertainties. The risks are unknown and unclear and the decisions are made on ad-hoc anecdotal basis. A serious effort to collect reliable data and analysis would be an extremely helpful to (i) assess the state of information (in) security, (ii) risk management. With long term consistent data, one can evaluate which policies work, which industries are more susceptible and the overall pattern of cyber-attacks. Such data would benefit not only the policy makers but also the individual firms to make appropriate risk management decisions. How to manage information security risks is a critical challenge for an organization. Even though risk management is a widely studied topic, enterprise resiliency in the face of serious cyber-attacks is an important priority. Based on different industry segments, we need a good framework for enterprise risk management which helps firms not only quantify the value of their efforts in managing security risks but also explore and learn from industry practices. It will also help policy makers uncover why firms do not do the right thing and create	Ashish Arora, Jonathan Caulkins, Rahul Telang (2006), "Sell First, Fix Later: Impact of Patching on Software Quality", Management Science (Research Note), 52(3), 465-471. Nancy Mead (2003) "International Liability Issues for Software Quality", CERT technical report J Reese, S Bandhopadhyay, E Spafford (2003), "PFIRES: a policy

	Improving the quality/security of Software.	appropriate incentives in improving security at enterprise level. Many security incidences are a direct result of software vulnerabilities. How to improve security of software has been a long debated challenge. Software pose an interesting dilemma because even after the product is shipped, software vendors can take steps to patch these vulnerabilities in a timely fashion and improve the overall security. Disclosure of these vulnerabilities is an interesting problem in itself. As software becomes more and more integrated in our daily lives, software security will emerge as an important public policy issues. There is an opportunity to explore different policy levers including competition from open source, certification and labelling, disclosures and even imposing fines and liability.	framework for information security" Communications of the ACM A. Arora, R Krishnan, R Telang, Y Yang (2010) "An Empirical Analysis of Software Vendors' Patch Release Behaviour: Impact of Vulnerability Disclosure", Information Systems Research (ISR), 21(1), 115-132, http://www.cyber.st.dhs.gov/docs/RAND_RB9365-1.pdf.
Academia	Development of overall risk analysis method for organisations, based on business processes Development of security measurement	Risk analysis is an important basis for all subsequent calculations and measurements, e.g. ROSI; but most of the existing methods start on the basis of IT systems and/or applications; it would be helpful to have more methods and tools basing on the assessment of risks for business process, resp. to develop methods how to aggregate risks from IT systems to business projects Most of the well-known standards and guidelines in this field, like	

	constructs ROISI	ISO/IEC 27004, NIST 800-55 or CobiT, provide good guidance on how to develop measurements, but give only some examples of real ones. It would be helpful to develop comprehensive sets of measurement constructs for different scenarios and types of organisations Based on 1. and 2. concrete ROISI calculation could be developed and proposed	
Other stakeholders (e.g. consumer organisations, associations etc.)	Socio-economic impact due to failures of CIs and related domino effects Incentives to secure CIs (from operators' and stakeholders' perspective) and the particular role of information sharing Investment in security and resilience	Capability to assess socio-economic impact at macro level of CII failures may help operators and stakeholders (including policy makers) to set up prevention measures in order to minimize consequences. In particular, the pervasiveness of CIIs in the socio-economic context (from citizens' and productive point of view) may generate large-scale effects. In line with the guidelines of the Directive on ECI on energy and transport sectors, also the assessment of potential impacts due to CIIs failures and related cascading effects have to be investigated. Three main instruments can be adopted by policy makers to increase security on CI: impose through regulation some measures, directly finance some security improvements and create a framework that spurs CI operators' and stakeholders' "spontaneous" investment behaviours. In the last case, public authorities and governments may set up virtuosos tools able to stimulate investments of security. Different Information sharing mechanisms should be investigated to this purpose.	Bisogni F., Cavallini S., (2010), "Breakdown effects caused by information systems: economic losses and social damages", Eric Goetz and Sujeet Shenoi, "Critical Infrastructure Protection IV", Edited by Springer (paper attached) Bisogni F., Cavallini S., Di Trocchio S., (2011), "Cyber-security at European level: The Role of Information Availability", dossier "The Economics of

		Investment in security and resilience is structurally sub-optimal for 2 reasons: first of all CI operators and networked stakeholders CIs invest in security and resilience according to the expected damage they would directly suffer in case of failures; they do not internalise the social cost and are affected by the weakest link problem. The second reason is related to the lack of information on causes of failures especially in case of cyber-attacks; not adequate information leads operators and stakeholders to underestimation of risk and to a consequent underinvestment also respect to their desired levels. Analysis of methods to increase information of cyber-risk available to CI operators and stakeholders may support policy makers in reducing social effects of failures of CIs.	Cyber-security", No. 81, edited by Communications & Strategies (paper attached)
Industry	The cost of regulatory failure. Spending on information security management. Cost-effectiveness of threat management.	With the increasing demands and complexity of legal and regulatory frameworks, especially for organizations working across international boundaries, it is becoming more essential for management to understand the cost implications of regulatory failure. This is not simply from the point-of-view of the fines and impositions that result directly from the failure; but in terms of costs of recovery, notification of affected parties, legal fees, payment for auditors and, especially, potential loss of market value. In most organizations, responsibility for information security is split between a number of different departments and groups. For example, in addition to the information security group itself, these may include: IT infrastructure (e.g. cost of installing and maintaining firewalls, switches etc.); HR (e.g. recruitment vetting, training and awareness	For regulatory failure a paper by the University of Texas School of Management in 2002 estimated that "Breached firms, on average, lose approximately 2.1% of their market values within two days surrounding the events."The Effect of Internet Security Breach Announcements on Market Value of

		etc.); estate management (e.g. physical barriers and entry controls, CCTV cameras and security guards etc.); audit and compliance and; risk management. Because of this split responsibility, spending on information security is not transparent and readily accountable. As a result it is difficult both to understand and manage the effectiveness of this spending and to see where new spending should best be targeted. Threats are the element of the risk equation which are both the least understood and most difficult to control. Yet, most organizations seem mesmerized by the changing threat scene and focus much of their attention on combatting threats. So far as I am aware, no comparative study has been conducted on the relative cost effectiveness of spending on threat detection and prevention versus spending on vulnerability management or incident management. Such a study would prove particularly useful for small to medium-sized businesses with limited resources, who need to know where best to target these.	Breached Firms and Internet Security Developers Huseyin Cavusoglu, Birendra Mishra, Srinivasan Raghunathan huseyin@utdallas.edu, bmishra@utdallas.edu, raghu@utdallas.edu. Surveys have been published on the cost of fines. But, so far as I am aware, no study has looked at the whole cost of regulatory failure. Spending on information security is the subject of many studies (e.g. the annual CSI/FBI survey, the UK bi-annual information security breaches survey (UK DTI - now BIS, CSO magazine: http://www.csoonline.com/read/090104/survey.html). However, none

			of these studies has taken into account the full cost across of the departmental groups to which I refer.
Academia	Experimental economics of security (human subjects experiments) Economic Modelling and integration of field data Multivariate decision-making problems (e.g., mitigation and prevention)	Real-life decisions inherently more complex than simple models Combination of lab-generated and field data with models enhances validity	http://people.ischool.berkeley.edu/~jensg/research/index.html
Industry	Building a data pool with quantitative data on information security incidents from organizations for the privacy preserving	Historical data is one of the key most important elements for the estimation of risks. This is also true for information security risks. Yet in practice organizations are lacking reliable data. Furthermore especially for the important high impact/low frequency risks historical data from the own organization is not sufficient. Like in	Thomas Nowey: Konzeption eines Systems zur überbetrieblichen Sammlung und Nutzung von quantitativen Daten

	pan-european exchange and analysis of impact data. Benchmarking economic metrics on information security between organizations using multi-party computations. Development of common taxonomy for security incidents, it-assets (and their value), security measures and risk measures.	other domains (banking, insurance) a pan-European data pool with quantitative data on information security incidents from commercial and non-profit organizations (like European institutions) will be a valuable source for better risk management decisions and thus for increased profitability competitive advantage. Such a data pool or platform using a common language for security incidents is not available today. Since the information on incidents can be highly critical it is necessary to develop a system that preserves the privacy of the contributors while still giving enough information for the users. As described in my below-mentioned PhD thesis (Nowey 2011) some key issues have to be addressed to make such a platform possible: - Anonymity - Security - A common taxonomy/language - Mechanisms for fair use - A demand-oriented data preparation Nowey 2011 also develops some basic concepts on how those issues can be resolved. Yet a practical implementation of such a platform is still not existent. Like Social Networks and Wikis are a means to use the wisdom of the crowd (as described by Don Tapscott) such a platform might leverage	über Informationssicherheitsvorfälle. Vieweg+Teubner, 2010. http://www.viewegteubner.de/Buch/978-3-8348-1423-4/Konzeption-eines-Systems-zur-ueberbetrieblichen-Sammlung-und-Nutzung-von-quantitativen-Daten-ueber-Informationssicherheitsvorfaelle.html Economic Security Metrics. http://www1.inf.tu-dresden.de/~rb21/publications/BN2008_Economic_Security_Metrics.pdf Collection of Quantitative Data on Security Incidents. http://www-sec.uni-regensburg.de/publ/200

		this development to the level of cooperation between organizations. Microeconomic models remain virtually useless for organizations if they cannot be used to make better risk management decisions. Gathering of real-world quantitative data is a key to make economic models verifiable and useful for companies and non-profit organizations Such a data pool can not only be used by companies or institutions but on a higher level in can be utilized by academia to verify models and hypotheses on the economics of information security. The practical use of economic models requires doing calculations using the data from different organizations. One important activity in economic analysis in organizations is benchmarking. Benchmarking becomes non-trivial, though, when competitors are mutually distrustful or unwilling to hand over their KPI values to a Trusted Third Party. In theory it has been shown that the application of secure multi-party computation (SMC) protocols can be a solution. Yet there is no pan-European platform to really such calculations in the field of information security indicators. Such a platform could also be used for specific communities like the benchmarking between European institutions, associations, etc.	7/NoFe2007ARESQuantitativeData.pdf A Privacy-Preserving Platform for User-Centric Quantitative Benchmarking. http://www.springerlink.com/content/41h381k7487w7472/fulltext.pdf

		Microeconomic models remain virtually useless for organizations if they cannot be made utilizable for better management decisions. Microeconomic papers on information security often use terms like security investment, cost for information security, annual loss expectancy, cost of a security measure, impact, damage categories, loss, insurance premium, asset value, probability of an event, threat, vulnerability, exploitability, etc. However in practice there is no common understanding of how to define, calculate or measure those terms. Furthermore not only metrics and indicators have to be defined, but there is also a need for a common language to describe it-assets (and their value), information security incidents and their consequences and security measures. Without that it is virtually impossible to do comparisons between organizations (e.g. benchmarking).	
Other stakeholder **Test and evaluation laboratory**	Utilise organisational transparency (as a framework for balancing business profit / outcome and integrated security) Specify a quality metric of effective security (as a basis for	Transparency is a pre-requisite for economic approach due to the comprehensive character of security, which is interwoven with all areas of life and business. Otherwise, a lack of necessary input for management decisions and control is the risk. To an end, organisational compliance is not given and dynamic business development impossible. (see also the attached short presentation - to keep the upload file small, pictures or diagrams were skipped from the presentation) Quality metrics are the rulers for measuring, if security is in place and	

	security auditing and e.g. SLAs) Adopt known standards and practices of areas closely related to security (like industrial safety, product and process quality or environmental protection)	maintained. Such criteria can be used as e.g. Security SLAs to improve G2B, B2B and B/B2C relationships regarding security and data privacy. On long-term, a resilient Security SLA to investment relation can be derived as a best practice "experience". (see also the attached short presentation) Learn from FMEA, (tool based) process optimisation or e.g. EFQM Excellence model as potential resources to enrich the programme. Potential outcomes are derived "simple" sets of security measures, applicable in typical business and life scenarios, to meet the TOP 2 Security SLAs. Or developed public security training courses (e.g. web-based "How to Surf Safe") which could cover educational needs of school, university, business or life. (see also the attached short presentation)	
Academia	Behavioral Economics approaches to understanding security and privacy decision making. Applying soft paternalistic solutions (or "nudges"), based on behavioural economics, to assist and improve security	Understanding security decision making purely in terms of costs and benefits can be misleading, as it ignores how those costs and benefits are actually perceived, and acted upon, by economic agents. Soft paternalistic approaches hold great promise as they rely on first understanding, and then anticipating, possible cognitive and behavioural biases that may adversely affect individuals' security decision making.	http://www.computer.org/portal/web/computingnow/1209/whatsnew/securityandprivacy

	and privacy decision making.		
Academia	Liability Efficiency of Security Investment (Security Productivity) Cyber-insurance	Network security is a public good. Without liability, the resulting externalities cannot be internalized. Short-sighted compliance regulation leads to over-spending in ineffective protection technology. No further security spending should be mandated without efficiency measuring their efficiency. Risk transfer is an essential building block of risk management. Without a mature market for cyber-insurance, proper cyber-risk management remains a distant goal.	http://www.wi.uni-muenster.de/security/research/publications/Boehme2010_InsurableNetworkArchitectures.pdf http://www.wi.uni-muenster.de/security/research/publications/BS2010_Modeling_Cyber-Insurance_WEIS.pdf http://www.wi.uni-muenster.de/security/research/publications/Boehme2010_SecurityInvestment-IWSEC.pdf
Academia	Strengthening the incentives of ISPs to protect customers and mitigate infected machines	Botnets are a critical current threat and while the ecosystem is moving in new directions, i.e., cloud based services, the machines of end users will remain a critical resource for criminal and other malicious purposes.	http://www.oecd-ilibrary.org/docserver/download/fulltext/5km4k7m9n3vj.pdf?expires=1301522108&id=0000&accname=guest&checksum

	Aligning incentives for security of mobile devices and services (incl. mobile wallets) Designing reliable market signals for security of information services	For years, security researchers have predicted that mobile devices will be the next big target. That phase has now begun. Smart phones and tablets are capturing an increasingly dominant share of the market and more and more malware is being discovered. The value of services running on mobile devices will increase tremendously, making them a critical target for attackers. For new models like mobile wallets to enable economic growth, the incentives have to be aligned early on for security and consumer protection to be ensured. Currently, they are not. Even when business or home users care about the security of their information services, they typically have no reliable market signals telling them which providers perform better in terms of security. This holds for access providers, SAAS providers, software vendors, hosting providers etc. Better signals, like reputation mechanisms, would move the existing incentive structure for security closer to the social optimum.	=18206638972A3D9FD204D4152B6D72B1 http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation.html http://spw.stca.herts.ac.uk/2.pdf
Industry	How to identify and measure the economic role of IT asset within the organization. What should be the categories to identify the impact of the IT asset (for example:	Included in The CIIP Taskforce of CEPS (Center for European Policy Studies)	http://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf

	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		
Other stakeholders **Academia and Industry**	Integration of economic models of systems security with mathematical models of systems architecture and performance. The concept of information (information considered as a	This is a key first step for the next two points. Sophisticated economics-based analyses of security architectures must be based (at suitably chosen levels of abstraction) on the design of the underlying system (otherwise, the economic models may simply diverge from reality as the systems executes). There is also challenging (and deep) mathematical work in economics to be done here, of intellectual value in its own right. As information ecosystems become increasingly integrated and complex, with high levels of interdependence, and as their associated service offerings become increasingly complex, existing concepts of information assurance, whilst still essential, will be only part of the	www.abdn.ac.uk/~csc335 (more reference in the e-mail of sent my Mr. Pym)

	resource) stewardship in complex information ecosystems. The concept of `trust domain' from the perspective of information flow and its associated security issues (trade-offs, costs, etc).	story. What will be required is an understanding of the concept of information stewardship, capturing not only basic security requirements, but also management requirements such as the need to add/preserve value, the need to respect moral values and reputations, and the need to plan for future generations. A major challenge is to connect together work on trusted infrastructure (starting at the hardware layer) and information assurance (at the service layer). This will involve understanding not only how security architectures relate to one another at different layers, but also how the trade-offs and incentives associated with their design and use are related at the different layers. Such an account of security and its economic context will be applicable way beyond information systems, including into physical security, and may have applications in critical national/international infrastructure and transport.	
Industry	An EU reference Security Ontology and data base for security planners and decision makers Metods for quantifyind parameters of relevance for security	Harmonizing security decisions across Europe Base security decisions on a more transparent and rational foundation Exchange information on security related decision processes, rationalization and information base	VLUESEC: An FP7 project of relevance.

	measures and investments A community/ network of security decision makers		

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu