Economics of Security: Facing the Challenges

The Working Group Contributions

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

Contents

The Working Group Contributions

ENISA organised a working group with a view to identify, analyse and present the most prominent topics on Economics of Security. The main output of this work is the report "Economics of Security: Facing the Challenges" that can be found on the ENISA website www.enisa.europa.eu.

The contributions of the working group though are of particular value because they analyse in-depth the topics that have been presented in the aforementioned concise report. Therefore they are presented in this document in their original form, that is, they have not undergone any editorial changes from the ENISA team. Apart from detailed information on each topic, the contributions contain detailed bibliographic references to relevant work.

1 Economics of Resilience

By Professor David J. PYM, PhD, ScD, FIMA, FBCS, University of Aberdeen, Scotland and Ralf SCHNEIDER, TÜV Informationstechnik GmbH, Essen, Germany

1.1 Executive Summary

We take the resilience of a system to be that ability of a system, in the aftermath of a shock, to restore itself to a status that is within an acceptable range of its usual operating condition.

In economics, this is a satisficing condition, or constraint, upon the dynamics of the system's utility (from the perspective of an appropriate stakeholder). It is intimately related to the notion of sustainability, resilience being a short-cycle property and sustainability a long-cycle property.

Resilience is a vital aspect for the internal market of the EU, especially regarding the high dependency on information technology (IT). Setting an EU policy frame and homogeneous legislation with due enforceability for a resilient IT will support future wealth even in case of serious distortions and hazards. In any case, decisions should be compatible with an incentives regime. But what are realistic options, what are their consequences, and which are best supportive to stakeholders' utilities? This drafted report discusses means and methods to solve these questions from a conceptual and practical standpoint.

Following, this report is split in two parts. First part contains conceptual considerations of resilience, presenting state-of-the-art background from economic theory, conceptual security framework, mathematical ecosystem modelling and simulation as well as key contribution to decision making for stakeholders based on the concept of stewardship, even applied to cloud-based ecosystems.

Second part considers resilience with regards to policy and regulatory framework, organisations and technology development and application as well as auditing. We show the relation to management systems for quality, risk, security and continuity and derive realistic options for course of action.

1.2 Key words

Resilience, sustainability, robustness, adaptability, economics, eco-system, interconnection, dependency, social optimum, utility theory, stewardship, modelling, simulation, hazard, distortion, out-of-normal operational state, recover, critical information infrastructure, cloud, business continuity, BCM, integrated management systems, security, information security, ISMS, risk management, IT service management, ITSM, redundancy, resistance, EU internal market, policy makers, regulators.

1.3 First part

1.3.1 Introduction

Two pieces of resilience background are pertinent:

- The understanding and analysis of resilience and sustainability in the field of natural resource management; and
- Assurance models derived from information security and financial reporting (where there is useful quite old work in the accountancy literature).

Thus we view resilience, and its intimate relation sustainability, to be the key dynamic components of system stewardship. To this extent, these notes are based closely upon the paper, `Information Stewardship in Cloud Ecosystems: Towards Models, Economics, and Delivery', by Baldwin, Pym, Sadler, and Shiu, which is available at www.abdn.ac.uk/~csc335/pym-et-al-stewardship.pdf and in which the concepts of resilience and sustainability are explored within the context of cloud-based business ecosystems.

In addition to this conceptual perspective, we are also concerned here with the need for assurance models to be associated with stewardship properties in general and with resilience and sustainability properties in particular.

1.3.2 The Scientific and Technical Background

Information security is concerned with the confidentiality, integrity, and availability (CIA) of information — represented as stored data — in information processing systems, the objective information security operations being to protect these properties. Such protection is costly and is not absolute. Accordingly, the managers of information systems must determine not only their target levels of confidentiality, integrity, and availability, but also their target levels of investment or cost. In the analysis of information security architectures, with these concerns in mind, it has proved helpful to distinguish declarative and operational concepts [1]. This distinction sheds light on the inadequacy of many so-called refinements of the declarative concepts of confidentiality, integrity, and availability. Typically, such refinements confuse declarative and operational concepts and introduce concepts such as authentication, audit, non-repudiation, and even utility (see [26] for an extensive discussion along these lines). These are category errors: authentication (for example) should be seen as an operational mechanism by which aspects of the declarative objectives of confidentiality and availability can be delivered.

Utility theory, a cornerstone of economics, provides a conceptual and mathematical set-up for modelling how declarative security properties, such as confidentiality, integrity, and availability trade off against one another and against cost [14], [16], [15]. It also allows us to understand how the magnitudes of these properties may deviate from their targets as a system interacts with its environment and evolves. Expressions of utility are thus, with respect to (declarative) security objectives representations of the system manager's policy. The

management of inflation and unemployment by a central bank [31] provides a familiar example from macroeconomics. A bank might be set targets for these quantities, which trade off against each other, by its government. The bank's control variable that is the interest rate, and the bank's task is to set a monthly sequence of rates s0 that inflation and unemployment stay on target.

A key question here, explored in detail in [14], concerns the resilience of quantities of interest (with respect to maintaining target levels) when the system experiences shocks, such as a breach of confidentiality caused by a social engineering attack or the cracking of an encryption code, or the loss of a web-based service caused by a distributed denial of service attack.

This view of the economics of information security has proved to be valuable in advancing out conceptual under- standing of the decision processes around the protection of information in situations in which the owner or manager of the information maintains an intimate relationship with the service-provider and the information being processed by the provider. For example, as service-providers move to cloud ecosystems — that is, complex networks of interacting infrastructure providers, service providers and consumers — and as service-provision becomes more devolved and distributed within cloud ecosystems, this intimate relationship will be considerably weakened. Indeed, provided the information-owner's interests are properly protected, the opportunities provided by the cloud ecosystem may well be highly advantageous to the information-owner. Thus we are led to the concept of information stewardship. In this context, information stewardship would certainly encompass the security concerns that we have discussed, but would much more besides.

Informally, the notion of stewardship is understood to capture, in addition to the core concepts of information security, concepts such as the management and supervision of values, respect for ethics, duty of service, responsibility, and, in the context of stewardship of the ecosystem itself, the promotion of resilience and sustainability. The concepts and approaches that we have described above set out a collection of tools from economic and mathematical modelling that are of great utility in understanding the concept of information stewardship, it is useful to consider some notions of stewardship that have been found to be useful in other intellectual disciplines. One view (see, for example, various dictionaries) is that which has been developed in areas such political science, where the term is used to capture concepts such as the management and supervision of resources, adherence to principles, and the trusted prosecution of obligations. A steward, in this context, is one who is employed to carry out these functions on behalf of another or others. All of these notions might, at least in principle, be incorporated into the utility-theoretic and system modelling framework sketched above. However, we suggest that an alternative, and useful, point of departure is provided by the work of ecologists in understanding natural resource stewardship in natural social-ecological systems (for a comprehensive and thoughtful overview, see [13]). Here the key notion is that of a stakeholder in the ecosystem. For example, a cloud-based business ecosystem includes many stakeholders. Each stakeholder has a perspective on the structure and function of the ecosystem, which, together with its objectives, determines the

formulation of the stakeholder's utility function for its engagement in the operation of the ecosystem.

As we have seen, examples of stakeholders include individual participants (e.g., consumers, service providers, platform providers), policy-makers (within and outwith the ecosystem) and regulators (e.g., politicians, government agencies), providers of professional services in support of ecosystem operations (e.g., auditors, lawyers), and equipment manufacturers (e.g., computer and network infrastructure manufacturers). Each participant seeks to optimize, or at least satisfice, its own utility, according to the utility function that is appropriate for its perspective. The formulation of a stakeholder's utility function will, as usual, depend on a range of factors with, as has been argued in [14], [16], the perspective and techniques provided by macroeconomic and financial management being useful. The stakeholder will identify, as outlined above, a collection (sometimes called a basket) of quantities that are of concern, together with target values and weightings, and will identify a functional form to describe the desired utility as the value of each quantity deviates from target.

The challenge for the regulators is to identify a utility function that adequately reflects the objectives of the policy-makers. The policy-makers determine what is socially optimal, and the regulators must seek to deliver appropriate behaviour by the ecosystem by formulating an appropriate utility function for the overall system.

Overall, the stakeholders in the ecosystem are faced with the need to make multiple, multi-objective decisions about highly complex systems ([19], [2] are excellent starting points among many for the relevant theory). For policy-makers, and hence for regulators, it is likely that important objectives will be appropriate levels of resilience of the ecosystem as it is subject to shocks — such as changes in the economic conditions within which the ecosystem operates and security attacks against the technology or business processes — and the sustainability of the ecosystem over its lifetime of operations.

1.3.3 Resilience and Sustainability in Information-Business Ecosystems

In the world of natural resource management (e.g., [13], for a range of pertinent articles and a wealth of references), resilience and sustainability are perhaps the key drivers for the ecosystem's stewards. For Chapin, Kofinas, and Folke (in [13]), the key concept is that of resilience-based ecosystem stewardship, which 'involves responding to and shaping change in social-ecological systems to sustain the supply and opportunities for use of ecosystem services by society'. To provide an example, we discuss some of the key factors in the dynamics of cloud-based business ecosystems.

We can describe cloud-based business ecosystems in terms of the various participants (companies, etc.) who are either service consumers, service providers, or cloud platform providers. Each will interact with the others within the ecosystem, as well reacting to exogenous controls. Participants will use their knowledge of the state of the ecosystem to assess how they should interact with it to maintain their desired utility.

Ecologists consider ecosystems that vary overtime because of feedback loops. For example, a fast variable may be the population size of a particular animal. This variable will determine how much biomass is eaten, which in turn determines the available food and reflects back into the population size. Slower variables may be things like changes in the capacity of soil or sediments to supply water or nutrients or changes in types of plants and animals in the ecosystem. Exogenous controls may be changes in the regional climate. They then talk of two different factors being responsible for these changes, the ecological factors and the societal factors (i.e., the effect of humans on the ecosystem).

As we have mentioned, for Chapin, Kofinas , and Folke (in [13]), the key concept is that of resilience-based ecosystem stewardship, which they say 'involves responding to and shaping change in social-ecological systems to sustain the supply and opportunities for use of ecosystem services by society'. This view is useful because it emphasises two aspects of stewardship that are of particular concern in cloud ecosystems:

- Resilience: The capability of the system to recover from attacks that successfully compromise its declarative stewardship objectives (e.g., the confidentiality of a customer's PID is breached) or inhibit the effectiveness of its operational mechanisms to deliver its objectives (e.g., the loss of availability of authentication server); and
- Adaptability: The capability of the ecosystem to adapt to changes in its composition (infrastructure providers, service providers, consumers), in its required functionality, in its regulatory environment, and its threat environment. Adaptability is the key to sustainability.

Turning to questions of assurance for resilience, a useful starting point is provided by work in stewardship in the accountancy research literature that is concerned with financial reporting (e.g., [11, 12]).

1.4 Second Part

Our considerations below fit to certain OECD, EU and national principles and practices and, in particular, refer to international and national norms and standards like the ISO/IEC 27001 or the BS 25999-2.

At large scale, the EU, with its internal market, is an example of an interconnected ecosystem that is interdependent with the global non-EU economy and has a high level of complexity. Whenever policy-makers, as stakeholders of the EU, issue (political) objectives, economic and ecological considerations will help to carefully select policies and regulations promising optimal utility. Typical influencing aspects range from the political and social system, legislation, the regulatory framework, market structure, the (in)homogeneity of the internal market, the distribution and availability of natural resources, and the levels of infrastructural and technological development. Decisions can be based on gut feeling, which wasn't so bad for quite a few centuries, but which is hardly appropriate today. In considering how to support decision-making, we have discussed in the first part above the concept of stewardship and its

implications. In the following, realistic measures to assure a certain levels of resilience are discussed.

Information technologies (networks, systems, and components) have to support EU, nations, markets and citizens in reaching their desired utilities without unwanted disturbance or interruption, even in the presence of (a series of) crises. Because of the high dependency of almost any activities in the internal market on IT, the non-availability or corruption of IT networks with its services and data may have enormous impact. Therefore, the so called 'critical information infrastructure' (CII) must be identified at the EU level. A prerequisite for that is adequate knowledge of all 'critical activities', which are vital to the existence and survival of the whole EU, in the internal market. To gather that information, the various stakeholders of the internal market (governments, market players, task forces etc.) need to co-operate in a co-ordinated way abroad the EU, which is itself a substantial challenge.

Whenever the CII is known, we need to determine the objective of resilience. The property to resist a certain distortion requires knowledge of thinkable and possible distortions and their reasons. The reasons range, like it is usual in risk management, from human negligence, intentional attack through technical malfunction to force majeure (i.e., natural hazards). The impacts on the ecosystem activities in the EU can then be estimated. Two main thresholds are considerable for realistic scenarios: first, the required resistance of the CII against a defined strength of distortion without remarkable disturbance of the eco-system activities; second, the allowed amount of time to recover from a disastrous event to reach an acceptable level of service. One can consider that these are the over-arching resilience objectives for the CII.

There will be various different strategies needed to reach these CII resilience objectives. Also, they will differ for the different scales of the considered ecosystem. The underlying principles are easy to understand and based on an assumption, often underestimated: at small scale, say for a regular business organisation residing in the EU, the business with its critical business processes must be 'known' and 'managed' very well, comparable to the large scale consideration on the EU level, above. 'Managed' means thoroughly managing quality, risks and security of the organisation and its processes and results in case of 'normal' operation. Whenever the organization is seriously hurt by a change, hazard or attack, the organization is in an out-of-normal operational state – the regime of business continuity management (BCM). If we now want to reach the resilience objective related to 'resistance', then we are talking about measures applicable in the 'normal operational' regime of the organisation. In case of a disastrous event, the objective, to bring the organisation back to an acceptable level of service, will require another way of thinking, supportive measures known from the BCM.

To break down our considerations to the critical IT infrastructure of the aforementioned regular business organization residing in the EU, we have to call for organizational, infrastructural, personal and technological measures. Taken together, they will enforce the organizational 'resilience policy'. If the organization has an ISO/IEC 9000 like quality management system (QMS) in place, processes and procedures are known, their support to business is understood and assured, control and audit on whether defined organizational and procedural objectives are met will take place on a regular basis. Also, the effectiveness of the

underlying management system will be frequently reviewed, and accompanied by continuous improvements. A benefit assuring efficiency is the risk orientation of the QMS. This is because measures for risk treatment are to be derived and operated by the organization and targeted to assure that required performance of critical business processes be achieved. Here there would seem to be a role for employing underpinning management systems, like business risk management and (information) security management — as described, for example, in ISO/IEC 27001 (for information security management systems, ISMS) and ISO 31000.

Coming back to the IT as a regular business support including critical business processes. In the normal operational state, our example business organisation has regular "CIA" objectives in terms of information security, which require certain measures to support linked business objectives. This is embedded into the risk management context, i.e. efficiency has to be assured simultaneously. Dedicated IT measures are process based, so requirements engineering, release management, system monitoring or incident management are the frame in which specific dedicated technology measures are needed. That means, purchase of IT products or systems also need to thoroughly consider the purpose of use, so that the technical processes of an IT service are actually implementable by the organisation. For example, without a ticketing system, a balanced IT service is hardly possible. Incident reporting will then result in the possibility (and duty) of a certain follow-up. A simple power cut can then be tracked to its cause and then be fixed. If there would be neither reporting nor tracking (supported by automated means) and resolution, the organisational resilience in terms of 'resistance' can be expected very low.

A second aspect to strengthen the resistance is the architecture of the IT. For high availability purposes it is common to design the IT network and high load systems in a redundant manner. Examples are the use of multiple servers in parallel e.g. for web shops or a load balancing for directing network traffic to different network components. Redundancy, from its idea is simple. But, as it is with person and people, the more you have, the higher are the costs – and the (much) more difficult to manage. Take the example of a database system. If it is redundant, each data base should contain the same data, i.e. they need to be consistent. The network and DB design must be free of potential inconsistencies in effect, i.e. fault-tolerant, which is another supportive property of 'technical' resilience. You can think further of the fact, that a resilient IT will never work, if you use 'weak' components – for a 24x7 IT service infrastructure, it would be questionable to use hard drives for home use. To an end, you need to make sure to utilise inherently reliable components in the IT architecture. Finally, the used components, together with the architecture should follow the security principles, to continuously support the CIA objectives. Good practice for critical components, like a firewall or cryptographic operation is, to have an independent security analysis and so called 'evaluations'. They are a means to assure stat-of-the art security design, resistance against assumed threats and having less vulnerabilities than non-certified IT products. On system or network level, such analyses can be so called penetration tests.

In principle, we are fine now: resilient design and components will give a certain robustness. If we add furthermore a well-defined and rigorously implemented maintenance, then the job is

done. Business resilience is set up for normal operation. This is because in case of an incident, the maintenance will respond and not allow an unacceptable interruption.

The case is different, when there is a remarkable distortion, like the only site of our example organisation is flattened by an earthquake. The non-normal operational state requires emergency response teams with a specific organisational structure, use of out-of-site locations and connectivity. Customers, relatives and public agencies may to be contacted. This happens under the condition of a disaster. For that case, the BCM is the means to survive the moment and to bring the organisation, step-by-step, back to an acceptable level of operation and service. The discomfort of such situation should not lead to operational ignorance by any of its stakeholders. So the most important work to be done is before a disaster! If emergency processes, responsibilities and actions are not defined, tools and locations are not reserved and if the organisation is not trained, the disaster may be final to the organisation.

1.5 Conclusion

Resilience is a vital aspect 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 case of serious distortions and hazards. In any case, 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 also from a practical point of view. The balancing of utility (social wealth) and costs, avoiding externalities at the same time, is then the crucial part before decisions. A dedicated multi-disciplinary team of stakeholders might prepare bundles of course of actions for numerous realistic scenarios applicable to the EU internal market and identify most promising sets based on thorough in-depth analyses. The results will be then the resilience tools for the decision makers in alignment with existing policies and directives.

1.6 Stakeholders

European institutions, national authorities, national security institutions, sector regulators, Non-Governmental Organisations and Law Enforcement Agencies are stakeholders regarding policies, legislation, regulatory and law-enforcement related to resilience.

Individual and consumer organisations and professional associations are stakeholders with respect to the need and implementation of resilience.

IT developers, vendors and IT operators together with IT audit organisations and Research Institutions/Universities are stakeholders regarding development, distribution, operation and audit of robust IT.

1.7 Implication to EU policies and directives:

European Commission (2006): Defining the Commission's global policy on the fight against cyber crime. This report has implications in specific to problem

- Area 3: A lack of a coherent EU-level policy and legislation for the fight against cyber crime
- Area 5: Need to develop competence and technical tools (training and research)
- Area 8: The lack of awareness among consumers and others of the risks emanating from cyber crime

1.8 Bibliography on further reading

[1] A. Beautement and D. Pym. Structured systems economics for security management. In Tyler Moore, editor, Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS 2010), 2010. http: //weis2010.econinfosec.org/papers/session6/weis2010 beautement.pdf.

[2] Ken Binmore. Rational Decisions. Princeton University Press, 2008.

[11] Accounting Standards Board (ASB) et al. Stewardship/Accountability as an Objective of Financial Reporting: A comment on the IASB/FASB Conceptual Framework Project. Technical report, ASB, Foreningen af Statsautoriserede Revisor, Deutsches Rechnungslegungs Standards Committee, Komitet Standardo´w Rachunkowoci and EFRAG, 2007.

[12] F. Gjesdal. Accounting for Stewardship. Journal of Accounting Research, 19(1):208–231, 1981.

[13] Chapin III, F. S., G. P. Kofinas, and C. Folke (editors). Principles of Ecosystem Stewardship: Resilience-Based Natural Resource Management in a Changing World. Springer-Verlag, 2009.

[14] C. Ioannidis, D. Pym, and J. Williams. Investments and trade-offs in the economics of information security. In Roger Dingledine and Philippe Golle, editors, Proc. of Financial Cryptography and Data Security ’09, volume 5628 of LNCS, pages 148–166. Springer, 2009. Preprint at http://www.cs.bath.ac.uk/∼pym/IoannidisPymWilliams- FC09.pdf.

[15] C.Ioannidis, D.Pym, and J.Williams.Fixedcosts,investmentrigidities, and risk aversion in information security: A utility-theoretic approach. In Bruce Schneier, editor, Proc. 10th Workshop on the Economics of Information Security. Springer, 2011. In press.

[16] Christos Ioannidis, David Pym, and Julian Williams. Information Security Trade-offs and Optimal Patching Policies. European Journal of Operational Research, 2011. doi:10.1016/j.ejor.2011.05.050.

[17] R. Jain. The Art of Computer Systems Performance Analysis. Wiley, 1991.

[18] R.W.Y Kao. Stewardship-based economics. World Scientific, 2007.

[19] R.L. Keeney and H. Raiffa. Decisions with multiple objectives: Preferences and value tradeoffs. Wiley, 1976.

[26] Donn B. Parker. Fighting Computer Crime: A New Framework for Protecting Information. Wiley, 1998.

[31] Francisco J. Ruge-Murcia. Inflation targeting under asymmetric preferences. Journal of Money, Credit, and Banking, 35(5), 2003.

2 Behavioural Economics of Security

By Nicolas Christin, *Carnegie Mellon University* and Jens Grossklags, *The Pennsylvania State University*[1]

2.1 Keywords

Rational agents, Bounded rationality, Human biases, Behavioral interventions, Formal behavioral models, Field and laboratory experiments, Cybercrime measurement studies

2.2 Overview

The behavioral economics of security aims to advance the systematic understanding of the tussles between attackers and defenders by integrating lessons from behavioral research conducted in the lab and field. We can draw from a wide range of psychology research, but also 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.

The starting point of most studies is the concept of *rationality*. A variety of candidate definitions exist that invariably assume individuals to adhere to certain consistency requirements, but also that they can determine and implement optimal strategies without error [4].

Observed behaviors may frequently be misunderstood to be incompatible with the assumptions of rationality. An excellent example is the Peltzman effect that can be found in the domain of computer security [10]. Much like drivers wearing seatbelts or helmets tend to drive faster, people tend to behave more insecurely online when they believe they have adopted secure precautions, such as installing an anti-virus scanner [10]. However, as individuals optimize across multiple goals (e.g., safety and joy of driving) we may interpret such behavior as potentially rational.

However, the analysis of security scenarios rarely requires only simple and straightforward cost-benefit reasoning. The organization of attacks and defenses is typically highly complex and heightens the difficulty of determining reasonable predictions for associated probabilities and/or payoffs [3].

The intricacy of decision-making is also partly rooted in the spotty information availability. Asymmetric, limited, incomplete or even unknown information increases the burden when trying to identify optimal choices. Further, security decisions are required over a long time frame with consequences becoming known potentially much later. The variability and many-

[1] Authors listed in alphabetical order.

sidedness of potential attack and defense moves also dramatically increases the strategy space to be considered, in particular, in repeated and dynamic interactions.

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, due to strategic information advantages.

As a result, the existence of optimal security choices can be indeterminable for the human mind or even computationally intractable and thereby reveal our *bounded rationality* [45]. Humans (and human-programmed tools) can still exercise significant effort and utilize approximations to identify *near-optimal decisions* [11].

However, effort is not always spent in finding optimal or near-optimal outcomes. Subconsciously, decisions are often made in a *satisficing* manner to arrive at a sufficient response [27]. Indeed, human attention would be wasted if every time a full analysis would be conducted for reoccurring scenarios [5]. *Rational ignorance* will lead humans to consciously choose the satisficing path if the expected cost of analyzing a scenario would exceed the anticipated impact [2, 9, 20]. But satisficing also carries the possibility of serious decision mistakes.

The structure of security situations also triggers a number of psychological decision-making *biases and fallacies*. Humans deviate from optimal strategies in a predictable fashion when specific circumstances are met (even if the more advantageous course of action is known to the decision-maker). Individuals (and the organizations they lead) delay on important infrastructure investments or updates to key security technologies because they consistently underappreciate future consequences [38]. Decision-makers also have a strong tendency to isolate groups of events for analysis rather than to appreciate the bigger picture [43].

Taken together, security situations can be highly complex and diverse driving the utilization of heuristic and biased decision-making. Motivation can play a critical role in this process. Individuals need to accept the responsibility to invest the effort for a comprehensive analysis. In contrast, one might argue that our bounded rationality naturally implies a limited strategy and humans should be absolved from the burden of responsibility to make optimal decisions [16].

In the following, we review critical research that addresses the sources of complexity of security decisions. Further, we consider studies of human behavior and motivation and discuss avenues for intervention.

2.3 Understanding attackers

During the early days of the Internet, the majority of attackers were motivated by peer recognition, or curiosity [22, 47]. More recently, this tradition was carried forward in the form of hacktivism, i.e., the facilitation of security breaches to promote an activist agenda [44].

However, in the last ten years, financial motives have moved to the foreground as shown by a large body of recent literature [6, 12-15, 24, 25, 29, 30, 32-37, 48]. Monetization vectors

include email [24, 30] and social network [15] spam campaigns to peddle products; advertising frauds [36]; black hat search engine manipulation [29, 36]; and malware installations [6, 39, 40]. Studying the economic relationships existing between the different actors behind these frauds will yield precious clues regarding the efficiency of various intervention mechanisms. Specifically, we can discern potential behavioral patterns among attackers, that may reveal infrastructural weaknesses: for instance, if we notice that most phishing scams use only a couple of DNS registrars, it stands to reason that applying pressure onto these registrars would certainly make the attackers' job at least marginally more difficult.

Furthermore, a number of profits are illicitly obtained from social engineering scams, including phishing [32, 33, 35], 419 scams, fake anti-virus distribution [13, 48], and coercion scams [12]. In other words, attackers have become very apt at preying on certain behavioral traits (i.e., greed, fear, shame) that breed insecure practices, and extracting financial gain from them. Characterizing these human fallacies is needed to better know how to address them.

2.4 Understanding defenders

As mentioned above, attackers often prey on known behavioral traits that facilitate scams. Analyzing a number of confidence scams, Stajano and Wilson provide a taxonomy of these behavioral biases [46], and derive principles to address them and improve system security. Most of the principles derived (e.g., distraction, compliance to authority, ...) equally apply to the online realm as they do to the offline realm. However, the work in this field so far has been descriptive. In particular, there does not exist quantitative measurements of attacker success in the various categories of scams.

Another important line of work in behavioral aspects of security is in the evaluation and design of usable security policies. As an example, password composition rules (e.g., rules specifying that a password must consist of at least eight letters, and include at least a digit and a non-alphanumeric symbol) have long been thought to be useful in increasing the entropy, and thus the security of user-chosen passwords. Recent studies, e.g., [26], however show that, while, as expected, usability greatly suffers from too-stringent rules, password security is not necessarily increasing with the complexity of the password composition rules. Such insights are important as very often, policies are based on "common sense," rather than formal evaluation and verification.

2.4.1 Formalization of behavioral decision-making and experimental test

An important aspect of behavioral economics is the formalization of psychological insights in economic models [7, 42]. Spearheading this approach, Kahneman and Tversky developed prospect theory [23], i.e., humans tend to be risk-averse when it comes to gains; and risk-seeking in the domain of losses. Behaviorally-inspired models mainly aim to extend previous formalizations of fully rational behavior. Main fields of work include advances in the modeling of preferences, risk evaluation and behavior, understanding of (less than complete) information and ambiguity, and decision-making over time [8].

Individuals may have to consider incentives of other agents when they develop their own strategies. In the security arena, such incentives are typically in conflict (i.e., between attackers, between defenders, and, of course, between defenders and attackers). But it is conceivable that groups (e.g., hacker forums) also reveal helping, fairness or other-regarding preferences (e.g., [41]).

Moreover, the interaction between multiple decision-makers may be subject to interdependencies that shape incentives according to some topological or other structural rules [18, 28]. Matching laboratory studies have been performed to study the impact of interdependencies in the security context and to verify or challenge the accuracy of the models [17, 21].

2.4.2 Moving forward: Influencing defender behavior

Most work in the area of behavioral economics has focused on integrating behavioral insights as part of formal economic theory and to test these models. Equally relevant, however, is the development of intervention strategies. Economics has traditionally played a significant part in this area, for example, in the form of mechanism design. However, interventionist approaches in behavioral economics are still rare [31]. Notable exceptions include attempts to influence individuals' retirement savings behavior [49].

Most ideas in this area centre around the concept of nudging [50]. Essentially, the goal is to structure choices (e.g., by different ways of presenting options or setting defaults) such that individuals consider less harmful or in some other aspect preferable strategies that would otherwise be ignored because of behavioral biases. Nudging has also been considered in the context of protection of personal information [1]. Further, the combination of such ideas with classical carrot-and-stick economic incentives can help to, for example, overcome difficult coordination problems to protect or insure resources [19].

2.5 *Stakeholders and applicability to regulation*

While the above discussion clearly outlines the need for considering behavioral factors in security engineering, it does not make clear who should be in charge of performing this work; and who should be in charge of implementing possible intervention policies.

When it comes to behavioral economics of security, the primary stakeholders, on the defensive side, belong to three categories: *research institutions* – mostly universities, but possibly private research laboratories as well, *law enforcement agencies* or, perhaps more generally, *national security institutions*, and *content providers* (e.g., software manufacturers). Because a lot of the work needed in behavioral economics of security is at a fundamental

level, it can rarely be immediately translated into products,[2] and therefore seems a more natural fit for research universities than for private industrial research labs.

Law enforcement agencies – or national security institutions – have also a vested interest in this work. Similar to psychological profiling sometimes used to help identifying perpetrators of physical crimes, we argue that law enforcement agencies would be well-served by developing behavioral units to assist in their cybercrime investigations. This would help 1) identify the traits attackers may be looking for in victims, and 2) build profiles of attackers' motives.

Content providers such as software manufacturers also have a clear stake in this line of work, as they can translate some of the behavioral findings into actual mitigation strategies; for instance, when designing warnings or security configuration systems.

We stress the importance to the regulator that behavioral research be actively encouraged and supported. Regulators need to understand the shortcomings (outlined above) of relying on the rational model. But even more importantly, behavioral interventions cannot be deployed without having been properly studied in the field and laboratory prior to legislation.

Finally, several of the mechanisms miscreants use could be made more difficult to exploit by appropriate enforcement of existing rules. For instance, registration of an Internet domain name (e.g., example.com) requires, in principle, a valid identity, so that consumer protection authorities and/or law enforcement can contact the owner of the domain if said domain is engaging in questionable activities. However, this identification requirement is rarely enforced, and a number of domains are registered with fake identities. It goes without saying that vandals rarely use actual contact information when registering domains. In this example, mere enforcement of existing rules would go a long way toward making it more onerous for attackers to set up the infrastructure their schemes require. It is not clear whether supplemental regulation would be needed, or if, on the other hand, existing (contractual) obligations would suffice, as long as they are actively enforced.

What is more obvious, however, is that we still have a limited understanding of the behavioral and economic aspects factoring into modern attacks, and that we need to bridge that gap to be able to devise effective defenses.

References

[1] A. Acquisti. Nudging privacy: The behavioral economics of personal information. *IEEE Security & Privacy*, 7(6):82–85, November–December 2009.

[2] A few companies, such as Usable Systems, were able to transition their behavioral research into practical products, e.g., user authentication systems, but this is the exception rather than the rule.

[2] A. Acquisti and J. Grossklags. Privacy attitudes and privacy behavior: Losses, gains, and hyperbolic discounting. In J. Camp and S. Lewis, editors, *The Economics of Information Security*, pages 165–178. Kluwer Academic Publishers, 2004.

[3] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1):26–33, 2005.

[4] L. Blume and D. Easley. Rationality. In S. Durlauf and L. Blume, editors, *The New Palgrave Dictionary of Economics*. Palgrave Macmillan, 2008.

[5] R. Böhme and J. Grossklags. The security cost of cheap user interaction. In *Proceedings of the 2011 New Security Paradigms Workshop (NSPW)*, 2011.

[6] J. Caballero, C. Grier, C. Kreibich, and V. Paxson. Measuring pay-per-install: The commoditization of malware distribution. In *Proceedings of USENIX Security 2011*, San Francisco, CA, August 2011.

[7] C. Camerer. *Behavioral Game Theory: Experiments in Strategic Interaction*. Princeton University Press, Princeton, NJ, 2003.

[8] C. Camerer and G. Loewenstein. Behavioral economics: Past, present, future. In C. Camerer, G. Loewenstein, and M. Rabin, editors, *Advances in Behavioral Economics*, pages 3–51. Princeton University Press, 2004.

[9] B. Caplan. Rational irrationality. In C. Rowley and F. Schneider, editors, *The Encyclopedia of Public Choice*, pages 795–797. Springer Verlag, 2003.

[10] N. Christin, S. Egelman, T. Vidas, and J. Grossklags. It's all about the Benjamins: Incentivizing users to ignore security advice. In *Proceedings of IFCA Financial Cryptography'11*, Saint Lucia, March 2011.

[11] N. Christin, J. Grossklags, and J. Chuang. Near rationality and competitive equilibria in networked systems. In *Proceedings of ACM SIGCOMM'04 Workshop on Practice and Theory of Incentives in Networked Systems (PINS)*, pages 213–219, Portland, OR, August 2004.

[12] N. Christin, S. Yanagihara, and K. Kamataki. Dissecting one click frauds. In *Proc. ACM CCS'10*, Chicago, IL, October 2010.

[13] M. Cova, C. Leita, O. Thonnard, A. Keromytis, and M. Dacier. An analysis of rogue AV campaigns. In *Proc. RAID 2010*, Ottawa, ON, Canada, September 2010.

[14] J. Franklin, V. Paxson, A. Perrig, and S. Savage. An inquiry into the nature and causes of the wealth of internet miscreants. In *Proceedings of 14th ACM Conference on Computer and Communications Security (CCS)*, pages 375–388, Alexandria, VA, October 2007.

[15] C. Grier, K. Thomas, V. Paxson, and M. Zhang. @spam: The underground in 140 characters or less. In *Proceedings of ACM CCS 2010*, Chicago, IL, October 2010.

[16] J. Gross Stein. Can decision-makers be rational and should they be? Evaluating the quality of decisions. In M. Brecher, editor, *Studies in crisis behavior*, pages 316–338. The Hebrew University of Jerusalem, 1978.

[17] J. Grossklags, N. Christin, and J. Chuang. Predicted and observed behavior in the weakest-link security game. In *Proceedings of the 2008 USENIX Workshop on Usability, Privacy and Security (UPSEC'08)*, San Francisco, CA, April 2008.

[18] J. Grossklags, N. Christin, and J. Chuang. Secure or insure? A game-theoretic analysis of information security games. In *Proceedings of the 2008 World Wide Web Conference (WWW'08)*, pages 209–218, Beijing, China, April 2008.

[19] J. Grossklags, S. Radosavac, A. Cárdenas, and J. Chuang. Nudge: Intermediaries' role in interdependent network security. In *Proceedings of the 3rd International Conference on Trust and Trustworthy Computing (TRUST)*, pages 323–336, Berlin, Germany, June 2010.

[20] C. Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 New Security Paradigms Workshop (NSPW)*, pages 133–144, 2009.

[21] R. Hess, C. Holt, and A. Smith. Coordination of strategic responses to security threats: Laboratory evidence. *Experimental Economics*, 10(3):235–250, September 2007.

[22] T. Jordan and P. Taylor. A sociology of hackers. *The Sociological Review*, 46(4):757–780, November 1998.

[23] D. Kahneman and A. Tversky. Prospect theory: An analysis of decision under risk. *Econometrica*, XLVII:263–291, 1979.

[24] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage. Spamalytics: An empirical analysis of spam marketing conversion. In *Proceedings of the Conference on Computer and Communications Security (CCS)*, Alexandria, VA, October 2008.

[25] C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G. Voelker, and S. Savage. Show me the money: Characterizing spam-advertised revenue. In *Proceedings of USENIX Security 2011*, San Francisco, CA, August 2011.

[26] S. Komanduri, R. Shay, P. Kelley, M. Mazurek, L. Bauer, N. Christin, L. Cranor, and S. Egelman. Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of 2011 ACM Symposium on Computer-Human Interaction (CHI'08)*, pages 2595–2604, Vancouver, BC, Canada, May 2011.

[27] J. Krosnick. Response strategies for coping with the cognitive demands of attitude measures in surveys. *Applied Cognitive Psychology*, 5:213–236, 1991.

[28] H. Kunreuther and G. Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26(2–3):231–249, March 2003.

[29] N. Leontiadis, T. Moore, and N. Christin. Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade. In *Proceedings of USENIX Security 2011*, San Francisco, CA, August 2011.

[30] K. Levchenko, N. Chachra, B. Enright, M. Felegyhazi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, A. Pitsillidis, N. Weaver, V. Paxson, G. Voelker, and S. Savage. Click trajectories: End-to-end analysis of the spam value chain. In *Proceedings of the IEEE Symposium and Security and Privacy*, Oakland, CA, May 2011.

[31] K. Milkman, D. Chugh, and M. Bazerman. How can decision making be improved? *Perspectives on Psychological Science*, 4(4):379–383, July 2009.

[32] T. Moore and R. Clayton. Examining the impact of website take-down on phishing. In *Proceedings of the Second APWG eCrime Researcher's Summit*, Pittsburgh, PA, October 2007.

[33] T. Moore and R. Clayton. Evil searching: Compromise and recompromise of internet hosts for phishing. In *Proceedings of the 13th International Conference on Financial Cryptography and Data Security*, Barbados, February 2009.

[34] T. Moore, R. Clayton, and R. Anderson. The economics of online crime. *Journal of Economic Perspectives*, 23(3):3–20, Summer 2009.

[35] T. Moore, R. Clayton, and H. Stern. Temporal correlations between spam and phishing websites. In *2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)*, Boston, MA, April 2009.

[36] T. Moore, N. Leontiadis, and N. Christin. Fashion crimes: Trending-term exploitation on the web. In *Proceedings of ACM CCS 2011*, Chicago, IL, October 2011.

[37] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. Voelker. Dirty jobs: The role of freelance labor in web service abuse. In *Proceedings of USENIX Security 2011*, San Francisco, CA, August 2011.

[38] T. O'Donoghue and M. Rabin. Doing it now or later. *American Economic Review*, 89(1):103–124, March 1999.

[39] N. Provos, P. Mavrommatis, M. Rajab, and F. Monrose. All your iFrames point to us. In *Proceedings of the 17th USENIX Security Symposium*, August 2008.

[40] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N. Modadugu. The ghost in the browser: Analysis of web-based malware. In *Proceedings of the First USENIX Workshop on Hot Topics in Understanding Botnets (HotBots'07)*, Cambridge, MA, April 2007.

[41] M. Rabin. Incorporating fairness into game theory and economics. *American Economic Review*, 83(5):1281–1302, December 1993.

[42] M. Rabin. Psychology and economics. *Journal of Economic Literature*, 36(1):11–46, March 1998.

[43] D. Read, G. Loewenstein, and M. Rabin. Choice bracketing. *Journal of Risk and Uncertainty*, 19(1–3):171–197, 1999.

[44] A. Samuel. *Hacktivism and the Future of Political Participation*. PhD thesis, Harvard University, Cambridge, MA, September 2004. Department of Government.

[45] R. Selten. Features of experimentally observed bounded rationality. *European Economic Review*, 42:413–436, 1998.

[46] F. Stajano and P. Wilson. Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, 54(3):70–75, March 2011.

[47] B. Sterling. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Bantam Books, New York, NY, 1992.

[48] B. Stone-Gross, R. Abman, R. Kemmerer, C. Kruegel, D. Steigerwald, and G. Vigna. The underground economy of fake antivirus software. In *Proceedings of the 10th Workshop on the Economics of Information Security*, Fairfax, VA, June 2011.

[49] R. Thaler and S. Benartzi. Save more tomorrow: Using behavioral economics to increase employee savings. *Journal of Political Economy*, 112(1):S164–S187, February 2004.

[50] R. Thaler and C. Sunstein. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press, New Haven, CT, 2008.

3 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, picot/janello/kranz@lmu.de)

In this section, we (1) outline to which extent information security can be categorized as public good and (2) show the affected stakeholders' major economic challenges of information security (incentives, information asymmetries, and externalities) and (3) provide an outlook on a future research and policy agenda.

First of all, we have to address the question why security can be seen as a good at all. As security comes at a cost, this becomes obvious and hence, tolerating some level of insecurity is economically rational. From an economic perspective, the key question is whether the costs and benefits perceived by market players are aligned with social costs and benefits of an activity (van Eeten and Bauer 2008).

As the internet itself can be seen as a public good (Huberman and Lukose 1997), it is likely that ICT-Security shows public good-characteristics as well. The consumption of public goods is defined to be non-rivalrous and non-excludable, as shown in the well-known matrix below (Olson 1965, Musgrave 1969, Picot 2009). Common examples for public goods are e.g. street-lighting or clean air.

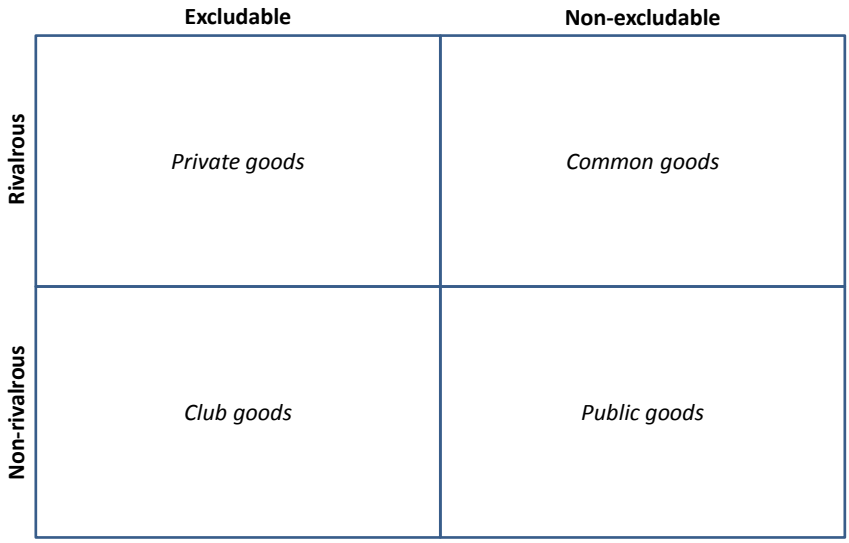


Figure 1 – Classification of goods (based on Picot 2009)

As rivalry in the context of information security measures will hardly occur, we only have to determine if security-measures are excludable from consumption by price-mechanisms. This is surely the case with e.g. encryption technologies ensuring confidentiality of information. But on the contrary, some level of ICT-security is a prerequisite for the globally interconnected

economy to work. This is also true for the internet's services to function. Basically a secure internet resembles a functioning banking sector which is essential for doing business. Malevolent or careless users can cause harm to other users, e.g. through spam-messages. Thus, they emit negative externalities. Further their incentive to invest in security is insufficient as they only partly, if at all, have to bear the negative effect.

Due to these effects, public goods often lead to market failures. If their existence is nevertheless desired by society, their provision has to be safeguarded by means of regulatory intervention from some superseding level of governance (Picot 2009). To these means pertain, e.g. legislation (such as liability laws), taxes, requirements, bans and rules and quotas, often designed to fight external effects.

A reasonable goal for regulation of ICT-security as a public good would be the provision of an economically sufficient level of ICT-security to ensure the operability of the ICT-economy.

In the following, we briefly outline the major economic challenges of information security for each of the main stakeholders regarding ICT products' security and services. Table 1 shows each stakeholder's received externalities, incentives, and information asymmetries as well as the entities that are most important for reducing or eliminating these negative externalities and incentives for the respective stakeholder. As mentioned above, total security is neither achievable nor desirable. Hence, each actor will carefully make a tradeoff between costs and benefits associated with security measures since they often do not bear the full costs of failure. Additionally, they are not able to internalize the full benefits as in IT systems third parties regularly benefit from others' security investments.

Thus, from a societal perspective, the question is whether the respective actor's incentives are in line with the costs and benefits of the society as a whole. Incentives can be classified as either monetary or non-monetary with either a short- or long-term effect. Depending on the effect on the objective they are referred to as either "positive" or "negative" incentives. An actor's specific incentives will result in a decision (e.g., whether and how much to invest in security) which will cause externalities for the other stakeholders.

Externalities are "forms on interdependence between agents that are not reflected in market transactions" (van Eeten and Bauer 2008) and, thus, not in usual accounting procedures. This leads to deviations from a socially optimal allocation of resources. Externalities either cause a good's underuse or underproduction (positive externality) or overuse or overproduction (negative externality) (Friedman 2002, pp. 599). When a good's production causes positive or negative externalities it often indicates that a public good might be affected.

Owing to the high degree of stakeholders' interconnectedness in ICT networks, many externalities arise within these IT systems. Moreover, these externalities rapidly percolate through ICT networks. Thus, understanding the stakeholders' incentives, existing information asymmetries, and the externalities they are exposed to is vital for identifying open issues for a future research agenda and the role of governmental and other regulatory agencies.

3.1 Areas of applicability

Owing to the high degree of stakeholders' interconnectedness in ICT networks, many externalities arise within these IT systems. Moreover, these externalities rapidly percolate through ICT networks. Thus, understanding the stakeholders' incentives, existing information asymmetries, and the externalities they are exposed to is vital for identifying open issues for a future research agenda and the role of governmental and other regulatory agencies.

3.2 List of bibliographic references

- Anderson, R. and Moore, T. (2007). Information Security Economics - and Beyond. Computer Laboratory, University of Cambridge. http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf.
- Arbor Networks (2007). Worldwide Infrastructure Security Report, Volume III. http://www.arbornetworks.com/report.
- Bélanger, F. and Carter, L. (2008). Trust and risk in e-government adoption. The Journal of Strategic Information Systems, Vol. 17, No. 2, pp. 165-176.
- Christin, N., Egelman, S., Vidas, T. and Grossklags, J. (2011). It's All About the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice. Proceedings of the 15th International Conference on Financial Cryptography and Data Security (FC'11). St Lucia. http://www.andrew.cmu.edu/user/nicolasc/publications/CEVG-FC11.pdf.
- Florencio, D. and Herley, C. (2007). A Large-Scale Study of Web Password Habits. http://research.microsoft.com/pubs/74164/www2007.pdf.
- Friedman, L. (2002). The Microeconomics of Public Policy Analysised. Princeton: Princeton University Press.
- Grossklags, J., Christin, N. and Chuang, J. (2008). Predicted and Observed User Behavior in the Weakest-Link Security Game. In Proceedings of the 2008 USENIX Workshop on Usability, Psychology, and Security (UPSEC'08). San Francisco, CA. April 2008. http://www.usenix.org/events/upsec08/tech/full_papers/grossklags/grossklags.pdf.
- Herley, C. (2009). So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf.
- Higgins, K. (2007). Battling Bots, Doing No Harm. Dark Reading. http://www.darkreading.com/document.asp?doc_id=118739.
- House of Lords (2007). Science and Technology Committee, 5th Report of Session 2006-07, Personal Internet Security, Volume I: Report. Authority of the House of Lords. http://www.publications.parliament.uk/pa/ld/ldsctech.htm.
- Huberman, B. A. and Lukose, R. M. (1997). Social Dilemmas and Internet Congestion. Science, Vol. 277, No. 5325, pp. 535-537.
- Jakobsson, M., Tsow, A., Shah, A., Blevis, E. and Lim, Y. (2007). What Instills Trust? A Qualitative Study of Phishing. http://www.informatics.indiana.edu/markus/papers/trust_USEC.pdf.

- Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G., Paxson, V. and S., S. (2008). Spamalytics: An empirical analysis of spam marketing conversion. In Proceedings of the 15th ACM Conference on Computer and Communications Security. Alexandria, Virginia, USA, October 2008. http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf.
- Komiak, S. and Benbasat, I. (2004). Understanding Customer Trust in Agent-Mediated Electronic Commerce, Web-Mediated Electronic Commerce, and Traditional Commerce. Information Technology and Management, Vol. 5, No. 1-2, pp. 181-207.
- Komiak, S. and Benbasat, I. (2006). The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents. MIS Quarterly, Vol. 30, No. 4.
- Mitnick, K. and Simon, W. (2008). The Art of Deception. Controlling the Human Element of Securityed. New York: Wiley.
- Moore, T. and Clayton, R. (2011). The Impact of Public Information on Phishing Attack and Defense. Communications and Strategies, Vol. 81, No. 1, pp. pp. 45-68.
- Mulligan, D. and Bamberger, K. (2007). Security breach notification laws: Views from chief security officers. Samuelson Law, Technology & Public Policy Clinic, Univ. of California, Berkeley School of Law. http://www.law.berkeley.edu/clinics/samuelson/csostudy.pdf.
- Musgrave, R. A. (1969). Provision for social goods. In: Public economics. Margolis, J. and Guitton, H. (eds.). London/New York: pp. 124-144.
- Olson, M. (1965). The logic of collective action – Public goods and the theory of groupsed. Cambridge.
- Pavlou, P., Liang, H. and Xue, Y. (2005). Understanding and mitigating uncertainty in online environments: A longitudinal analysis of the role of trust and social presence. Academy of Management Conference,
- Picot, A. (2009). Unternehmen zwischen Markt und Staat – Regulierung als Herausforderung. zfbf, Vol. 61, No. 9, pp. 655-678.
- Ransbotham, S. (2010). An Empirical Analysis of Exploitation Attempts based on Vulnerabilities in Open Source Software at the Workshop on the Economics of Information Security, (Harvard University, Cambridge). http://www.samransbotham.com/sites/default/files/Ransbotham_OpenSourceExploitationDiffusion_WEIS_2010.pdf.
- Van Eeten, M., Bauer, J., Asghari, H. and Tabatabaie, S. (2010). The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data. STI Working Paper 2010/5. OECD. http://www.oecd.org/officialdocuments/displaydocument/?doclanguage=en&cote=dsti/doc(2010)5.
- Van Eeten, M. J. and Bauer, J. M. (2008). Economics of Malware.

4 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, s.cavallini/f.bisogni@formit.org)

4.1 Abstract

This paper aims at illustrating how lack of information may affect security strategy of the potential stakeholders inducing a sub-optimal behaviour. In the NIS context, the bias perception of risk for the limited information may induce under-investments in security and the network feature of information systems spreads to all connected stakeholders negative externalities. Economic incentives addressing the different types of stakeholders may induce a higher protection of the single and, consequently, of the entire information system. For each identified effect caused by the lack of information an example of economic incentive will be proposed with a potential policy indication.

4.2 Keywords

Externalities (ENISA list), incentives, information asymmetries, lack of information, public goods, risk assessment, investment, market failures, security.

4.3 Executive summary

Security matters, and especially those related to network and information security, affect the overall society. Each single type of stakeholder (e.g. citizens, NIS operator, infrastructure operator, public administrator) defines its security level according to potential suffered damages in case of lack of security, but this behaviour leads to a sub-optimal level of security at least for two main reasons:

- The nature of public good of security. Each stakeholder defines its (high/low) security level that affects (positively/negatively) also other connected stakeholders.
- The role of information asymmetry and lack of information. Each stakeholder would define its security strategy according to potential suffered damages, if he/she had all information available on potential threats, their damages and their probability. Information asymmetries or lack of information induce to define security level different from the optimal one.
-

Both of these market failures may lead to an underinvestment in security: in the first case especially from the societal point of view, in the second case also for the single stakeholder.

Economic incentives are not to be considered as direct transfer of money addressed to one or more types of stakeholders to improve their security levels but as mechanisms leading to spontaneous efficient behaviours addressed to increase protection.

To this purpose, specific economic incentives should be addressed to the different types of stakeholders in order to solve potential distortions affecting the security market.

4.4 Involved Stakeholders

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 (Kolfal et al., 2010). To this aim, different stakeholder types with specific roles in security of information systems can be identified. Among these, citizens, public bodies/authorities, ICT operators and operators of other critical infrastructures assume a strategic role.

- Citizens, intended as general private end-users, carry the social interest in using ICT infrastructures and services provided by other critical infrastructures. For instance, in the event of a cyber-attack on the mentioned infrastructures, the society, as the aggregation of all citizens, would suffer larger negative externalities since it has less direct capacity to contain effects.
- Public bodies and authorities have the main goal to protect the social interest and can directly support prevention, protection and reaction to security breaches through regulation (top-down approach) or action (bottom-up approach) that encourage all stakeholders to bear part of the security costs.
- ICT operators, intended as operators who directly manage Internet connections (such as Internet Service Providers and telecom operators), are directly involved in the security issues and considered the most liable actors. Due to the fact that they manage ICT infrastructures and connected services, in the case of a successful attack, they would suffer the most direct consequences, but wide damages would also affect the rest of society.
- Operators of other critical infrastructures have a double damage-spreading role that has recently increased their responsibilities. On the one hand, if an operator of a critical infrastructure affecting ICT operators (e.g. an electricity provider) becomes, for example, a cyber-crime target, its failure may cause a large disruption of ICT services. On the other hand, if an ICT operator suffers a cyber-attack, cascading effects on other critical infrastructures (e.g. hospitals) might be spread to the entire society with relevant impacts for non-ICT users.

Each of these 4 stakeholder types has to balance investments and costs suffered as consequence of expected security failures. Starting from the analysis of the security investment behaviour of ICT operators, effective actions in terms of economic incentives can be suggested to public decision makers in order to overpass potential market failures related to the security market.

4.5 Summary of existing work

Mainstream literature and consolidated on economics incentives for security strongly focus on the role of information asymmetry and lack of information in defining security strategies. Information availability represents a key element influencing risk assessment processes and, consequently, security investment decisions.

In each context, information and its availability among the possible stakeholders represent one of the essential elements for the definition of complete markets. Information can be asymmetric or lacking.

In the first case, one stakeholder can take advantage from the complete information respect to the others. The market for lemons of the used cars proposed by Akerloff (1970) shows the bias effects on the car market of the complete information on the quality of the car of the seller respect to the inexpert buyer.

In the case of lack of information, the interested stakeholders behave in a sub-optimal way without any advantage for other stakeholders.

Business users, public authorities and citizens demand secure information systems, and ICT operators have set up investment strategies in order to provide ICT services at a suitable level of security.

The societal demand of security provides an indication to ICT operators of their costs in terms of losses related to the lack of security and, consequently, the needed amount of investment. For an ICT operator, the optimal level of investment in security is the level providing a protection that minimizes its expected costs in case of critical events. This optimal solution occurs when marginal security investments equal the expected marginal costs that the operator would sustain. Nevertheless, market failures may impede the pursuit of the optimal level of investments and the consequent optimal level of security (Bruck et al., 2006,).

Gordon and Loeb (2002) defined a model to determine the optimal amount of investment needed to protect a given set of information. Considering the vulnerability of an information system, the main finding is a biased behavior on the part of the operator: a firm spends only a small fraction (approximately 37%) of the potential loss that would result in case of a breach occurrence. According to this model, the level of security investment of the ICT operator can be defined on the basis of the expected loss $E(L)$ associated with its available information set, with L representing the incurred loss in case of failure. The expected loss $E(L)$ is the result of the probability of the threat occurrence, t, times the vulnerability of the system, v (which is the probability of threat effectiveness), and the potential loss due to the threat realization, λ. In order to avoid huge unexpected losses, the ICT operator sets up a level of security S as a function of the implemented security investments I_s and of the level of vulnerability of the system v.

The ICT operator chooses the level of security investment according to his risk attitude and his risk assessment. In fact, the level of chosen investment depends on the operator's risk propensity: if the operator is risk adverse, he would prefer a lower level of expected loss

increasing current costs; otherwise, if the ICT operator is risk loving, he would accept a high risk situation increasing of current benefits (e.g. reduced security costs).

In the real world, complete information on potential failures and related risk is not available to ICT operators, first of all, because malicious attack techniques evolve rapidly and are becoming increasingly sophisticated. In addition, ICT operators suffering failures are reluctant to publicly communicate and report to the authorities any disruption in services, the causes, frequencies and costs. This operator behavior can be ascribed to the concern of suffering reputational damages, breaking confidentiality obligations and being addressed on grounds of liability. Moreover, the particular sensitivity of information on security incidents makes information sharing a particularly risky issue, hindering the development of a confident and fruitful environment[3].

In fact, from the perspective of a single operator, there are no immediate advantages in sharing information on past attacks[4], although all ICT operators and other critical infrastructure community members would gain from better information on failures.

The reluctance to share information about security failures experienced entails a biased knowledge on risk. These circumstances influence the extent of implemented security provisions and the realized security investment: because ICT operators are not properly aware of the real extent of risk, the chosen level of investment is different than that which would be desired by the operator himself.

These assumptions are supported by the results of a leading study on information sharing by Gal-Or and Ghose (2004). The analysis made in the article *"The Economic Consequences of Sharing Security Information"* investigates the competitive implications of information sharing on breaches and the level of investment dedicated to security. The main conclusion is that market characteristics affect incentives for information sharing among competing firms, but information sharing encourages additional security investments.

4.6 Areas of applicability

The strategic role of ICT services in the current European economies is increasing the policy makers' interest on security issues and towards possible measures to reduce related market failures.

---

[3] Information sharing, characterized by restricted disclosure of sensitive information, could be misinterpreted by an enforcement agency or used to hide the flow of information for anticompetitive purposes.

For a general overview of the antitrust issue in information sharing, among the main reference works there are *"Information Exchanges Among Firms and their Impact on Competition"* by Kühn and Vives, *"Overcoming impediments to information sharing"* by Aviram and Tor and *"Information sharing, innovation, Antitrust"* by Teece.

[4] *In the perspective of the operator, the immediate advantages of sharing information may be not enough to overcome the potential risk of reputation loss coming from breaches or improper disclosure.*

One of the possible regulation solutions is suggested by Garcia and Horowitz (2007) in "The potential for underinvestment in internet security: implications for regulatory policy", where incentives and obstacles to security provisions in the Internet market are investigated. Their model confirms the security underinvestment (from a social perspective) by Internet providers: the social value derived from Internet largely exceeds potential and actual revenues associated with the telecommunication companies. Garcia and Horowitz sustain appropriate, at least in the long term, the implementation of regulatory instruments focusing on a standardized security risk analysis for Internet companies even if there are difficulties due to the inability to measure the current level of security, the evolution of malicious attackers' tools, the implementation of homogeneous security tools, the capacity of ranking security risks and the different organisations' financial readiness and technological profile to support security of the internet infrastructure.

All the regulatory initiatives against security issues of information systems and especially those related to malicious attacks undertaken at the European level are focused on the critical role of information on crime and on the network nature of information systems and its consequence on security (COM (2009) 149 final). Most of the proposed measures aim to increase the social awareness of security failure effects and to reduce the biased optimal choice behaviour of ICT operators, targeting with policy indications also the other actor categories as stakeholders able to impact directly on the security provisions.

In order to improve security, an economic incentive framework can be set up by policy makers for:

- Sharing technical information through a bottom-up approach essentially involving ICT operators and other critical infrastructure operators to better assess the security risk at the organization level. Information sharing circles may represent one of the most efficient tools to solve limitations related to the lack of information and data on security for the ICT operators and partially for other critical infrastructure operators. At the organization level, the improvement of security related information allows a better assessment of the risk of disruptions and supports more effective investment choices both to improve preparedness and to respond to emergencies. The exchange of information may increase security awareness of ICT circles' members and result in benefits for individual stakeholders and for the network security of the society as a whole.
- Sharing technical information through a top-down approach essentially involving ICT operators and public authorities/bodies to set up measures to prevent security failures and to better assess risk at the social level. One solution is the implementation of homogenous practices for disruption reporting, allowing competent authorities to have a complete overview of the emerging threats and related vulnerabilities and to collect significant data for the social risk evaluation. Key-element for overcoming lack of information at European level is therefore a common strategy for collecting detailed data and widening reliable sources (e.g. main ICT stakeholders).
  Spreading information on the security threats and impacts, increasing the knowledge for each category of ICT stakeholder (ICT operators, other critical infrastructure operators,

public authorities/bodies and citizens). Due to the network features of ICT systems and the presence of the weakest link, the development of baseline security technological skills for the largest part of the population may improve the overall security of the ICT systems and those strictly connected. Filling the gap in terms of technological skills with the aim of increasing security would mean setting up different education measures for citizens according to their potential user role: home user, ICT professional and worker.

4.7 List of bibliographic references

- Abel A.B., Eberly J.C., 1999, "The impact of uncertainty on capital accumulation", Journal of monetary economics, Vol. 44, pp. 330-377
- Alcatel-Lucent's Bell Labs and professional services, 2007, "Availability and Robustness of Electronic Communication Infrastructures - ARECI", Final Report of the ARECI project supported by DG Information Society and Media of the European Commission
- Anderson R., 2001, "Why Information Security is Hard – An Economic Perspective", Proceedings of the 17th annual Computer Security Application Conference
- Anderson R., Moore T., 2006, "The Economics of Information Security" Science Vol. 314 no. 5799 pp. 610-613
- Aviram A., Tor A., 2004, "Overcoming impediments to information sharing" Harvard Law school discussion paper, Alabama Law Review Vol. 55
- Bisogni F., Cavallini S., Bellotti, F., Tancioni M., Remotti, L. A., Wright A. C., Gasperini G., Anselmucci S., 2009, "The Vulnerability of Information Systems and its inter-sectoral, Economic and Social Impacts – VIS", Final Report of the VIS project supported by DG Justice, Freedom and Security of the European Commission, September 2009
- Bisogni F., Cavallini S., Di Trocchio S., 2011, "Cybersecurity at European level: The Role of Information Availability", in "The Economics of Cybersecurity", First quarter 2001, No. 81, edited by Communications & Strategies, March 2011
- Borg S., 2009, "The Economics of Loss" in Enterprise Information Security and Privacy, edited by C. Warren Axelrod, Jennifer L. Bayuk & Dainel Schutzer (2009)
- Brück T., Karaisi M., Schneider F., 2008, "A survey of the economics of security", NEAT Economics of Security working paper 1
- Caballero R. J., 1991, "On the sign of the investment-uncertainty relationship", American Economic Review, Vol. 81, No. 1, pp. 279-288
- Cambacédès L. P., Chaudet c., 2010, "The SEMA Referential Framework: Avoiding Ambiguities in Security and Safety Issues", presentation at the Fourth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Fort McNair, Washington, DC, USA, March 14 - 17, 2010
- Cavallini S., Di Trocchio S., Bisogni F., Tancioni M., Trucco P. C., 2010, "Study for the Development of a Methodology and Research of Quantitative Data on the Economics of Security and Resilience in Critical Communications and Information Infrastructures – CIIS – SMART-SEC", Final Report of the SMART-SEC project supported by DG Information Society and Media of the European Commission
- Choi J.P., Fershtman C., Gandal N., 2004, "Internet Security, Vulnerability Disclosure, and Software Provision", Fourth Workshop on the Economics of Information Security, Harvard University, Cambridge
- COM (2001) 298. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Region. "Network and Information Security: Proposal for a European policy approach"
- COM (2006) 251. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Region. "A Strategy for a secure information society - Dialogue, partnership and empowerment"
- COM (2009) 149 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information

Infrastructure Protection – "Protecting Europe from large Scale Cyber-Attacks and Disruption: Enhancing Preparedness, Security and Resilience".

- COM (2010) 245. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. "A digital agenda for Europe".
- COM (2010) 250 final. Proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration
- COM (2010) 251 final. Proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)
- Directive 2002/21/EC of of 7 March 2002 "On a common regulatory framework for electronic communications networks and services" (Framework Directive)
- Directive 2008/114/EC of 8 December 2008 "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection"
- Dixit A.K., Pindyck R. S., 1994, "Investment under Uncertainty" Princeton University Press
- ENISA, 2007a, "EISAS – European Information Sharing and Alert System. A Feasibility Study 2006/2007", ENISA Report
- ENISA, 2007b, "Examining the feasibility of a data collection framework", ENISA Report
- ENISA, 2009a, "Good Practice Guide for Information Sharing", ENISA Report
- ENISA, 2009b, "Good Practice Guide Network Security Information Exchanges", ENISA Report
- ENISA, 2009c, "Good Practices for Reporting Security Incidents", ENISA Report
- ENISA, 2009d, "The growing requirement for information security awareness", ENISA Report
- ENISA, 2010, "Incentives and Challenges for Information Sharing in the Context of Network and Information Security", ENISA Report
- ENISA, 2011, "Inventory of CERT activities in Europe Publicly listed teams, co-operation, support and standardisation activities", ENISA Report
- Gal-Or E., Ghose A., 2004, "The Economic Consequences of Sharing Security Information" Advances in Information Security, Vol 12
- Garcia A., Horowitz B., 2007 "The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy" Journal of Regulatory Economics, Vol. 31
- Gordon L.A., Loeb M.P., 2002, "The Economics of Information Security Investment" Advances in information security, Vol 12
- Hausken K., 2006, "Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability", Information systems frontiers Vol. 8, N. 5, pp 338-349
- Kannan K., Telang R., 2005, "Market for Software Vulnerabilities? Think Again" Management Science, Vol.51, N.5, pp. 726-740
- Kolfal B, Patterson R., Yeo M. L., 2010 "Market impact on it security spending", Workshop on the Economics of Information Security, Arlington, USA
- Kühn K. U., Vives X., 1995, "Information Exchanges Among Firms and their Impact on Competition", Institut d'Anàlisi Econòmica (CSIC)
- Liu D., Ji Y., Mookerjee V. M,. 2005, "Information Security Investment with Different Information Types: A Two-Firm Analysis", AMCIS 2005 Proceedings
- Markusen A.R., 2003, "The Case Against Privatizing National Security" Governance, An International Journal of Policy, Administration and Institutions, Vol. 16, Issue 4, pp. 471–501
- Schneider F., Brück T., Meierrieks D., 2011, "The Economics of Terrorism and Counter-Terrorism: A Survey (Part I), EUSECON Economics of Security working paper 44
- Schneider F., Brück T., Meierrieks D., 2011, "The Economics of Terrorism and Counter-Terrorism: A Survey (Part II), EUSECON Economics of Security working paper 45
- Teece D., 2003, "Information sharing, innovation, Antitrust" in Essay in technology management and policy Published by World Scientific
- Varian H.R., 2004, "System Reliability and Free Riding" in Economics of Information Security. Springer.

Willemson J., 2006, “On the Gordon & Loeb Model for Information Security Investment” Workshop on the Economics of Information Security, Cambridge, England

5 Impact Assessment of Intervention Policies:

Starting from the evaluation of socio-economic impacts due to security and resilience failures

By Simona Cavallini and Fabio Bisogni (Fondazione FORMIT, via Giovanni Gemelli Careri 11, 00147 Rome, Italy, s.cavallini/f.bisogni@formit.org)

5.1 Abstract

This paper aims at summarizing the main elements to be considered for the impact assessment of intervention policies in security and resilience related topics. In particular, it is pointing out how the need of impact assessment policies relies on the evaluation of macro-level effects due to security and resilience failures. Policy effectiveness in the NIS context should be evaluated having a clear perception of the potential effects of failures in security and resilience such as those affecting critical infrastructures. Among the different strands of literature investigating impacts of security and resilience failures and according the most recent European policy debate, evaluation of socio-economic damages due to disruptions of critical infrastructures, also taking into account their interdependencies and cascading effects, has become one of the main goals of the related research activities. Indications on severity of events affecting the entire society through its critical infrastructures may support impact assessment of policies devoted to improve protection and to increase security and resilience at macro level.

5.2 Keywords

Critical infrastructures, sectoral interdependencies, socio-economic effects, input-output models, security and resilience intervention policies.

5.3 Involved Stakeholders

Adoption of new security and policies aims at improving protection conditions of all the actors of the society. Assessment of intervention policies in terms of improves security and resilience at societal level should consider the effect that specific measures may have in terms of costs and benefits of each actor type in interested society. In particular, among the different stakeholder types, the most involved both in the case of failures due to critical events and in the case of policy interventions are:

- Citizens, intended as general private end-users. In the case of a critical event they would suffer socio-economic impacts that may be reduced by effective policy measures. Apart from actions devoted to raise security awareness, they are not usually the main target of policies.
- Public bodies and authorities (including decision makers at national and at European level) have the main goal to protect the social interest and can directly support prevention, protection and reaction to security and resilience disruptions. They have the direct role of setting up policies, defining targets (such as stakeholder types),

assessing effectiveness of policies along time, and, if necessary, revising/enforcing them. They are in charge of evaluating social costs and benefits of each implemented or planned measure.

- Private economic operators. Operators providing essential goods and services are usually the direct target of security and resilience policies. They are also the actors that mainly bear the direct cost of security and resilience provisions (mandatory or not) and that are request to invest in order to reduce socio-economic effects in case of critical events. This role is particularly strategic for those operators owning/managing critical infrastructures.
- Academic researchers have a threefold role: to assess potential and real socio-economic effects of disruptions; to suggest effective indications (e.g. incentives) to minimize costs and maximizing social benefits of security and resilience measures; support decision markers in impact assessment of intervention policies.

5.4 Approach to the impact assessment of intervention policies

Intervention policies related to security and resilience may be classified at least in 6 different categories[5] of initiatives (European Commission, 2009a):

1. Non-legislative initiatives/Communications/Recommendations/White papers which set out commitments for future legislative actions
2. 'Cross-cutting' legislative action, such as regulations and directives that address broad issues and are likely to have significant impacts in at least two of the three pillars (economic, environmental and social) and on a wide range of stakeholders across different sectors
3. 'Narrow' legislative action in a particular field or sector, and unlikely to have significant impacts beyond the immediate policy area
4. Expenditure programmes: decisions to establish or renew spending programmes
5. Commitology decisions: different executive initiatives defined by the procedure of adoption

The *Impact assessment guidelines* of the European Commission propose a procedure for the impact assessment of policies according to the following key analytical steps (European Commission 2009a, pag .5):

1. ***Identifying the problem***
    - *Describe the nature and extent of the problem.*
    - *Identify the key players/affected populations.*
    - *Establish the drivers and underlying causes.*
    - *Is the problem in the Union's remit to act? Does it pass the necessity and value added test?*

[5] *Each impact assessment process is more affected by the content of the initiative rather than any formal classification.*

- *Develop a clear baseline scenario, including, where necessary, sensitivity analysis and risk assessment.*

2. ***Define the objectives***
   - *Set objectives that correspond to the problem and its root causes.*
   - *Establish objectives at a number of levels, going from general to specific/operational.*
   - *Ensure that the objectives are coherent with existing EU policies and strategies, such as the Lisbon and Sustainable Development Strategies, respect for Fundamental Rights as well as the Commission's main priorities and proposals.*
3. ***Develop main policy options***
   - *Identify policy options, where appropriate distinguishing between options for content and options for delivery mechanisms (regulatory/non-regulatory approaches).*
   - *Check the proportionality principle.*
   - *Begin to narrow the range through screening for technical and other constraints, and measuring against criteria of effectiveness, efficiency and coherence.*
   - *Draw-up a shortlist of potentially valid options for further analysis.*
4. ***Analyse the impacts of the options***
   - *Identify (direct and indirect) economic, social and environmental impacts and how they occur (causality).*
   - *Identify who is affected (including those outside the EU) and in what way.*
   - *Assess the impacts against the baseline in qualitative, quantitative and monetary terms. If quantification is not possible explain why.*
   - *Identify and assess administrative burden/simplification benefits (or provide a justification if this is not done).*
   - *Consider the risks and uncertainties in the policy choices, including obstacles to transposition/compliance.*
5. ***Compare the options***
   - *Weigh-up the positive and negative impacts for each option on the basis of criteria clearly linked to the objectives.*
   - *Where feasible, display aggregated and disaggregated results.*
   - *Present comparisons between options by categories of impacts or affected stakeholder.*
   - *Identify, where possible and appropriate, a preferred option.*
6. ***Outline policy monitoring and evaluation***
   - *Identify core progress indicators for the key objectives of the possible intervention.*
   - *Provide a broad outline of possible monitoring and evaluation arrangements.*

Concerning the analysis of the impacts of the policy, significance is recommended to be evaluated at least in the economic, social and environmental fields affecting elements such as economic actors, groups of citizens, SMEs, cultural goods.

In particular, within the *Impact assessment guidelines* the analysis of impacts consists of three major steps:

1. Identification of economic, social and environmental impacts
2. Qualitative assessment of the more significant impacts
3. In-depth qualitative and quantitative analysis of the most significant impacts

The suggested assessment of impacts implies the identification of the areas in which the proposed action is intended to produce benefits, as well as the areas where this may lead to direct costs or unintended negative impacts assign likelihoods (e.g. low, medium or high probability) that the impact will occur (or conversely the risk that the impact will not occur). Assumptions about factors that may influence the probability that impacts will occur should complete the evaluation.

5.5 Summary of existing work

In the specific context policies related to security and resilience, the worldwide current policy debate is strongly focused on protection of critical infrastructures. Framework policies at the European level and intervention strategies at the national level aim at securing society towards physical and cyber threats.

The complex structure of socio-economic relationships has imposed special attention to interdependencies among infrastructures leading decision makers:

- To focus on wide-scope security measures such as with the identification of European Critical Infrastructures with the Directive “On the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection”, 2008/114/EC (European Commission, 2008a)
- To identify and study elements amplifying potential effects of security failures such as ICT systems embedded in all the socio-economic function with Communication for “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”, COM (2009) 149 final (European Commission, 2009b)

The evaluation of the security and resilience related policies relies on an assessment of socio-economic impact due to extended failures that may affect the entire society. Adoption of security and resilience measures implies costs that should be compared with tangible and intangible benefits of their implementation. For instance, comparisons of effects between scenarios with and without policy measures represent the starting point for the evaluation of the impact of intervention policies. In such evaluations critical point is usually the quantification of benefits. In the field of security, the framework is furthermore complex. Apart from intangible benefits of a security policy such as the “security feeling” of citizens, tangible advantages for the society should be evaluated in terms of reduced impacts in case of critical events.

Critical infrastructures intended as assets, operators or delivered services are considered a key element in security and resilience related policies for their potential disruptive effects on the overall society. Apart from the essential service of the critical infrastructure itself, its interconnections with other critical infrastructures add a multiplier effect to the expected socio-economic loss.

Needs to assess socio-economic effects of disruption of critical infrastructures can be found in the policy regulations themselves.

The Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection (European Commission, 2008a) defines critical infrastructure as *"an asset, system or part thereof … which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.",* while indications of effects of failures are detailed in the related Guidelines for its application (European Commission, 2008b) *"Cross-cutting criteria consist of three families of criteria, namely casualties criteria, economic effects criteria and public effects criteria… economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects). The starting point for the assessment is that a loss of service will lead to a loss of production of services and goods. This loss and its effect incurred in the supply chain constitute the total size and extent of economic damage."*

Referring to possible assessment methods with macro perspective, *Guidelines of the Directive* (European Commission, 2008b) suggests as *"A suitable calculation method is input-output analysis. This method has the advantages that it automatically excludes private losses, includes cascading economic effects, and uses current data. In short, an input-output model is a description of the dependencies that exist within an economy amongst all its sectors of activities. An input-output model explains, for example, how the output of the oil and gas sector is used within other sectors such as, industry, agriculture, etc. What is important to note is that there is a direct link between the input-output table and the national accounts. This makes it possible to express the consequences of a disruption in one sector and its rippling effect to the rest of the economy and eventually on the GDP. The required data for building input-output models is available from Eurostat."*

In recent years large part of literature on potential effects of critical infrastructures in case of security and resilience failures at macro level relies on input-output modelling. Industrial relationships expressed through the input-output tables reporting the production and the consumption behaviour of each sector of a specific economic system were initially considered in the seminal contribution of Haimes and Jiang (2001).

Rinaldi (2004) considers input-output models of economic flows described by Leontief (1986) applicable to infrastructure studies, where, in general, economic sectors represent infrastructures and economic sectors which output serves extensively and intensively all the

other sectors, in particular, represent critical infrastructures. As described in Sarriegi et al. (2009), input-output models are one of the most effective modelling paradigms to face the CIs interdependencies problem allowing a more extensive comprehension on which economic sectors might be considered the most vulnerable to CIs breakdowns.

Haimes et al. (2007) lists among the 4 potential couplings models for describing CIs interdependencies those developed for including inter-sector economic features on the basis of input-output relationships. The Inoperability Input-Output Model (IIM), developed by Haimes and Jiang (2001), Santos, J. R., Haimes, Y. Y., (2004), is a transformation of the Leontief static input-output model in which, after a shock, the IIM estimates the effects in terms of sector inoperability and the economic impact.

In order to solve to time-invariant problem of the IIM, Lian and Haimes (2006) proposed the Dynamic Input-Output Inoperability Model (DIIM) as an extension of the IIM able to include the time dimension for the recovery of sectors after a critical event. Although the DIIM is more general than the IIM, it still does not appropriately include the domino effects of disruptions occurring in interdependent economic sectors.

An attempt to address the above identified IIM and DIIM issues is proposed by Kujawski (2006) with the Multi-Period Model for Disruptive Events in Interdependent Systems (MPMDEIS). The premise of the MPMDEIS is that a critical event impacts on the economic system according to a 4-phase life-cycle starting from a pre-event period, to a post-recovery period. In MPMDEIS a critical event is modeled as a shock which, through the sectoral interdependencies, perturbs the equilibrium, cascades from one sector to another and reduces their production capacity. The systems dynamics approach for modeling the recovery period constitutes the key element.

In Bisogni and Cavallini (2010), the input-out relationships are employed to assess the most vulnerable sectors to unexpected critical Information System (IS) sector failures. The model simulates IS disruptions and provides estimates of socio-economic impacts for all the sectors at both national and European level, taking into account in a dynamic framework of sectoral interdependencies and cascading effects. Differently from the above mentioned literature, the proposed approach is a computational general equilibrium (CGE) model characterized by a supply side and a demand side that define the equilibrium condition that an sector failure perturbs, making possible the comparison of rankings of damages at sectoral level.

The policy indications and the evolving different strands of literature on failures in critical infrastructures highlight the need of a macro-level assessment of potential socio-economic effects of unexpected events affecting security and resilience. Extent of impacts affects the urgency of the policies and allows evaluating their effectiveness in reducing potential damages.

5.6 Areas of applicability

Impact assessment of intervention policies and evaluation of socio-economic impacts due to security and resilience failures can be performed at any operational and geographical level.

Socio-economic impacts due to security and resilience failures may be assessed also at operator level. A lot of papers and recent European studies are focusing in investigating from different perspectives relationships among single operators and/or specific sectors, while impact assessment of intervention policies may be intended as analysis of strategies of security and resilience of operators (including business continuity).

Effects of security failures and resilience may be obviously also analysed at any geographical level implying an involvement of different decision makers for implementing and evaluating policy effectiveness.

5.7 Open issues

According to the analysis carried out in the previous paragraphs, the following topics should be included in the open issues:

- Definition of methodologies able to make comparable assessment (at macro level) of socio-economic impacts due to security and resilience failures
- Refinement and harmonization of indicators for assessing socio-economic effects of security and resilience failures (e.g. loss of turnover)
- Identification of categories of benefits related security provisions for all the different types of actors

Among the new sub-topics to be further investigated:

- Specific methodologies and tools for impact assessment of security and resilience related policies (including definition data and information to collect and use)
- Ex-post evaluation of effects of current security policies in the medium term also according to the specific sources of threats

5.8 List of bibliographic references

- 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
- Bisogni F., Cavallini S., Bellotti, F., Tancioni M., Remotti, L. A., Wright A. C., Gasperini G., Anselmucci S., (2009), “The Vulnerability of Information Systems and its inter-sectoral, Economic and Social Impacts – VIS”, Final Report of the VIS project supported by DG Justice, Freedom and Security of the European Commission, September 2009
- Bisogni F., Cavallini S., Di Trocchio S., (2011), “Cybersecurity at European level: The Role of Information Availability”, in “The Economics of Cybersecurity”, First quarter 2001, No. 81, edited by Communications & Strategies, March 2011
- Cavallini S., Di Trocchio S., Bisogni F., Tancioni M., Trucco P. C., (2010), “Study for the Development of a Methodology and Research of Quantitative Data on the Economics of Security and Resilience in Critical Communications and Information Infrastructures – CIIS – SMART-SEC”, Final Report of the SMART-SEC project supported by DG Information Society and Media of the European Commission
- European Commission (2009a), “Impact assessment guidelines”, 15 January 2009, http://ec.europa.eu/governance/impact/commission_guidelines/docs/iag_2009_en.pdf
- European Commission, (2005), “i2010: A European Information Society for Growth and Employment”, communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM (2005) 229 Final

- European Commission, (2008a), “Non-Binding Guidelines for application of the Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection”
- European Commission, (2008b), “On the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection”, Council Directive 2008/114/EC
- European Commission, (2009b), “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”, Communication from the Commission to European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions on Critical Information Infrastructure Protection, COM (2009) 149 final
- European Programme for Critical Infrastructure Protection (EPCIP) Programme - http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm
- Haimes, Y., Jiang, P., (2001), “Leontief-based model of risk in complex interconnected infrastructures” Journal of Infrastructure Systems, Vol. 7, No. 1, March 2001, pp. 1-12.
- Haimes, Y., Santos, J., Crowther, K., Henry, M.., Lian, C., Yan, Z., (2007),“Risk Analysis in Interdependent Infrastructures” in “Critical Infrastructure Protection”, IFIP International Federation for Information Processing, Publisher Springer Boston, pp. 297-310
- Kujawski, E., (2006) “Multi-period model for disruptive events in interdependent systems”, Systems Engineering, vol. 9, n. 4, pp. 281-295
- Leontief, W.W. (1986), “Input-Output Economics”, 2nd ed., New York: Oxford University Press
- Lian, C., Haimes, Y. Y. (2006), “Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input-output model”, Systems Engineering, Vol. 9 Issue 3, pp. 241 - 258
- Luiijf, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M., Cruz, E. (2009), “Empirical Findings on Critical Infrastructure Dependencies in Europe" in “Critical Information Infrastructure Security”, Third International Workshop, CRITIS 2008, Rome, October 13-15, 2008, Springer Berlin – Heidelberg 2009, pp. 302-310.
- Markusen A.R., 2003, “The Case Against Privatizing National Security” Governance, An International Journal of Policy, Administration and Institutions, Vol. 16, Issue 4, pp. 471–501
- Pederson, P., Dudenhoeffer, D., Hartley, S., Permann, M., (2006), “Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research”, Idaho National Laboratory, August 2006
- Prevention Preparedness and Consequence Management of Terrorism and other related Risks (CIPS) Programme –http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm
- Rinaldi, S. M., (2004), "Modeling and Simulating Critical Infrastructures and Their Interdependencies", vol. 2, pp.20054a, Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04)
- Rinaldi, S.M., Peerenboom, J., Kelly, T., (2001), “Complexities in identifying, Understanding, and Analyzing Critical Infrastructure Dependencies”, Special issue IEEE Control Systems Magazine on Complex Interactive Networks (December 2001)
- Santos, J. R., Haimes, Y. Y., (2004), “Modeling the Demand Reduction Input-Output (I-O) Inoperability Due to Terrorism of Interconnected Infrastructures”, Risk Analysis, Volume 24, Number 6, December 2004, pp. 1437-1451
- Sarriegi, J. M., Sveen, F. O., Torres, J. M., Gonzalez, J. J., (2009), “Adaptation of Modelling Paradigms to the CIs Interdependencies Problem" in “Critical Information Infrastructure Security”, Third International Workshop, CRITIS 2008, Rome, October 13-15, 2008, Springer Berlin – Heidelberg 2009, pp. 295-301.
- Schneider F., Brück T., Meierrieks D., 2011, “The Economics of Terrorism and Counter-Terrorism: A Survey (Part I), EUSEOCON Economics of Security working paper 44
- Schneider F., Brück T., Meierrieks D., 2011, “The Economics of Terrorism and Counter-Terrorism: A Survey (Part II), EUSEOCON Economics of Security working paper 45

- Statistical Classification of Economic Activities - Concordance tables NACE-ISIC - http://www.fifoost.org/database/nace/nace-en_2002c.php
- Svendsen, N. K., Wolthusen, S. D., (2007), "Connectivity models of interdependency in mixed-type critical infrastructure networks", Volume 12 , Issue 1 (March 2007), pp. 44-55
- Zimmerman, R., Restrepo, C., (2006), "The next step: Quantifying infrastructure interdependencies to improve security", International Journal of Critical Infrastructures 2(2-3), 215–230 (2006)

6 Collection of Data on Security Incidents

By Dr. Thomas Nowey, Krones AG, Neutraubling, Germany

6.1 Abstract of the topic

Precise quantitative data related to information security incidents like 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 multitude of incidents from various organizations and individuals in a standardized way.

Individual organizations, especially SME, 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 organizations. 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 organization is needed. Approaches like Return on Security Investment (ROSI) are based on the assumption that there is sufficient data available to estimate risks and annual loss expectancies correctly.

Research institutions, providers of security solutions, centers of excellence for information security as well as national information sharing systems as well as European institutions need historical data on information security incidents to analyze and understand cyber-threats and cybercrime, to be able to advise individuals and organizations on risks and countermeasures and to develop and validate economic models and simulations. Furthermore accurate loss data is one of the essential prerequisites for cyber insurance.

Yet in practice all of the stakeholders mentioned are lacking reliable data. This can mainly be attributed to the absence of a common standard for the collection of risk-related information on security incidents and to the nonexistence of an inter-organizational initiative and technical platform for secure and anonymous collection of such data. Like in 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) could be a valuable source for better risk management decisions and thus for increased profitability, competitive advantage as well as for more precise accurate insights in the nature of cyber-attacks. Such a data pool or platform using a common language for security incidents is not yet available today.

However key requirements of such systems have already been identified. In academic research there are also proposed solutions to the restraints identified as well as prototype implementations for such initiatives. The main barrier nowadays lies in finding a suitable organization that is capable of establishing a common taxonomy and process for the collection of incident data, that can establish a anonymity preserving technical platform, that

is trusted by the contributors, that is capable of being a technical and organizational mediator, and that has the necessary funding to establish and run a pan-European platform for the collection of incident information. The expansion of a European Information Sharing and Alert System could be a feasible solution.

6.2 Keywords

Annual Loss Expectancy. Asset. Benchmarking. Business Risk. Cyber Insurance. Damage Assessment. Event. Exposure. Financial Impact. High Risk Areas. Impact Analysis. Incident. Incident Categorisation. Information Security. Key Performance Indicator. Likelihood. Loss. Loss Database. Operational Risk. Probability. Quantification. Risk. Quantitative Assessment. Risk Assessment/Analysis. Risk Controls. Risk Management. Security. Threat. Vulnerability.

6.3 Summary of existing work

There is a significant amount of work on different aspects of this topic:

- Initiatives for the collection of incident related information like computer emergency response teams (CERTs) or information sharing and analysis centers. However there is no initiative focusing on the assessment of quantitative data. Different papers outline the positive economic impact of sharing security-related information between organizations [9], [10], [12].
- Data pools on risks are common in other areas like banking or insurance. Yet those data pools do not consider information security incidents.
- Several substantiated taxonomies for the classification of security incidents exist, as well as common standards like CVE for uniquely identifying vulnerabilities, etc. For an overview see [15].
- Research on the secure and anonymity preserving benchmarking between organizations [13].
- Methods for economic analysis of information security investments and risks like ROSI [7], [18].
- Micro-economic models on information security risks [17].
- Studies/Surveys on Cybercrime. Yet those studies are hardly comparable, the loss figures vary considerably (up to a factor of 1.000) due to different methods, definitions and taxonomies [8].
- Transferring risks to third parties by means of insurance is common for various types of risks. Requirements and economic models for cyber insurance have been analysed [4], [11], [20]. Yet today there is no efficient market for cyber insurance. The lack of

actuarial data is one of the major drawbacks for the development of a market for cyber insurance products.

- Nowey describes key issues that have to be addressed to make a platform for the sharing of incident information possible along with proposed solutions [15], [16]. The most important aspects being:
  - anonymity,
  - security,
  - common taxonomy,
  - mechanisms for fair use,
  - and demand oriented data preparation.
- 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.
- Research on electronic crime. For example Anderson et al. recommend "that the Commission (or the European Central Bank) regulate to ensure the publication of robust loss statistics for electronic crime." [2].
- Research on the so called wisdom of the crowd (as described by Don Tapscott) shows the added value that is generated by exchanging information between different parties [19].
- RISI – The Repository of Security Incidents: http://www.securityincidents.org. Commercial System focusing on industrial security incidents. No quantitative data recorded.
- Event studies that analyse the impact of security incidents on firm value [8].

6.4 Areas of applicability of the topic

Data on information security incidents can be applied for various purposes. Among them:

- Improved information security management and risk management in organizations through substantiated quantitative data for risk assessments.
- Benchmarking between organizations.
- Development of cyber insurance products.
- Verifying the utility of risk reduction measures.
- Studies on cybercrime.
- Assessing macroeconomic impact of security breaches, cybercrime, etc.

- Development, application and verification of economic models and simulation models on economic aspects of information security. Empirical validation of theoretical models.
- Comparing and analysing the real severeness of pan-European security incidents (e.g. Stuxnet virus, etc.). Assessing the real economic impact of security breaches on national economy.
- Fostering information exchange between stakeholders (e.g. European institutions, national authorities, Professional associations, research institutions, companies, service providers, vendors of security products, individuals) on threats, vulnerabilities, incidents and countermeasures.

6.5 Links to ENISA-Goals

The Digital Agenda for Europe – 2.3 Trust and Security:
"Establish a European cybercrime platform by 2012;"
"Establish by 2012 a well-functioning network of CERTs at national level covering all of Europe;"

CIIP - Implementation activities – Pillar 2:
European Information Sharing and Alert System (EISAS)
"Action: Detection and response development and deployment of a European Information Sharing and Alert System, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems."

The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM (2010) 673 final
"OBJECTIVE 3: Raise levels of security for citizens and businesses in cyberspace"

Draft Internal Security Strategy for the European Union: "Towards a European Security Model" "Information exchange"

6.6 Involved Stakeholders

- **Commercial and non-profit organizations (like European institutions), companies, especially SMEs:** Collecting and providing incident data, consuming data, analysis and recommendations based on the data. Professional Associations can provide analysis for their members.
- **Research Institutions/Academia:** Proposing methods for collecting and analysing the data, developing new economic models and using data to empirically validate models.
- **European institutions, National Security Institutions, CERTs, ISAS, PPPs:** Setting standards for the collection of incident data, establishing and promoting taxonomy,

acting as a mediator in the development process, providing/running a platform for the collection of incident data, providing analysis and recommendations, extending existing ISAS, providing regulation, guaranteeing privacy and security of the information exchange, advising organizations, helping organizations in implementing, analysing change in overall risk profile, Assessing macroeconomic impact of security breaches, cybercrime, etc.

- **Security Industry:** provide funding, gaining insights into attack patterns, develop optimized security products, implementing standards and technical interfaces for the collection of security in security management products.
- **Security professionals:** Providing input for a common taxonomy on incident data.
- **Sector Regulators:** Possibly setting of rules for the obligation of disclosing security incidents to certain institutions.

6.7 Open issues regarding the topic

1. Establishing and promoting a common taxonomy for documentation of information security incidents and their impact together with a methodology for the collection of information on security incidents. Helping organizations in establishing the necessary processes and analysis capabilities. Providing a taxonomy for IT-assets (and their value), security measures and risk measures.
2. Building a data pool with quantitative data on information security incidents from organizations for the privacy preserving pan-European exchange and analysis of impact data. Providing technical and organizational means for a centralized collection of information on security incidents in private and public organizations.
    a. Technical entity – data pool
    b. Legal entity – custodian for the data
3. Integration of existing data sources into a common framework. E.g. information from studies, data pools, information sharing initiatives, CERTs, etc.
4. Integrating capabilities for the quantitative assessment of information security incidents in information security management products (e.g. issue-tracking-systems).
5. Establishing an anonymity preserving benchmarking initiative for information on security incidents and their impact.
6. Improvement of economic models for cyber insurance based on historic loss data.

6.8 List of bibliographic references

[1] Ross Anderson: Why Information Security is Hard - An Economic Perspective. In: ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference, 358–365. IEEE Computer Society, 2001.

[2] Ross Anderson, Rainer Böhme, Richard Clayton, Tyler Moore: Security Economics and the Internal Market. European Network and Information Security Agency, 2008. http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport

[3] Rainer Böhme and Thomas Nowey: Economic Security Metrics. Dependability Metrics, Lecture Notes in Computer Science, Vol. 4909, Springer, Berlin 2008, 182-193. http://www1.inf.tu-dresden.de/~rb21/publications/BN2008_Economic_Security_Metrics.pdf

[4] Rainer Böhme: Cyber-Insurance Revisited. Proc. of Workshop on the Economics of Information Security (WEIS), Kennedy School of Government, Harvard University, 2005

[5] Carsten Casper. Examining the Feasibility of a Data Collection Framework. European Network and Information Security Agency, 2007.

[6] ENISA: EISAS – European Information Sharing and Alert System for citizens and SMEs - A Roadmap for further development and deployment. European Network and Information Security Agency, 2011

[7] Ulrich Faisst, Oliver Prokein and Nico Wegmann: Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. Zeitschrift für Betriebswirtschaft, 77(5), 511–538, 2007.

[8] Ashish Garg, Jeffrey Curtis and Hilary Halper: Quantifying the Financial Impact of IT Security Breaches. Information Management & Computer Security, 11(2), 74–83, 2003.

[9] Esther Gal-Or und Anindya Ghose. The Economic Incentives for Sharing Security Information. Information Systems Research, 16(2), 186–208, 2005.

[10] Lawrence A. Gordon, Martin P. Loeb and William Lucyshyn: Sharing Information on Computer Systems Security: An Economic Analysis. Journal of Accounting and Public Policy, 22(6), 461–485, 2003.

[11] Torsten Grzebiela: Internet-Risiken. Versicherbarkeit und Alternativer Risikotransfer. Gabler Edition Wissenschaft. Markt- und Unternehmensentwicklung. Deutscher Universitäts-Verlag, 2002.

[12] Kjell Hausken: Information Sharing among Firms and Cyber Attacks. Journal of Accounting and Public Policy, 26, 639–688, 2007.

[13] Dominik Herrmann, Florian Scheuer, Philipp Feustel, Thomas Nowey and Hannes Federrath: A Privacy-Preserving Platform for User-Centric Quantitative Benchmarking. Trust, privacy and security in digital business: 6th international conference, TrustBus 2009, Linz, Austria, September 3 - 4, 2009; Lecture Notes in Computer Science, Vol. 5695, Springer, Berlin, Heidelberg 2009, 32-41. http://www.springerlink.com/content/41h381k7487w7472/fulltext.pdf

[14] Ruperto P. Majuca, William Yurcik, and Jay P. Kesan: The Evolution of Cyberinsurance. In ACM Computing Research Repository (CoRR). CR/0601020, 2006.

[15] Thomas Nowey: Konzeption eines Systems zur überbetrieblichen Sammlung und Nutzung von quantitativen Daten über Informationssicherheitsvorfälle. Vieweg+Teubner, 2010.

[16] Thomas Nowey, Hannes Federrath: Collection of Quantitative Data on Security Incidents. The Second International Conference on Availability, Reliability and Security (ARES 2007), Wien, 10. - 13. April 2007. http://www-sec.uni-regensburg.de/publ/2007/NoFe2007ARESQuantitativeData.pdf

[17] Stuart Schechter und Michael Smith: How Much Security is Enough to Stop a Thief? The Economics of Outsider Theft via Computer Systems and Networks. In: Financial Cryptography, 122–137. Springer, 2003.

[18] Kevin J. Soo Hoo: How Much Is Enough? A Risk-Management Approach to Computer Security. Consortium for Research on Information Security and Policy (CRISP), 2000. http://iis-db.stanford.edu/pubs/11900/soohoo.pdf

[19] Don Tapscott and Anthony D. Williams: Macrowikinomics. Portfolio Hardcover, 2010

[20] William Yurcik, David Voss: Cyber Insurance: A Market Solution to Internet Security Market Failure, 1st Workshop on Economics and Information Security, University of California - Berkeley USA, 2002.

7 Software Liability

By Prof. Dr. Rainer BÖHME, Westfälische Wilhelms-Universität Münster, Germany - Dr. Michael RATH, Luther Rechtsanwaltsgesellschaft mbH, Köln, Germany - Ralf SCHNEIDER, TÜV Informationstechnik GmbH, Essen, Germany - Prof. Rahul TELANG, Carnegie Mellon University, Pittsburgh, PA, USA

7.1 Executive Summary

This report gives an overview of economic aspects of liability related to the use of software either for governmental, business or private purposes, in case of a damage caused by a security breach which presumably has its origin in the software itself. Therefore, the focus of this report is not to evaluate the impacts of faults and errors contained in the software leading to contractual or statutory warranty claims, but rather to concentrate on third party liability. Software does not always fall under product liability and there is little specific case law. Almost all cases, if they are brought against the vendors, are solved outside the courts.

Software is immaterial, other than conventional products. 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 be readily predicted. As a result, imperfections of the software cannot be fully foreseen, avoided, or assigned as a reason for malfunction. Additionally, in case of an incident it is difficult to attribute damages to the software and to quantify actual losses. Causation requires potentially remarkable efforts. Software liability in particular can cause significant obstacles to open and free software distribution. And it raises market entry barriers to innovative competitors.

Balancing many stakeholders' interests therefore requires careful policy. We suggest limited liability as an option. Software vendors, then, may have upper and lower liability thresholds. They may have incentives to certify their organisation and products according to recognised and reasonable criteria. Or, they may provide patches to users immediately after vulnerability reporting. A stepwise transition to stricter liability regime could be based on potential harm or criticality of product types. Intermediaries like ISPs are potential other parties subject to a tighter liability regime. Internationally harmonised legislation and regulation of liability might be the main driver for due enforceability.

7.2 Keywords

Software liability, limited liability, free software, economics, information society, economic obstacles, security, incentive-compatible regime, market failure, allocation theory, interdependence, social optimum, externalities, impunity, inhomogeneous legislation, EU internal market, policy options, unpredictability, patching, certification, regulators, software vendors, intermediaries, consumers.

7.3 Status Quo

The software industry has managed to operate in a favourable position. It has established a culture of impunity by disclaiming all liability for losses generated from software malfunction or failure. This stands in stark contrast to the principle that liability is best assigned to the parties who are in a position to fix problems so that they have incentives to do so. Because software is decisive in the information society this misallocation generates substantial social cost. In other words, the liability regime shapes the quality of software that we get.

To understand how this culture of impunity emerged and is further maintained, it is important to evaluate what distinguishes software from other goods. First, the immaterial nature of software has facilitated to disclaim product liability beyond the narrow scope of warranty for the material part, i.e., the data medium. Second, software systems reach unprecedented complexity. This implies that the behaviour of software cannot readily be determined from scrutinizing its design. Third, many software products are highly interdependent. Interdependence refers to the fact that the behaviour of a software product also depends on the interaction with other software products or input from the user. For example, an application might be secure on one operating system, but fail in combination with another version of the same operating system, another set of drivers loaded at runtime, or a different execution environment, such as a virtual machine. Forth, software has the properties of information goods that can be reproduced at zero marginal cost. In the absence of market frictions, the price of commodity software drops to zero. The existence of free software developed by a community of volunteers and released with open source code is an example for this economic rationale. Comprehensive software liability would raise the marginal cost of software products to the risk premium of potential liability charges. Fifth, software markets exhibit a strong dominance of few vendors. Such market structures limit the bargaining power of users. Even if liability is contractible in principle, vendors of standard software choose take-it-or-leave-it terms disclaiming all liability. Only highly specialized or customized software are exempt from this rule.

Liability can be approached from three major legal theories: Contract, tort and statutory. In most EU member states, statutory provisions will provide the framework for contract and tort. As the name implies, in contract, the seller and buyer conclude a contract and that becomes the basis for dispute resolution in case of software malfunctions. An End User License Agreement (EULA) is part of or constitutes the contract that a software vendor makes a user sign before using the product. In tort, typically either the strict product liability or negligence is used as a basis for a case. In negligence, the plaintiff has to prove duty, breach, causation and damage. In strict product liability cases, the need to prove breach is eliminated. However, only personal injury or damage to property is compensable under the strict product liability. Courts generally rule that economics damage should be contracted for. In addition, legislature can pass a statutory provision for software liability. They can then specify what the responsibilities of various parties are and the penalty in case the rules are not upheld.

However, software is not always regarded as a product under product liability rules. Notwithstanding the culture of impunity, from a general legal perspective, software companies can be held liable under civil and criminal law (contract and tort) for any malfunction of security and/or efficacy of their products, e.g., for death caused by a hospital software malfunction. However, it has to be noted that literally all software liability cases are being solved outside the courts. This is due to the burden of proof described above, but also due to the fact that vendors often disclaim liability by means of contractual agreements (cf. discussion on EULA above), or the outcome of such liability claims cannot be predicted.

There is not much case law about third party software liability in civil cases that can be used as general landmark decisions. Nonetheless, it can be stated that in case of a security breach, it will almost always be problematic to directly blame and assign liability. If the cause of the security breach cannot be clearly identified (meaning that the fault-based approach is not tenable), an attorney's view will likely be to sue all involved parties or the economically most powerful party, especially if it is unclear which of multiple components was vulnerable.

7.4 Obstacles Preventing more Incentive-Compatible Regimes

One of the biggest challenges in establishing a tighter software liability regime is the difficulty of establishing causation. High interdependence limits the usefulness of analysing software components in isolation. Thus after any incident, it is not easy to attribute the cause of a loss to a particular piece of code originating from a specific vendor. Other reasons for damages can be inappropriate installation or configuration by the operator, or the specifics of the operational environment. In some instances this exercise can be costly enough to deter any possibility of lawsuit. This creates a dilemma for any liability regime: either it lacks enforceability if the root cause of losses is hard to determine, or vendors have to restrict interoperability if superficial investigation bear the risk of false attribution.

The second challenge is to quantify the losses. Security-related damages are not only intangible, but also spread over a long period of time. In both instances, assigning an economic value to these damages can be highly challenging. More importantly, even if economics damages can be quantified, they are usually not compensated in liability cases, especially under strict product liability

The question of software liability stands in a complex relationship with the market structure on software markets. Two aspects are relevant. First, many software markets exhibit homogeneous code bases, maintained by a few dominant vendors, which increases the risk of correlated or cascaded failures, potentially leading to very large aggregate claims from many users, unlike in the conventional product market. This could exhaust even large vendors' financial resources in a strict liability regime and again lead to a socialisation of losses. This lock-in in the current market structure and code base is a substantial obstacle to any sudden policy change on software liability. The second obstacle with regard to market structure addresses the concern that a stricter liability regime may in fact serve as market entry barrier to innovative competitors, thus directing rents to established players and slowing down innovation in a field that has been a substantial driver for growth over the past decades. This

is particularly important for a fast moving technology markets where software usually plays a dominant role.

Another significant challenge to instituting liability regime is the growth of free software economic systems. By definition, free software vendors (so called distributors) do not have an ability to economically compensate their customers. Thus any liability regime would need to make provisions for free software vendors. Otherwise, free software products cannot stay in the market. Since free software products have become large players in some markets and are generally held as a model for software development and innovation compared to proprietary (or closed source) products, any regulatory changes in liability regime would have significant stifling consequences for these products.

A challenge for software regulations is that has to be an international effort. No one country (especially if it has small market size) can pass tough regulations by itself. It would allow the vendors to bypass that country instead of making serious investments in improving security.

7.5 Realistic Policy Options

The above discussion has shown that the status quo is unsatisfactory but finding the right balance between the conflicting interests is not easy. Here we outline some compromises that seem more feasible than a regime shift to strict software liability.

One option is to impose stricter general liability and then limit the amount of liability, both from below to keep the legal system free of trifles[6] and from above to make vendors' financial risks more predictable. One can distinguish between an upper threshold per product sold or per unique flaw. The former is less attractive for mass markets whereas the latter complicates litigation in defining the uniqueness of flaws and raises new questions on the distribution of compensation payments among all affected users. To avoid market-entry barriers, upper thresholds should not be fixed but depend on certain parameters of the vendor, such as size, sales, retail price, or market share. However, limited liability is not a panacea and has to be designed carefully to avoid evasion by contractual terms. For example, under the current regime, vendors are often found to force customers into additional support and maintenance agreements upon each license purchase in order to limit the factual liability arising from the EULA and to fulfil its warranty obligations. Depending on the jurisdiction, such a liability cap may be the contractual value of the licensing. Note that such liability caps are sometimes held to be null and void. For instance, courts have held that a software company's stipulation that customers could not take action against it for the poor performance of its software was unfair and could not be enforced.

Aside from limiting the amount of liability, one can also adjust its scope. For example, liability could be waived for software which has either been certified after thorough inspection by a

[6] *For example, the EC Product Liability Directive includes a lower threshold of 500 Euros.*

trusted party, or been developed in a secure environment following a certified design process. There are already many such efforts underway, and bringing them under one umbrella can prove a fruitful policy option. Liability can also be limited if the vendor has provided a patch for a problem (and hence the responsibility for implementing the patch is with the users). Patch uptake is often reported to be slow because it involves testing and opportunity costs. So another way to impose limited liability is let vendors pay for the patching cost (up to a limit) but refrain from imposing loss liability. Conversely, extensive liability might apply for particularly sensitive software components, such as operating systems, hardware drivers, and security software. To ensure a smooth adjustment to any new liability regime, grandfathering clauses can be devised to exempt legacy systems from stricter liability temporarily.

Another way to smoothen the transition is to tighten the liability regime stepwise by starting in sectors where bad software can do most harm (e.g., healthcare, energy, finance) and gradually rolling out the regime to other sectors. Similarly, one could start by product classes (e.g., security software, network equipment first) with a clear timeline how this list will be amended. This helps vendors to plan ahead and anchors their expectations. Of course drawing the line will be tricky in each case and prone to lobbying attempts.

A broader application of the principle that liability should be assigned to the party in the best position to prevent losses might identify other parties in a network ecosystem than the developer (i.e., vendor) or end user. For example, when insecurity results from the interaction between multiple parties, for example in the case of malware distribution, it might be efficient to assign limited liability to an intermediary. This can be for instance a service provider who can benefit from economics of scale in threat monitoring and aggregate usage pattern in order to identify threats and to actively prevent further propagation. Any regulation in this direction has to be carefully drafted to set the right incentives while respecting data protection and avoiding excessive price rises or service rationing. Both are more likely for less competitive services.

The limitations of national legislation in an international software ecosystem call for international coordination at least on the level of the EU. As large parts of the software industry are based in developed countries outside the EU, an OECD initiative to create guidelines for its member governments might facilitate a global approach towards clearer, and potentially stricter, software liability. A clear and coordinated signal to software vendors allows them to adjust their strategies, minimised misallocation of resources due to uncertainty and loopholes between jurisdictions, and frees resources for further innovation.

7.6 Conclusion

The approach taken on software liability crucially shapes the software ecosystem that runs our information society. After decades of factual impunity and legal uncertainty spurring innovation and productivity growth, society's dependence on its information infrastructure has grown to a point where it is time to rethink the balance between opportunity and responsibility. As several substantial obstacles impede finding and enforcing the right policy

for an economically efficient software liability regime, a gradual approach towards tighter software liability appears most realistic.

7.7 Stakeholders:

European institutions, national authorities, national security institutions, sector regulators, Non-Governmental Organisations and Law Enforcement Agencies are stakeholders regarding policies, legislation, regulatory and law-enforcement.

Individual and consumer organisations and professional associations are stakeholders with respect to the use of software.

IT developers, vendors and IT operators together with IT audit organisations and Research Institutions/Universities are stakeholders regarding development, distribution, operation and audit of software.

7.8 Implication to EU policies and directives:

European Commission (2006): Defining the Commission's global policy on the fight against cyber crime. This report has implications in specific to problem

- Area 7: Unclear system of responsibilities and liabilities for the security of applications as well as for computer soft- and hardware

7.9 Terminology

Term	Explanation
(IT) Security	All aspects relating to defining, achieving and maintaining data confidentiality, integrity, availability, accountability, authenticity and reliability. Source: ENISA – Glossary of Terms
Liability	From a legal perspective a person or company is said to be liable when they are financially and legally responsible for something. Manufacturer's liability is a legal concept in most countries that reflects the fact that producers have a responsibility not to sell a defective product. However, product liability does not always cover software and all damages caused by defective software (e. g. it is disputed whether software falls under the categories of product liability).
Software	Software is a set of programs, procedures, algorithms and its documentation. Program software performs the function of the program it implements, either by directly providing instructions to the computer hardware or by serving as input to another piece of software. Source: en.wikipedia.org

7.10 Short annotated bibliography on further reading

- August, T. & Tunca, T. I. (2011): Who Should be Responsible for Software Security? A Comparative Analysis of Liability Policies in Network Environments. In: *Workshop on the Economics of Information Security (WEIS),* Fairfax, VA [The authors differentiate between loss liability and limited liability in the sense of covering the cost of patching. A third option in their model is mandatory security standards. They study both short-term and longer-term effects on software quality. The conclusions depend on the exposure to attacks against *unpatched* systems and loss liability is never optimal in their model. The paper also includes a literature review of alternative economic analysis with a focus on patch provisioning.]
- Anderson, R., Böhme, R., Clayton, R. & Moore, T. (2008): *Security Economics and the Internal Market*. Study commissioned by ENISA. [The authors acknowledge that a sudden regime shift on software liability is unrealistic. Instead they discuss two forms of limited liability: secure defaults with free and unbundled patches, and intermediary liability targeted at ISPs to intercept malware propagation. The report contains no formal model or analysis of the proposed policies.]
- Kim, B. C., Chen, P.-Y. & Mukhopadhyay, T. (2011): The Effect of Liability and Patch Release on Software Security: The Monopoly Case. *Production and Operations Management* 20 (4): 603-617. [An economic analysis investigating the effect of full and limited software liability on a monopolistic vendors' decision to on security quality. Their model suggests that the effectiveness of the liability regime depends on the dispersion of the loss distribution.]
- Two opposing views on software liability in the special case of security software were published in the January/February 2003 issue of IEEE Security & Privacy Magazine (volume 2).
- High Court of Justice Queen's Bench Division Technology and Construction Court [2010] EWHC 965 (TCC) Case No: HT-08-111 Kingsway / Red Sky

8 Return on Security Investment

By Jeremy Ward - HP Enterprise Security Services

8.1 Abstract

This paper examines the background, history and limitations of the Return on Security Investment (ROSI) concept. It considers the way that ROSI has been used by governments and by other organisations. It concludes that the concept is not one that is significant to the EU regulatory framework. It identifies 11 significant actions in connection with a ROSI implementation and the principal stakeholders associated with those actions. Finally it suggests 6 issues which require further work.

8.2 Keywords

Annual Loss Expectancy. Asset. Business Risk. Event. Impact Analysis. Incident. Information Security. Quantification. Risk. Risk Assessment. Risk Controls. Security. Threat. Vulnerability.

8.3 Executive summary

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 for the calculation of ROSI have been in existence for more than 10 years. Despite this, their use has not been extensive in either government or industry within the EU. ROSI techniques, however, are in use by both the USA and Australian governments.

Major issues that have limited the take-up of ROSI techniques have been:

- Their association with the security vendor community, as a way of justifying security spending.
- The difficulty of estimating the cost of security controls.
- The difficulty of estimating their effectiveness.
- Lack of good data on the frequency and impact of security incidents.
- The lack of a universally recognised, practical standard for ROSI.

The implementation of a ROSI analysis requires the organisation to carry out 11 essential actions, as follows:

A. Identification of relevant security controls.
B. Quantification of costs of relevant security controls.
C. Determination of business asset value at risk.
D. Identification of security incidents having the potential to impact business asset value.
E. Quantification of frequency of security incidents potentially impacting asset value.
F. Quantification of potential extent of impact of security incidents on asset value.
G. Quantification of effectiveness of identified security controls.

H. Calculation of ROSI based on the four quantified values above.
I. Identification and prioritisation of improvement areas for security controls.
J. Planning for improvements, based on prioritisation.
K. Implementation of improvements.

Involvement in carrying out and being consulted and informed on these actions is widespread across the organisational structure; with stakeholders in disparate areas. As such, the adoption of a ROSI analysis would serve to improve understanding of information security risk management throughout an organisation, as well as ensuring the adoption of cost-effective security controls.

It is suggested that the EU may wish to consider the example of the US government in the adoption of ROSI techniques in government agencies. This could be accompanied by the production of a simple, practical ROSI standard that would encourage more widespread take-up of this useful technique.

8.4 Summary of existing works

8.4.1 Background and history

Unlike most business investment, investment in information security controls does not give easily quantifiable improvements in revenue or operating efficiency. The concept of Return on Investment (ROI) is therefore of little use when seeking to establish a business case for information security spending. To justify such spending therefore, organisations may seek to link it to the mitigation or management of risk; and thus the potential to reduce harmful impact on an organisation's business. This concept is known as Return on Security Investment (ROSI).

The ROSI concept may be expressed as an equation that can occur in a number of forms, the simplest of which is:

ROSI =((Cost of Risk Exposure x % of Risk Mitigated)-Cost of Controls)/Cost of Controls

(equation adapted from Sonnenreich, 2006[1]).

Research in the software development community has found that there is a 21% return on security investment at the software design phase, a 15% return at the implementation stage and a 12% return at the testing stage (Berinato, 2002[2]). This research gives quantitative support to the value of building security in at an early stage of any project.

ROSI emerged as a topic of interest more than ten years ago. An early reference to ROSI (Korofsky 2001[3]) is in work on the subject by a digital security company (@stake – subsequently bought by Symantec). From this, it may be concluded that the concept of ROSI (as distinct from ROI) was first initiated by the IT security vendor community as a mechanism to help businesses build a case for spending on information security technology and services.

By 2004 the ROSI concept had attained enough momentum for it to be adopted by the Australian government (Lockstep Consulting, 2004[4]) and incorporated into the US government requirements under the Federal Information Security Management Act (FISMA) (see NIST-SP-800-65, 2005[5]). In 2005 ROSI was of sufficient interest to major corporations to be the subject of a report by the Information Security Forum (Information Security Forum, 2005[6]).

Over the past five years interest in ROSI has been steady and the concept may be spreading in emerging markets (Marcos 2009[7]). A number of security vendors and other organisations have developed and marketed tools that aim to assist businesses with the calculation of ROSI; for example: the tool attached to the Australian government report (Lockstep Consulting 2004[4]) and a free ROSI calculator offered by the Information Security and Business Continuity Academy in 2011[8].

8.4.2 Limitations

Major drawbacks to understanding and use of ROSI have been confusion over its scope and the fact that it can be seen as a "vendor driven" attempt to promote the sale of security products. Although primarily used to denote information security investment, ROSI can also be applied to investment in physical security, for example in building management systems (Dimmick 2011[9]), which further confuses the issue.

However, the greatest limitation on the use of ROSI is the difficulty organisations have in collecting the material needed to calculate a value for it. In its simplest expression, ROSI can be determined as the difference between the annual loss to be expected as a result of the impact of security failures and the annual expenditure on security controls. However, even this simple statement raises two fundamental problems. First, how organisations are able to calculate annual loss expectancy (ALE). Second, the difficulty of collecting data on the cost of security controls. This, although apparently simpler, in practice is not easy for most organisations; since costs contain elements of technology, people and process that are divided between disparate parts of the organisation.

In calculating ALE, organisations are faced with the decision whether to include both direct and indirect, financial and non-financial elements. Non-financial, indirect elements may include reputation , customer satisfaction, employee effectiveness and compliance (Information Security Forum, 2005[6]). Direct elements may include revenue and earnings, management and operating costs (Information Security Forum, 2005[6]). All these elements can appear as either losses or gains in the risk equation. Not all elements will be applicable to every type of organisation; governments for example will be little affected by revenue concerns, since they are effectively monopoly suppliers (Lockstep Consulting, 2004[4]). As will be appreciated, losses and gains in some elements are more difficult to calculate than in others (reputation for example, as opposed to revenue).

Perhaps the major issue faced by organisations wishing to calculate ALE is the selection of a workable and appropriate means of assessing the cost of security events and incidents. Most organisations lack appropriate metrics that enable them to calculate the frequency of occurrence of these, or their cost (Sonnenreich, 2006[1] – and personal observation). In the

absence of such data, assessments have to be made on the basis of estimates of frequency and cost impact. This requires the adoption of an appropriate risk assessment methodology and the expertise to use it.

In assessing the cost of controls, most ROSI models take account only of those that are technological. This simplifies the issue, but does not necessarily make the calculation easy. For example, the cost should take account of any potential loss of productivity that will arise from the implementation of the control (Sonnenreich, 2006[1]). However, some models have attempted to quantify the cost of broader information security management systems control, such as those in ISO 27002 (Ward, 2007[10]).

8.5 Areas of applicability

8.5.1 Governments

As has already been mentioned, ROSI has been adopted by the Australian government (Lockstep Consulting, 2004[4]) and by the US Federal government (NIST-SP-800-65, 2005[5]). The Australian use of ROSI is not mandatory, and is intended to assist government agency IT managers to evaluate and quantify the potential security return from investing in (specifically) perimeter security controls. The control guideline is accompanied by a spreadsheet that enables the evaluation to be carried out practically. The spreadsheet tool is especially interesting, as it uses freeware "Monte Carlo" simulation software in order to calculate returns that result from a spread of the number and severity of incidents. This gives a more realistic calculation than that which would be achieved by using simple "one off" values for number and severity. The Australian guidance document would be relatively simple to use, and could be adapted to commercial organisations. The extent of take-up of this methodology by Australian government agencies is unknown.

The US Federal Information Security Management Act of 2002 charged Federal government agencies with the need to combine information security with capital planning and investment control. As a result, the National Institutes of Standards and Technology (NIST) of the US Department of Commerce, produced a special publication (SP 800-65) that introduced common criteria for ensuring cost-effective implementation of information security controls. Arising from this was a requirement for agencies to use these criteria annually in order to self-assess the cost effectiveness of controls implemented. SP 800-65 sets out a series of processes that are intended to enable Federal agencies to prioritise their security control actions on the basis of a gap analysis of their current against target effectiveness, the cost of taking corrective action and the impact of that action on the security of the systems to which it is applied. SP 800-65 is a highly detailed standard that would require significant resources to implement and is unlikely to be of value to any but the largest commercial organisations.

8.5.2 Commercial and other organisations

The Information Systems Audit and Control Association (ISACA) has produced an IT audit and assurance guideline for ROSI (ISACA, 2010[11]). The purpose of this guideline is to assist IT auditors in commercial organisations to review returns on security investments. There is little published evidence of commercial organisations applying ROSI. However, the Intel Corporation has produced a White Paper based on its own experience (Rosenquist, 2007[12]). From personal experience, it is probable that ROSI is used to some extent in large corporations (especially those that are members of the ISF) but that its take-up has not been general because of the limitations described above. There is no evidence that ROSI is used to any great extent in not-for-profit organisations or in the academic sector.

8.5.3 EU regulatory framework

Below is a summary of the relevance of ROSI to the EU regulatory framework:

- The ENISA Founding Regulation: Article 16: "The promotion and development of best practices for risk assessment and for interoperable risk management solutions within public and private sector organisations".
- Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA): Section 1.5: "identify economic and regulatory incentives for security and resilience".
- The Digital Agenda for Europe: Section 2.3: Trust and Security: no mention of cost-effective security measures.
- Information from the thematic portal on Critical Information Infrastructure Protection, CIIP.
  No mention of security cost-effectiveness.

  The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM (2010) 673 final. No mention of security cost-effectiveness.
- Draft Internal Security Strategy for the European Union: "Towards a European Security Model". No mention of security cost-effectiveness.
- Single Market Act, Twelve levers to boost growth and strengthen confidence, COM(2011) 206 final. No mention of security cost-effectiveness.

8.6 Involved stakeholders - organisational

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 there is now a requirement 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.

The essential actions required for a ROSI analysis can be summarised as:

A. Identification of relevant security controls.
B. Quantification of costs of relevant security controls.
C. Determination of business asset value at risk.
D. Identification of security incidents having the potential to impact business asset value.
E. Quantification of frequency of security incidents potentially impacting asset value.
F. Quantification of potential extent of impact of security incidents on asset value.
G. Quantification of effectiveness of identified security controls.
H. Calculation of ROSI based on the four quantified values above.

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

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

Table 1 indicates, at a high level, the stakeholders likely to be involved in carrying out the actions listed above. The matrix indicates if the relevant stakeholder is responsible for carrying out the action (R), accountable for the action (A), should be consulted (C), or merely informed (I). A dash is used to indicate where the stakeholder has no involvement. Where consultation is shared, the subjust of consultation is indicated in the appropriate box. The table illustrates that ROSI has widespread ramifications throughout an organisation, and is thus a useful vehicle for promoting the understanding of information security risk management.

ROSI Actions	**Stakeholders**				
	Information Security	**IT**	**Business Asset Owners**	**Finance**	**Board-Level Management**
A. Control identification	R/A	C About technical controls	C About asset criticality	-	-

ROSI Actions	Stakeholders				
	Information Security	**IT**	**Business Asset Owners**	**Finance**	**Board-Level Management**
B. Control cost quantification	R	C About technical controls	C About asset criticality	A	I
C. Asset value at risk	R	C About risks	A	C About costs	I
D. Security incidents	R	A	I	I	I
E. Incident frequency	R	A	I	I	I
F. Incident impact	R	C About impacts	A	C About costs	I
G. Control effectiveness	R/A	C About technical effectiveness	C About business effectiveness	I	I
H. ROSI calculation	R/A	I	I	I	I
I. Improvement areas	R/A	C About technical improvements	C About process improvements	C About improvement costs	I

ROSI Actions	Stakeholders				
	Information Security	IT	Business Asset Owners	Finance	Board-Level Management
J. Improvement planning	C About security issues	R	C About process issues	C About financial issues	A
K. Improvement implementation	C	R	I	I	A

Table 1: RACI Matrix for ROSI Organisational Stakeholders

8.7 Involved stakeholders – potential further actions

More widely, stakeholder groups have a potential interest in driving the adoption and use of ROSI throughout the EU. It is suggested that this could be achieved through the implementation of a number of actions:

- Definition of metrics associated with ROSI
- Definition of a ROSI standard
- Adoption of a ROSI standard by government agencies
- Implementation of ROSI certification for government suppliers
- Wider adoption of ROSI techniques by regulated private enterprise organisations.

Each of these factors is considered in table 2, which shows a RACI matrix for concerned stakeholders; these are defined in the appendix to this paper.

Stakeholders	Actions				
	Definition of Metrics	Definition of Standard	Adoption of Government Standard	Certification for Government Suppliers	Adoption of ROSI techniques
European Institutions	A	A	A	A	A
National Authorities	C	C	R	R	R

Stakeholders	Actions				
	Definition of Metrics	**Definition of Standard**	**Adoption of Government Standard**	**Certification for Government Suppliers**	**Adoption of ROSI techniques**
	About policy	About policy			
National Security Institutions	C About security	C About security	C About security	C About security	I
Sector Regulators	I	I	I	C About applicability	C
Law Enforcement Agencies	I	I	I	I	I
Non-Government Organisations	I	I	I	I	I
Professional Associations	C About technicalities	R	C About applicability	I	I
Research Institutions	R	C About technicalities	C About technicalities	I	I
Individual Organizations	I	I	C	C About ability to comply	R
Consumer Organizations	I	I	I	I	I

Table 2: RACI Matrix for ROSI Concerned Stakeholders

8.8 Conclusion

ROSI is a concept which should have widespread applicability and use, particularly in times of greater economic stringency. In addition, the use of ROSI by large organisations would lead to improved understanding of information security risk management throughout the organisation and would be conducive to a more holistic and strategic approach to information security. However, the difficulties of scoping and gathering data on the cost of security controls and on the frequency and impact of security incidents have been significant barriers to the uptake of ROSI.

As suggested in table 2, it is worthwhile considering if the EU should introduce the use of ROSI within government agencies (as has been done in the USA). It is possible that, in doing so, it could also introduce a standard, practical version of ROSI that could be widely deployed in both government and industry. This might also have the added effect of improving the quantity and quality of data concerning the quantifiable measures required by the ROSI analysis.

8.9 Open issues

The following issues require further examination:

1. What is the take-up of ROSI within public and private organisations within the EU?
2. What are the most significant barriers to the take-up of ROSI?
3. What measures should be taken to overcome those barriers?
4. Can a practical ROSI implementation standard be introduced within the EU?
5. If so, who should produce it and how likely is it to be accepted?
6. Should ROSI be required within EU government agencies?
7. Should ROSI (or a cost/risk analysis) be required for all new EU information security initiatives?

8.10 List of bibliographic references

1. Sonnenreich, Wes. Return on Security Investment (ROSI): A Practical Quantitative Model. Journal of Research and Practice in Information Technology, Volume 38, no. 1, February 2006.
2. Berinato, Scott. Calculating Return on Security Investment. February 2002. http://www.cio.com/article/30856/Calculating_Return_on_Security_Investment
3. Korofsky, Eric. Insight Into Return on Security Investment. Secure Business Quarterly, Volume 1, Issue 2. 2001. http://www.sbq.com/sbq/rosi/sbq_rosi_insight.pdf. [Note: this reference is no longer Internet accessible].
4. Lockstep Consulting. A guide for government agencies calculating return on security investment. June 2004. http://services.nsw.gov.au/inside-dfs/information-communications-technology/publications/return-security-investment

5. NIST: Integrating IT security into the capital planning and investment process. SP-800-65. January 2005. http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf
6. Information Security Forum. ROSI: Return on Security Investment Workshop Report. July 2005. [Note: this reference is only available to ISF members].
7. Marcos, Gabriel. ROSI – Return on Security Investment. September 2009. http://blogs.globalcrossing.com/?q=node/496
8. Information Security and Business Continuity Academy. Free Return on Security Investment (ROSI) Calculator. June 2011. http://www.iso27001standard.com/en/rosi/return-on-security-investment#
9. Dimmick, Matthew. Improving Return on Security Investment. July 2011. http://www.msasecurity.net/security-and-counterterrorism-blog/bid/60062/Improving-Return-on-Security-Investment .
10. Ward, Jeremy. Building the information assurance community of purpose. International Journal of Computer Systems Science and Engineering, Volume 5, 247-257. 2007.
11. ISACA®. IT Audit and Assurance Guideline G41: Return on Security Investment (ROSI). March 2010. http://www.isaca.org/Knowledge-Center/Standards/Documents/G41-ROSI-5Feb10.pdf
12. Rosenquist, Matthew. Measuring the return on IT security investments. White Paper, December 2007. http://www.intel.com/it/pdf/measuring-the-return-on-IT-security-investments.pdf

9 Risk Management of IT-Security Business Processes

By Mr. Eyal ADAR, White Cyber Knight Inc., Bnei-Brak, Israel and Mr. Ralf SCHNEIDER, TÜV Informationstechnik GmbH, Essen, Germany

9.1 Executive Summary

Reliable and secure performance of business processes depends on their implementation by people, procedures, and technical systems like IT (which are built by components). The business impact due to failure in availability or insecure operation by manipulated data or disclosure can be manifold. By this, the question comes up: what are the rules of interdependencies between business processes and implementing components and how 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 i.e. business processes are dependent on IT systems and their components like applications, information, servers or networking devices. Analysing IT and security risks with business processes perspectives will enable us to link the two worlds that use today a different language: the business world and the ICT world. This link is an important contributor to the economics of security as it will enable to provide transparency of risk posture to the business management, to receive their needs and priorities, and to enable support to informed decisions.

This report describes the need and the concepts of Business Process Risk Management and provides examples of such methods. It outlines ways to integrate those aspects in the risk assessment activities, existing information security standards and best practices, and brings practical examples of methods for such assessment.

9.2 Key Words

Security, governance, risk, compliance, GRC, risk management, risk scenarios, critical risk, critical infrastructure, criticality level, resilience, robustness, economics, dependency, interdependency hierarchy, cloud, EU, European institutions, national authorities, national security institutions, sector regulators, policies, legislation, regulatory and law-enforcement, business process, smaller business (SMB), business performance, business support, IT systems, IT assets, applications, servers, databases, network devices, RiskMap, EESA, ISO/IEC 15408, ISO 27001/2/5, BSI-Standard 100-3, NIST 800-53.

9.3 Status Quo

In the following, we compare the principle, that risks should be taken care by the party in best position to mitigate threats, with the actual situation. In the ideal world, every business knows its risks and does effectively counter risks to an acceptable, i.e. efficient level. In other words: risk management is a means to economically counter obstacles preventing achievement of business objectives. For that all critical risk scenarios have to be known to and ruled by the

business management. Risks, resulting from the use of IT due to security failures, need to be covered as well.

Large business organisations are used to have a business risk management in place. But interdependencies with the IT risks are often outside the focus of established management systems and their players. This decoupling is risky by itself, especially if security matters, like in many cases. Even more difficult the situation is for the vast majority of smaller business (SMB) organisations not having any risk management in place. Consequences may be the loss of business performance, e.g. by disturbance of system availability or the loss of market acceptance, e.g. by data privacy issues. Theft of internal business secrets like business plans or construction details may result in loss of a unique selling proposition etc. To an end, the risk here is not only to miss the business objectives or even purpose, but to generate unwanted externalities with social costs.

The reason for the lack of risk awareness and handling by business organisations can be found in the characteristics of IT compared to common technologies. The IT is a relatively young technology; its knowledge is highly specialised and not common to all senior people, especially at management level. Changes in the IT are typically much faster than common technologies, which may interfere with the habit and culture of people, who are primarily used to common technologies. Finally, business organisations ask for quick time-to-market rather to question the business support by IT and its security. On the other hand, security people speak a different language that only they understand, and it doesn't translate to business aspects easily. All this takes place in a situation, where business is increasingly vulnerable to cyber attacks because of its growing dependency on the IT and the 'cyber space'. In addition, business is facing a permanent raise of attack potential by raise of frequency and sophistication.

9.4 Obstacles Preventing Business-Centric Approach to Cyber Risks Management

Organisational issues

Even if all critical business risks are known, the bridge to the IT security risks is a Fata Morgana, because those people dealing with business risks are typically having a non-IT education and therefore are blind to the IT implied security risks. Furthermore, the Governance, Risk and Compliance (GRC) team is normally associated to different business divisions than the IT is. Vice versa, members of the IT team are not having the background nor having the information on the real business world, which they are supposed to professionally support. So a chain of cause to business impact is difficult to be derived. Aside the different perspectives, involved people have different ways of thinking and behaviour. All together one is facing a combination of organisational, educational, sociological and even psychological and cultural issues to risk management.

A second obstacle is the limited transparency of organisational processes and procedures. Organisations may even not have documented their business processes, which would be a

must for a reasonable risk management. But this is true also for the IT side, which is sometimes careless in documentation. So organisational information asymmetry counters risk control. At the same time, business organisations deal with high complexity, pre-maturity, distribution and de-allocation of organisations, their processes and technologies. Enormous potential for weaknesses results from this. Sometimes, organisations don't want a high transparency of their risks, because known risks may hinder technology and market innovations, which is also a cultural and psychological issue. If the business organisation together with the GRC team, the process or quality team and the IT and security team are asked to interact efficiently, then communication is critical to success. This is a clash with the combined issues above.

The situation is similar for an internal or external audit team. It does need to have a multidisciplinary background, so that it is capable of all the challenges such that it can deliver quality and value to the organisation. At the same time, a high dependency results from the applied methods, see below.

Technology driven issues

Complexity of today IT products and IT systems together with shortest time-to-market requirement is a source for functional and security flaws, resulting in a multitude of weaknesses to users and threats. Aside force-majeure, human negligence or limited capability of used technology, a malicious attacker may intentionally abuse these weaknesses to his profit or malicious aim. But as it is always with innovative and complex things, every weakness or threat scenario cannot be foreseen and prevented by design. Even analytic measures of an organisation will be limited in effect, especially if they shall be efficient and time-to-market compatible at the same time.

One indicator for complexity is the interdependency. Software systems may rely on their applications, the underlying operating system together with used hardware, its resources and mediated services. Core components have to implement the generic security objectives integrity, confidentiality and availability. But again, these components do rely on each other. Certain security specific criteria may be used to confirm the required security level on components level, like the "Common Criteria" for security evaluations, ISO/IEC 15408. But very often, the actual evaluation result is limited to sub-subsets of the used systems. And if the story is not complex enough, the assembly of many components to a system and further systems to networks and networks to the "web" or "cloud" will even exponentially raise the complexity. There is by today not a single entity capable of knowing all potential weaknesses and vulnerabilities to threats. And for sure, no one is having a cure for all of them by effective countermeasures, not to say efficient.

Another limit of IT product evaluations is the "assumed" operational environment, which is in fact not known to the developer. In other words, one has to include the operational environment into risk considerations, where physical infrastructure, organisation and people are the players, bringing in additional threats to be countered.

Automated means supporting such complex risk analyses are existing manifold. But most approaches are limited to the IT and its narrow environment. They are not taking into consideration the type of organisation that the IT systems serve and the specific business activities. Thus the results of the assessments can provide only limited view of the real risks to the business that can be driven from the IT environments.

9.4.1 Methodical issues

Much work was achieved in setting IT security risk assessment methods and best practices, such as ISO/IEC 27005, German 'BSI-Standard 100-3' or 'NIST 800-53' from the USA that brings a strong driver of robustness, driven by identification of vulnerabilities, risks, and their treatment, as a proactive activity. And 'Octave', that is focused on attack scenarios. Also, risk assessment 'ISA 99', which is looking at industry control systems or 'Process FMEA' and variants, mainly set in the automotive industry.

But all are limited to some extent: Either, there is a more managerial approach, like by ISO/IEC 27005, and less based on technical details of the IT. Or the method is not directly addressing the IT, like FMEA. So the bridge between the business and the IT security, the causation between IT security flaws and incidents to business impacts, is not thoroughly supported.

9.4.2 Policy issues

The large number of statutory requirements, applicable to organisations, further raises complexity of the organisation and lowers its productivity. Legal compliance is becoming sophisticated, requiring inevitable resources for control and implementation. And in practice, it is limiting the business attention, also in regards to risk management. As an outcome, typical financial risks are ranking higher than IT security risks – the latter may even not be addressed by the top management.

Although risk management is an indispensable mean for business success, still it is typically applied only by huge organisations. A vast majority of SMBs deals with its risks by instinct. With all in-transparency consequences like to overlook risks, under-/overestimation of risks and necessary measures, liability issues for the organisation and its management. In addition, legislation is not harmonised and often risk management is required only for the minority of business organisations. As a consequence, externalities with social costs are to be expected, if a business organisation fails in its economic environment due to failure in risk management of IT security.

Information on security flaws and imperfections of used IT and a cure to it, is only partly available or for high costs. This is another information asymmetry, countering the needed transparency for risk management. As well as, a consensus by all stakeholders on a reasonable and holistic risk management approach is not available, so far

Finally, the only common incentive for a thorough risk management seems to be the potential relief from accusations by proof of a state-of-the-art business approach. Vice versa, in-

homogeneity of internal legislation may allow organisations to bypass strict regulations of other countries, which limits enforceability e.g. of a liability regime. A homogenous and supporting incentive-compliant regime for a holistic risk management at business level covering specifics of the IT and its security seems to be a desirable future for the EU.

9.5 Realistic Options

As we have seen, there is enormous potential for weaknesses in today's business. This is due to high complexity, pre-maturity, distribution and de-allocation of organisations, processes and technologies together with different people behaviour, culture and education. A lack of knowledge and information about the real world and limited availability of means, methods and tools make it not easier.

9.5.1 Policy options

To improve the real situation on mid-term, the EU should consider, either it is possible to issue policies, so that business organisations have incentive to establish and operate a holistic risk management in their organisation. These policies need to be in line with the EU objective of a coherent and liberal internal market. Course of action within such an incentives regime will allow growth of best solutions for a reasonable level of security and, at the same time, keep externalities small. Obstacles for competition should be limited to the inevitable. Additional punitive actions should focus on the small group of 'non-conformists' and, for sure, illegal activities.

Possible regulatory options should consider allowing light risk management approaches, where reasonable. This could mean e.g. reduced efforts for documenting purposes. Also acceptance of organisational certifications might be a further help, to limit efforts and to raise utility of such certifications.

Harmonised and alleviated legislation, at least throughout the internal market, would help organisations to efficiently handle legal requirements and compliance.

9.5.2 Organisational options

Multidisciplinary teams will be a key factor for holistic risk management in any organisation. These teams need ICT specialists and business managers, which may be challenging in the beginning. However, if a clear logic process will be built, especially those two worlds could be bridged. The teams need to be carefully selected. Selection should base on broad competence and qualification profiles, calling for expertise, soft skills and methodical competences in combination with well attitudes. Communication culture and transparency within the organisation should support exchange of knowledge to the extent that risks get obvious and can be treated. The same applies especially to internal and external audit teams.

9.5.3 Methodical options

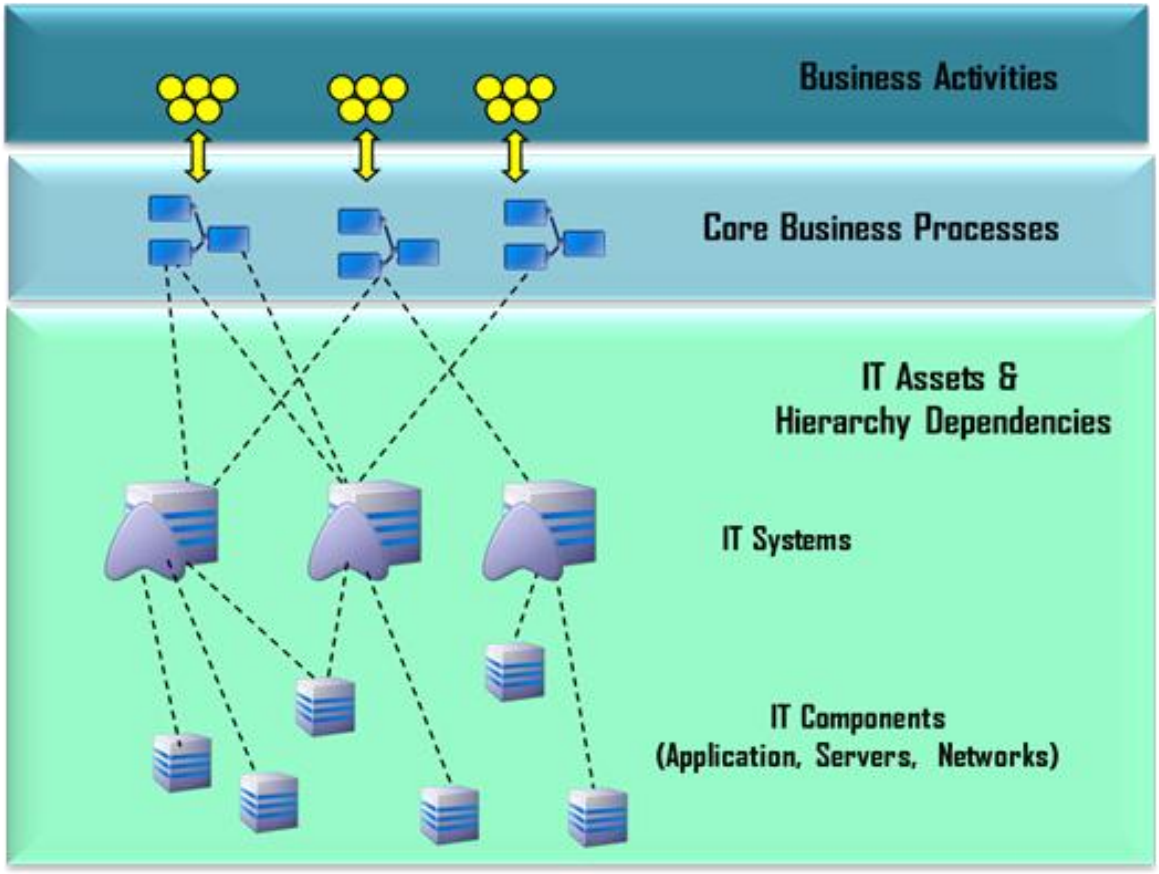
The connecting elements between the organisational worlds are the core business processes within the organisation. A core business process serves a business area or specific business

activities within the organisation. It usually contains a number of sub-processes and being performed through a set of IT systems and their IT assets (or components) such as: applications, servers, databases or network devices.

The IT assets are linked to the business process in hierarchy structure (see figure 1). By mapping the hierarchy and dependencies between each component and the business process, that it serves, it is possible to define the real importance of each component to the business, and what could be the real impact, in case of a security incident. It enables not only to 'speak' in technical language, but to measure the IT risks according to business areas that the IT components serve (such as: money transfer of e-banking in the financial sector, or billing in telecom, or energy distribution in smart grid). The principles of business process risk assessment are

- Assets approach – identifying the dependencies between business process and IT assets
- Assets hierarchy – finding the link between the assets themselves, and towards the business processes they serve
- Assets criticality classification: identifying assets criticality level in security terms (CIA)
- Assets impact type – which type of impact they could have on the organization (financial, legal, brand, productivity, safety)
- Dependencies – measuring the aggregated criticality of each asset (to be explained)

Figure 1: Core Business Processes Hierarchy:



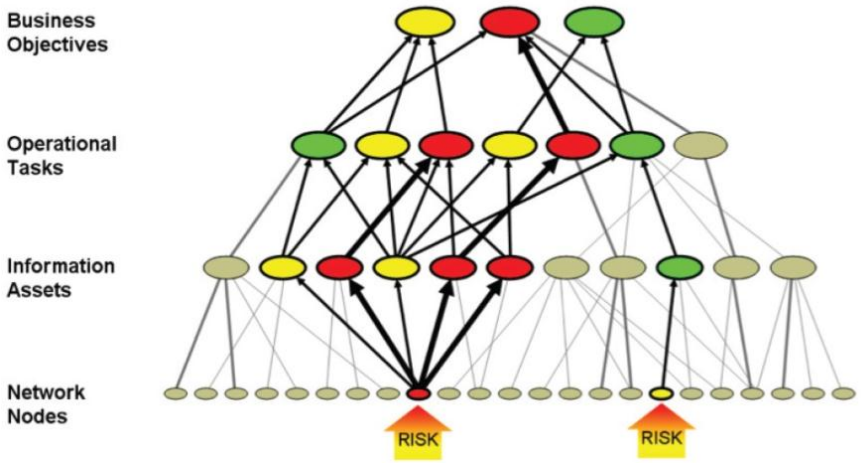
Once these principles are implemented, it is possible to use the regular risk management methods, such as ISO 27001/2/5, NIST 800-53, and to add the business aspect to their results. Here is an example of two methods that carryout the hierarchy and business approach, RiskMap (Risk-to-Mission Assessment Process) and EESA (End to End Security Assessment). The main approach of the two methods is similar. The differences are mainly in the calculations and areas where the methods were demonstrated.

9.5.4 RiskMAP – The Risk-to-Mission Assessment Process

The method is published in the article „A Sensitivity Analysis and an Extension to Treat Confidentiality Issues" in July 2009 (bibliography #5). The article deals with network risks to control systems in critical infrastructure. The initial purpose of the sensitivity analysis is to determine the range of conditions under which RiskMAP's calculation of relative weights for Tasks, Assets and Nodes would behave as order-preserving operations. The need: A process for assessing PCS network risk and translating the results into terms meaningful to corporate-level managers. The approach: Model key features of an organization, from the Business

(Mission) Objectives to the Operational Tasks and Information Assets needed to achieve them, down to the Network Nodes.

Figure 2: RiskMap Hierarchy:

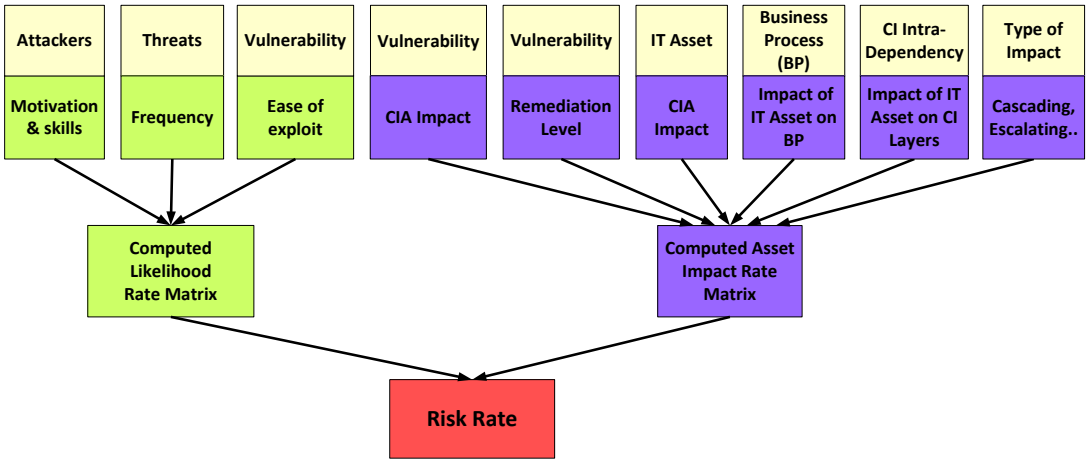


Source: http://www.thei3p.org/docs/publications/riskmap-2009-02-09.pdf

9.5.5 EESA – End to End Security Assessment Framework

This method was published in the first CIP workshop in Frankfurt (bibliography #3). It was part of the analysis of the European Commission's ACIP project that set the research roadmap for CIP Assessment methods, and published in the CEPS (Central for European Policy Studies) report on CIP (bibliography #1). The initial purpose is to add it as another layer to existing good-practices for IT and security risk management methods, in order to add a business centric approach that will be linked to the detailed technical addeddment. The need: Ability to create transparency of risk posture to business management in business terms. To get priorities and needs from the business managers and to enable business decision support. The approach: by identifying IT hierarchy of IT assets, and by classifying the assets according to their business role and business parameters, it is possible to classify the technical findings of the risk assessment in business terms. In addition, adding relevant parameters to the IT assessment enables better understanding of the risk, and as an outcome, better understanding of the organisation's status and the corrective steps that should be taken. Aspects such as: type of impact (normal cause, cascading, escalating), remediation level of the potential incident and impact of the IT to the other Critical Infrastructure layers (the physical and organisational layer).

Figure 3: EESA Framework:



Source: CEPS CIIP TASK FORCE Report (bibliography #1)

So far, the analytic measures above will be a trigger for decisions on risk treatment, i.e. the organisational, technical, personal and infrastructural measures. Whenever they are implemented, effectiveness of these measures is required. Audit trail will show gaps. And incidents report further weaknesses in the risk map. Helpful means to analyse the actual security of an IT network and of its services are also so called 'penetration tests', also called 'ethical hacking'. Based on known vulnerabilities, the security vitality of the IT network and its services can be rated. The output will be helpful recommendations for improvements. There are a few public and national schemes, allowing even certification. The value of such certifications needs to be carefully considered.

9.5.6 Technical options

Protection against technology immanent flaws and vulnerabilities can be improved by due organisational processes, e.g. requesting frequent patch uptake, application, platform and network hardening or continuous network monitoring. Procedural measures will have their limits. So the combination of these measures with dedicated technical measures should be opted. For example, use of regular network protective means could be extended to so called 'appliances', which are said to promise to automatically keep 'known vulnerabilities' attacks outside the network. Care needs to be taken, if the promise is fulfilled. Third party reviews could be a means to get an independent opinion.

Strict or limited liability regimes applicable to IT products and services could help to improve overall quality and security of the IT. A number of international and public evaluation and testing criteria are available in the national schemes. In some cases, like for ISO/IEC 15408, there are even international 'mutual recognition arrangements' which allow acceptance of evaluation results according Common Criteria in many national schemes. For further details see also the results of the WG-EOS group "Software Liability".

To better overcome the 'complexity' issue, the development of means for more transparency of complex systems will help. Today, there are only a few, highly sophisticated methods, which raise insight into the 'mechanics' of complex systems. Economic theory is used to this problem. For further reading, see the results of WG-EOS "economics of resilience". An example architecture is studied in the "CRUTIAL" paper, see below.

Whenever chosen IT components have a security label, i.e. if they are certified, then we have to bring them into the operational IT environment of the business organisation. Here, the organisational quality, risk , security and IT service management are called, to best fit to the organisational goals. To keep flaws and vulnerabilities low in the IT products and systems, strict development processes with requirements definition, control loops, quality assurance measures, thorough testing, effective configuration management and so on. A balanced approach between what is necessary and what is hindering, is needed.

9.6 Stakeholders:

European institutions, national authorities, national security institutions, sector regulators are stakeholders regarding policies, legislation, regulatory and law-enforcement.

Individual and consumer organisations and professional associations are stakeholders with respect to organisational implications.

IT developers, vendors and IT operators together with IT audit organisations are stakeholders regarding technology and methodology aspects of IT security risk management.

9.7 Implication to EU policies and directives:

European Commission (2006): Defining the Commission's global policy on the fight against cyber crime. This report has implications in specific to problem

- Area 3: A lack of a coherent EU-level policy and legislation for the fight against cyber crime
- Area 5: Need to develop competence and technical tools (training and research)

9.8 Terminology:

Terminology	Explanation
(IT) Security	All aspects relating to defining, achieving and maintaining data confidentiality, integrity, availability, accountability, authenticity and reliability. Source: ENISA - Glossary of Terms
Dependency	The state of relying on or being controlled by someone or something else. Source: http://www.websters-online-dictionary.org/definitions/dependency
Interdependency	A bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when

each is dependent on the other. Source: Critical Infrastructure Interdependencies (Annex #2)

9.9 Short annotated bibliography on further reading:

- **"Protecting Critical Infrastructure in the EU"**, Report, from the CIIP (Critical Information Infrastructure Protection) Task Force, of CEPS (The Centre for European Policy Studies), 2010
- **Critical Infrastructure Interdependencies.** By Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly. IEEE Control Systems Magazine, 2001
- **End to End Security Assessment (EESA) for Critical Infrastructure Protection**. E. Adar (iTcon, Tel Aviv) & H. Thielmann (SIT-FhG, Darmstadt) CRITICAL INFRASTRUCTURE PROTECTION (CIP). – STATUS AND PERSPECTIVES – From: Preprints of the First GI Workshop on CIP, Frankfurt a.M. 2003 Edited by Willi Stein, Bernhard Hämmerli, Hartmut Pohl, & Reinhard Posch
- **eTOM - The Business Process Framework** For The Information and Communications Services Industry GB921.
- **Process Control, System Security, Technical Risk Assessment Methodology & Technical Implementation.** Peter Kertzner, Jim Watters, Deborah Bodeau and Adam Hahn, The MITRE Corporation. March 27
- **Risk Assessment Method Based on Business Process-Oriented Asset Evaluation for Information System Security.** Jung-Ho Eom, Seon-Ho Park, Young-Ju Han and Tai-Myoung Chung. Lecture Notes in Computer Science Volume 1 / 1973 – Volume 6837 / 2011.
- **CRUTIAL: The Blueprint of a Reference Critical Information Infrastructure architecture.** Paulo Verissimo, Nuno Ferreira Neves, and Miguel Correia. Proceedings of the 1st International Workshop on Critical Information Infrastructures @ ISC'06, Samos - Greece, August 2006.

European Network and Information Security Agency

Economics of Security: Facing the Challenges – The Working Group Contributions

Luxembourg: Publications Office of the European Union, 20121

ISBN: 978-92-9204-058-1

DOI:10.2824/23074

Catalogue Number: TP-32-12-066-EN-N

TP-32-12-066-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