Position papers of the 2014 Federated Conference on Computer Science and Information Systems pp. 119–122
DOI: 10.15439/2014F439
ACSIS, Vol. 3

ICT Security Risk Management: Economic Perspectives

Gebhard Geiger
Technical University of Munich.
Faculty of Economics
Arcisstrasse 21
80333 München, Germany
Email: g.geiger@ws.tum.de

***Abstract*—ICT security incidents are frequent and prevalent. They not only pose threats to the integrity and operation of the critical infrastructures of modern society, but also tend to cause enormous damage to the public economy. In addition, ICT security management can be very costly, while the success of security technologies and strategies often remains uncertain. From the economic perspective, this situation requires various basic research approaches to be taken to increase ICT security. These include an improved understanding of the far-reaching, highly interconnected consequences of ICT security incidents, development of methodologically sound measures of ICT security risk as well as approaches to measure the effectiveness and cost-efficiency of the ICT security management.**

I. Introduction

MODERN societies almost completely depend on electronic information and communications services and systems that are susceptible to *cyber*-attack. This susceptibility also characterises socio-economic organisations that provide society, in ICT-dependent ways (information and communications technology, ICT), with vital services such as administration, telecommunications, energy, transport, and financial services ("Critical Information Infrastructures", CII).

While in the engineering sciences conventional risk and vulnerability analyses of complex systems have largely focussed on problems of technological safety, research on ICT systems is also concerned with the security of critical infrastructures *vis-à-vis* information- and network-based threats and attacks. Threat thereby means intentional, including preparatory, individual or organised social action directed against the integrity and availability of data, ICT systems and infrastructures. Violation of ICT security, on its part, usually entails consequences that go far beyond the technological and operational problems of systems engineering and management. When successful, *cyber*-attacks tend to cause enormous damage to the public economy. In addition, ICT security management can be very costly, while the success of security technologies and strategies often remains uncertain. From the economic perspective, this situation requires various basic approaches to be taken to improve ICT security. These include an improved understanding of the far-reaching, highly interconnected consequences of ICT security incidents (systems analysis), methodologically sound measures of ICT security risk (quantitative risk analysis) as well as measures of the effectiveness and cost-efficiency of the ICT security management (quantitative risk assessment).

The present paper provides selected theoretical and methodological perspectives on ICT security management and some of its basic economic requirements and implications. It is in part adapted from earlier contributions by the author to security and risk management theory [1], [2].

II. ICT and CII Systems Analysis

From the methodological point of view, two basic questions arise in the economic analysis of ICT and CII security risk management. First, how much effort does modern society have to invest into CII security provisions to keep potential losses from *cyber*-attacks within the boundaries of acceptable risk? Secondly, how can potential losses be measured or estimated, given the fact that the infrastructures under attack are normally highly interconnected and the consequences of an attack are widely distributed and uncertain?

A suitable conceptual and methodological framework for attack consequence analysis is provided by modern systems research. In the social and engineering sciences, systems-theoretical concepts and methods have been developed and applied primarily to model, design and control complex socio-technological interactions. Their suitability for interdisciplinary research rests on their capacity to describe adequately the structure and behaviour of both physical systems and the "intentional" attributes of social action such as interests, preferences and purposes. Accordingly, conventional engineering approaches to systems safety can be directly extended to cover aspects of ICT security by combining, in systematic ways, models of systems behaviour, quality management, robust systems design, and failure response and recovery with threat and vulnerability analyses and strategies of ICT security management.

Using the conceptual frameworks of theoretical and applied systems analysis, four key approaches to ICT infrastructure protection can be identified. The first is the application of models and methods of operational research (OR) such as exercises, simulations, games of strategy and scenarios to information-based social systems. OR experiments and scenario techniques are particularly suitable for exploring the vulnerability of information infrastructures

under realistic conditions, especially incident response and recovery of large-scale information-based systems under computer network attack. The results obtained from OR experiments can be further analysed and refined by combining them with conventional fault tree (event tree, etc.) representations of IT security incidents. Scenarios established in this way can provide a detailed overview of possible incidents across the entire threat spectrum, which, even in the absence of probability estimates, admits realistic predictions of the effects particular incidents and responses to them will have. Alternatively, OR experiments simulating IT security threats can be carried out to generate the statistical data-bases required for the design and optimisation of risk and security management strategies.

The second key approach is based on the concept of systems vulnerability adapted from industrial safety engineering. ICT systems and infrastructures are said to be vulnerable to failures (risks, threats) to the degree to which they (will likely) lose their operability if one or more of their components fail (a safety or security incident occurs). Related concepts are the robustness, resilience, reliability and availability of systems. Vulnerability analysis is concerned with the interactions between system components, and the interrelationships between system design and function. Once combined with suitable OR techniques, vulnerability analyses can provide insight into the overall performance, degradation or robustness, of large-scale information infrastructures in the event of an IT-based attack. The political and economic significance of such insight would seem obvious.

The third key approach to the security of ICT systems and infrastructures to be included here elaborates upon modern business process simulation techniques. The significance of these approaches arises from the fact that the thrust of the economic damage caused by *cyber*-attacks is very likely not triggered by the physical destruction of the ICT systems themselves. It will arise rather from the delay or disruption of remote and ramified, computer-based economic transactions that are affected, for instance, the economic consequences of the disruption of international logistic chains, financial transactions or e-commerce.

Finally, advanced approaches to theoretical and applied risk analysis must be included here. ICT risk research is broadly concerned with the causes, frequency, consequences and management of damage that may arise from the operation of ICT systems. The public policy implications of IT security management (economic costs, limits of acceptable risk, comparative risk assessments, etc.) often require quantitative risk assessments. These could in principle be obtained using statistical methods and familiar models of rational planning and decision making under risk. Unfortunately, ICT security risks involve threats of purposeful, covered action rather than measurable system failure rates with recurrent, identifiable causes. Primarily because of this dependence on strategic as opposed to probabilistic uncertainty, however, ICT security risks are hard to assess in statistical terms.

III. Economics and Security Risk Assessment

In view of growing threats to public ICT security and increasing budgetary restraints, risk management in government, industry and business must be both effective and cost-efficient. To this goal, recent advance in the econometric and operational sciences must be exploited to develop and apply a generic quantitative risk assessment methodology as a security planning and management device to protect public infrastructures and large-scale ICT systems. The concept of quantitative risk assessment thereby means the coherent intrinsic, or “fair”, pricing of risks. It implies considerably more than risk measurement in the sense of statistical risk analysis (“intrinsic” refers to risk quantification within a given accounting system rather than to risk prices extrinsically determined by the market for risky goods or services). It is evident that the practical use of a coherent approach to measure the intrinsic value of any given risk would be considerable. It could help to determine, in a realistic and systematic way, the amount of risk reduction achieved per euro invested in technologies and management efforts to prevent safety and security incidents in CII, or mitigate the damage arising from such incidents. As for security management, this is exactly what is otherwise known (though badly missing in practical applications) as calculating the Return on Security Investment (ROSI).

IV. Quantitative Risk Assessment

Risk management has long been suffering from the fact that risk is an elusive concept. Correspondingly, existing methods to assess risks and risk reduction measures tend to be ambiguous and controversial, if not manifestly inconsistent, for one of the following two reasons. They are either *ad hoc* rather than systematic, meaning that they lack theoretical coherence, or hard to operationalise. In either case, they may not provide the reliable information decision makers need to solve their problems.

The following situation provides an instructive example. Although attempts have been reported to estimate probabilities of (e.g., terrorist, *cyber*-war) attacks in order to quantify security risks [3], [4]., the probability of such an event is generally not a well-defined concept, at least not in the strict sense of mathematical model building. In fact, security incidents imply planned, purposeful human action and, therefore, are quite the opposite of random events. When modelled in mathematical terms, they have to be conceptualised as “games of strategy” rather than “games of chance” [5]. To the extent that a terrorist´s plan of an attack is unknown to the operator of the system threatened, the attack (time, place, technology employed, etc.) involves uncertainty, but not probability. Accordingly, ICT security incidents must be modelled by “What-if” scenarios (uncertainty arbitrarily removed, probability of occurrence put equal to 1) and concentrate on their probabilistic damage consequences. The scenarios are based on the assumption that effective protection technologies will constrain the actions of the attackers and thus help to mitigate the consequences of the attacks or prevent them entirely.

Security risks are accordingly conceptualised as probability distributions of the amounts of loss or damage to be prevented or incurred in a security incident. In other words, "What-if" scenarios can be used as reference cases relative to which the probabilistic attributes of security incidents can be analysed in a definite way. For example, whether a *cyber*-attack may be successful or not may depend on whether the ICT assurance technology built into the system under attack has been updated recently or not – the classical case of risk reduction in the sense of incident consequence mitigation by means of physical protection.

V. The Econometric approach to risk assessment

Advance has recently been made on the basis of novel methodological approaches to economic utility theory and the statistical foundations of quantitative risk assessment. The methodology for optimal, cost-efficient risk and security management employed in these approaches involve concepts of "generalised expected utility" that have been demonstrated to be able to admit coherent, explicit numerical representations of risk preferences, while accommodating basic empirical, individual and social attitudes towards risk. Most importantly, however, they have proven to be sufficiently simple for operational use in applied risk research. In this context, it is also important to note that "utility" has nothing to do with naïve views of "degree of individual satisfaction", "desirability" and the like: it is a technical term simply meaning a behavioural risk preference score.

The core concept of quantitative risk assessment is the pricing of risk. Risks can be formally represented as probability functions $f(x)$ of the likely gains or losses x (in monetary terms or otherwise) obtained from safety or security incidents with uncertain consequences. A real number $c(f)$ is called the *certainty equivalent of the risk* $f(x)$, if $f(x)$ and the certain amount $c(f)$ of gain or loss are indifferent in preference terms from the perspective of the planner or decision maker. The certainty equivalent of a given risk can accordingly be viewed as the fair, or "intrinsic" price of that risk, considering that f and $c(f)$ are equal in preference. In practice, it can be explicitly calculated for every given probability function f.

Fig. 1 illustrates important realistic features of the quantitative account of risk assessment. One such feature is the marked deviation of the fair price (curved line in Fig. 1) from the probabilistic mean value of a risk (straight line), thus expressing widely observed, non-neutral human attitudes towards risk. Another feature is the capacity of the present approach to accommodate patterns of variability of risk attitude across various dimensions of risk. Finally, this simple and straightforward concept of intrinsic pricing of risks provides a powerful management tool, admitting direct assessments to be made of the effectiveness and cost-efficiency of planning and decision-making under risk.

VI. Effectiveness of ICT Security Risk Management

Real systems can generally be assumed to be operated with larger or smaller risk management effort. Two risks f and g linked to the effort aiming to mitigate them can be estimated, considering the likely consequences of security incidents affecting any such system considered. Furthermore, the risk prices $c(f)$ and $c(g)$ of the risks with and without appreciable risk management arrangements, respectively, can be calculated and compared. For example, the comparison $c(f) \geq c(g)$ shows the effectiveness of the measures planned or taken to reduce the risk g to f. In this example, the price difference $c(f) - c(g)$ is positive. It measures the Return on Security Investment (ROSI) that can be gained when the system changes from the risky state g to the less risky state f. If, on the other hand, the difference $c(f) - c(g)$ is small or even turns out negative, the risk management proves ineffective.

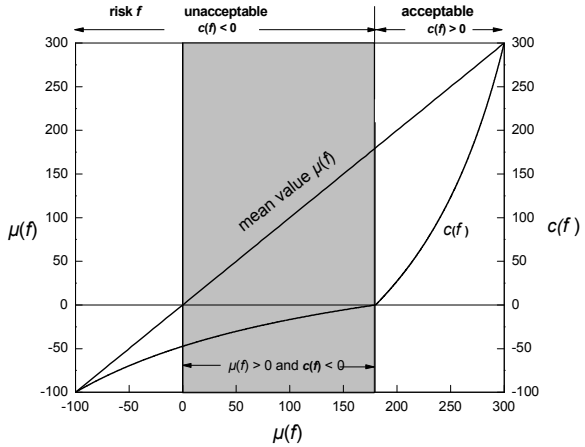

Fig. 1 Certainty equivalent $c(f)$ and mean value $\mu(f)$ of probability function f. Example after [1].

VII. Cost-Efficiency of Security Risk Management

Let $k(f, g)$ be the cost incurred by security managers to reduce the risk g to f. The ratio of ROSI to cost of the security arrangements made gives the amount of risk reduction per euro invested. It measures the cost-efficiency of the risk reduction achieved. Risk management is optimal if for given "*status quo* risk" g, the target risk level f is chosen so that the cost-efficiency ratio is at maximum within a given set of alternative risk mitigation choices.

A hypothetical numerical example is shown in Fig. 2. In the example, q is the rate at which a firewall technology detects hacker attacks and malware programmes of given types directed against a privately owned computer network. Without the firewall in operation, x is the amount of economic damage incurred or prevented with probability $g(x)$ (e. g., Euros, in monetary terms) if an attack occurs. The equivalent number of Euros saved or lost increases from the *status quo* with $c(g) = 0$ and $q = 0\%$ to $c(f)$, if money is invested to adjust q optimally. Clearly, it reaches its maximum for $q = 100\%$. The function $k(q)$ gives the buying price and operational cost (per unit time) of the firewall system. It shows the typical effects of "economies of scale" and increasing and decreasing marginal costs known from managerial economics [6]. The fact that for large q-values the k-curve is steeply rising results from disproportionate in-

creases in expenditure for large values of q. High levels of security may then become unaffordable. The cost-efficiency ratio $c(f)/k$ reaches its maximum at approximately q = 22% in this example. Such a low value of the cost efficiency ratio means that the firewall technology is very expensive, while the network-based applications involved are of moderate or little economic value.

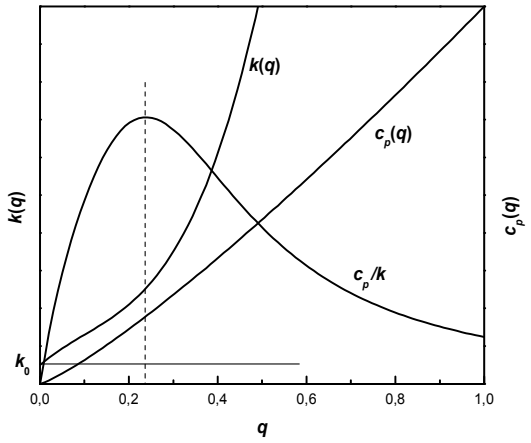

Fig. 2 Risk price $c_p(q)$, cost $k(q)$ of security technology and cost-efficiency ratio c_p/k as functions of the attack detection rate q achieved

The difference between an ideal optimum at q = 100% and another, arguably more realistic one at q = 22% reflects the impact of high costs of risk reduction on security: if risk management is expensive, the most efficient solutions may be ineffective, and conversely, if risk management is affordable, security solutions may appear cost-efficient, but ineffective. Unfortunately, this discrepancy between what is desirable and what is affordable in security corresponds to all too realistic, virtually daily experience. As the example demonstrates, however, this discrepancy can at least be understood very much in detail in systematic, quantitative ways, using a suitable, quantitative approach to ICT security economics.

VIII. Process Modelling and ICT Security Management

Safety and security planning in large-scale CPT and CII systems can be made very effective by combining scenario-based computer simulations of systems and processes (e. g., Monte Carlo simulations) with numerical estimates of damage probabilities in simulated security incidents. The effectiveness and cost-efficiency of technical, organisational and procedural risk management provisions can thus be assessed quantitatively prior to their implementation. Risk and security management as well as attacks can be modelled as processes. A process model may, in turn, help to identify all the relevant risks attached to a process itself or any further actions triggered by it. In ICT security analyses, it is therefore important to develop a generic process model of attacks against the systems considered. This can be done, in principle, using the systems modelling and simulation techniques indicated above.

IX. Conclusion

From the economic point of view, quantitative risk assessment is central to ICT and infrastructure security management for at least two reasons. First, disruptions of complex systems tend to affect large and diverse areas of public life, simultaneously involving many different individual needs, interests and preferences. Secondly, optimisation of risk management under constrained resources must accordingly be based on quantitative cost and cost-efficiency estimates as well as trade-offs between competing values and preferences. The problems arising here are highly significant for key risk management activities such as resource allocation, the prioritisation of competing or even mutually exclusive management goals, optimal planning and decision-making, and effective and cost-efficient organisation. While these problems have been widely discussed in the classical economic and management literature, risk-based solutions are still rare which are methodologically coherent (i.e. systematic rather than *ad hoc*), operational and broadly applicable at the same time.

As planning and decision support devices, the methods outlined above are suitable for government agencies and public safety and security services, operators of large-scale systems and for the security management of public infrastructures. They offer advantages especially for cost-efficient ICT security planning and procurement.

References

[1] G. Geiger, "Economic Perspectives on Security Management," *European CIIP Newsletter*, vol. 8, No. 1, pp. 17–19, March – July 2014.

[2] E. Petzel, R. Czaja, G. Geiger, and C. Blobner, „Does lift of liquid ban raise or compromise the current level of aviation security in the European Union? Simulation-based quantitative security risk analysis and assessment," presented at the 22nd SRA-E Conference, Trondheim, NO, June 17–19, 2013.

[3] T. Aven and O. Renn, "The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk," *Risk Analysis*, vol. 29, pp. 587-600, 2009. DOI 10.1111/j.1539-6924.2008.01175.x.

[4] G. G. Brown and L. A. Cox, "How probabilistic risk assessment can mislead terrorism risk analysts," *Risk Analysis*, vol. 31, pp. 196–204, 2011. DOI 10.1111/j.1539-6924.2010.01492.x.

[5] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior,* 2nd ed. Princeton, NJ: Princeton University Press, 1947.

[6] C. Thomas and S. C. Maurice, *Managerial Economics*, 10th ed. Boston, MA: McGraw-Hill/Irwin, 2010, ch. 10.