Applying Real Options Thinking to Information Security in Networked Organizations

Maya Daneva
University of Twente, Centre for Telematics and Information Technology
P.O. Box 217, 7500 AE Enschede, The Netherlands
m.daneva@utwente.nl

Abstract An information security strategy of an organization participating in a networked business sets out the plans for designing a variety of actions that ensure confidentiality, availability, and integrity of company's key information assets. The actions are concerned with authentication and nonrepudiation of authorized users of these assets. We assume that the primary objective of security efforts in a company is improving and sustaining resiliency, which means security contributes to the ability of an organization to withstand discontinuities and disruptive events, to get back to its normal operating state, and to adapt to ever changing risk environments. When companies collaborating in a value web view security as a business issue, risk assessment and cost-benefit analysis techniques are necessary and explicit part of their process of resource allocation and budgeting, no matter if security spendings are treated as capital investment or operating expenditures.

This paper contributes to the application of quantitative approaches to assessing risks, costs, and benefits associated with the various components making up the security strategy of a company participating in value networks. We take a risk-based approach to determining what types of security a strategy should include and how much of each type is enough. We adopt a real-options-based perspective of security and make a proposal to value the extent to which alternative components in a security strategy contribute to organizational resiliency and protect key information assets from being impeded, disrupted, or destroyed.

1. Introduction

Participating in value webs and sharing common resources has become a new major source of business success for many companies. Value webs are networks of independent, or nearly independent, businesses who work together to deliver value for a customer. An example value web is the business network of WalMart Stores Inc. who collaborates with a large number of non-U.S. companies and gives them direct access to the American market [CHA02]. The great extent of sharing in a value web and the new risks arising because of sharing are leading to the design of a wide range of policies and procedures that ensure secure sharing. For networked organizations, the ability to securely share information became an essential factor affecting the speed of business and the speed of developing partnerships [DYN05]. Moreover, it may even condition if some partnerships can happen at all.

Making the processes of secure information sharing work effectively and in a coordinated fashion at both intra-organizational and inter-organizational levels, however, does not come cheaply and is a bumpy road. It is, in fact, a multifaceted challenge into which companies throw sizeable budgets and resources each year. For example, while collaborating in a value network, each partner company's security decisions impact the overall security of the shared business process and data environment for the myriad of suppliers and channel partners who this company interacts with. Yet, each partner must be provided with secure sharing capabilities to make the network business work. Moreover, when partner companies externalize their operations and contribute part of their own process and data environments to the shared pool of resources, their environment's security arrangements may be very different, opening virtually a swing door between partners through which anything can move. That is, the least secure network partner exposes the entire network business at risk.

Existing practice confronts most of these challenges by applying the concept of security governance [CAR04]. It helps companies (i) take an economic perspective of security, (ii) set up decision making processes for security spendings with business drivers in mind, (iii) develop a strategic information security

CTIT Technical Report TR-CTIT-06-11
Centre for Telematics and Information Technology, University of Twente. Enschede, The Netherlands, 2006.

architecture and integrate it into a security program, and (iv) enforce the deployment of qualitative or quantitative approaches to systematically assessing how vulnerable and resilient business networks are to a partner's security failures [DYN05]. To make informed decisions on security budgets and resource allocation, at network business level, the partners have to define what shared information responsibilities they have to each other. They have to get clarity on who pays for security, who suffers in case of failure, who is liable for security being compromised [AND01] as well as who should manage security, what should be managed, where it should reside within the network, and how much should be spent on securing shared information assets. At network partner level, the shared responsibilities for information security must be translated into:

- what types of security and how much of it to include at each partner company, and
- how to compose a security architecture in the face of only partially known interdependencies between the security mechanisms at network level and the ones at partner level [LAK05].

These questions confront every day many security strategists and the answers to each question may well include a variety of options whose viability has to be compared and prioritized. Yet, traditional cost valuation methods used in software engineering in the past 40 years come short when applied to security decision-making as they do not account for specific aspects of organization's security requirements.

This paper has the objective to look into the facets that make up the problem domain of applying quantitative cost-benefits analysis methods to cross-organizational security, to assess the applicability of one promising approach, namely the real-option concept [BEN02], and to propose a research plan to improve risk-based cost-benefits-analysis practices. In Section 2, we provide a rundown of what is observable in the state-of-the-art literature and practices in regard to decision making on components of security strategy. We also make the case that security professionals need a more risk-and uncertainty-focused view of this topic. Section 3 explores how security strategy development can be seen from a real-options perspective. In Section 4 we derive research questions from the business and research challenges that we identified in the previous sections. Section 5 summarizes our contributions.

2. Current State-of-the-Art Practice in Security Decision Making

Since the concept of security has so many interpretations, it is useful at the outset to clarify our interpretation of the term. We refer to information security as to the variety of actions designed to ensure the following aspects of sharing key information assets among partners in a value network: (i) confidentiality, which means protecting shared information assets from unauthorized users, (ii) availability, which means providing authorized users with shared information when and where needed, (iii) integrity, which preserves the validity and accuracy of data of key information assets of both the networked organization and its partner companies, (iv) authentication which means making sure that the users of shared information are the ones who they claim to be, and (v) nonrepudiation, meaning that authorized users of a common information asset can not deny their using this asset. This definition covers a wide range of information assets, for example, shared data, common data bases, inter-organizational coordination support systems (e.g. data warehouses, enterprise resource planning systems), and interfaces between shared coordination support systems and each partner company's systems. It is this definition that we use in our research on security decision making in value webs.

In what follows, we summarize the findings from our survey of experience reports [ABE05, CAV04, CIS02, COY04, DEL06, ERN05, GAR05, GAR06a, GAR06b, GAR06c, BER04, BRO05, GOR06, VIS02, VAU02, CAR04] on the investment, budgeting, and resource allocation decision processes that are currently prevailing in large and midsized businesses with respect to security. The large businesses we surveyed are organizations from the Fortune 500 list of US companies (http://money.cnn.com/magazines/fortune/fortune500/). The midsized businesses we looked into are partners at either side of the value chain of the Fortune 500 organizations.

Our survey investigated a variety of questions among which: (i) what drives the spendings on security in business networks, (ii) how decisions on spendings are made, (iii) how resilient business networks are to security being compromised at partner's level, and (iv) what risk-based analysis techniques are used to support security decision making, (v) what factors are accounted for in these analysis techniques.

The literature sources consistently indicate that, within the past few years, there have been four major drivers setting directions to security decision-makers in organizations:

- Government and industry-sector-specific regulations, for example the US Public Company Accounting Reform and Investor Protection Act of 2002 (better known as Sarbanes-Oxley), and the Basel II Accord for international bancs, respectively.
- Standards, for example the ISO 17799 standard, and best practice models for IT security such as ITIL and COBIT [OGC00,BON05].
- Business risks and security requirements of the business network that an organization has or wants to join. For many companies, information security is a qualifier to be in business, for example, big companies like Motorola, Ford and General Motors require their partners or providers have appropriate security practices.
- Urgency to invent opportunities in the midst of security breakdowns that incur monetary damage, corporate liability, and loss of credibility [CAV04].

These sources of pressure to organizations necessitates for them to (i) establish security governance and (ii) make security a component of organizational resiliency. Security governance is concerned with setting directions, establishing standards and principles, and prioritizing investments, all needed to support the ability of a company to create a variety of new options as compelling alternatives to outdating security strategies. Furthermore, resiliency means the ability of an organization to withstand discontinuities and disruptive events, to get back to its normal operating state, and to adapt to ever changing risk environments [HAM01]. From resiliency viewpoint, security in a networked business context reflects the capacity of the networked business to reinvent itself before circumstances force it to. Both security governance and organizational resiliency imply for companies that they should manage their security fundings from an economic perspective [AND03,DYN05,GOR03,GAR06c]. That is, a firm should invest resources into security projects up to the point at which "the last dollar of information security investment yields a dollar of savings" [LAW06]. Indeed, we observe a shared agreement in the literature that increasingly large number of organizations assess in cost-benefit terms what they spend on security projects. As today's business practice indicates, fundings for information security projects are thought of as capital investments by many corporations and, in this context, the economic perspective is self-intuitive to security decision-makers [CISCO04]. Other companies see spendings on security as an operating expense, that is, a sunk cost that the company can not recover. For them, spending on security is part of the price paid to be in business [DYN05]. Regardless how security fundings are accounted for, experience reports indicate that when companies collaborating in a value web view security as a business issue, risk assessment and cost-benefit analysis techniques are necessary and explicit part of their process of resource allocation and budgeting.

Economic approaches to information security include the Return on Investment for Security (ROSI) model [SQ03], the Net Present Value (NPV) model, the Annualized Loss Expectancy method, the Security Attribute Evaluation (SEAM) method [BUT02] and the Cost Effectiveness Analysis. Each of these takes a specific form of a cost-benefit analysis supposed to serve as a basis for making decisions on the size of an investment or of a capital budget. Experiences indicate that this analysis is a sound basis for determining security expenditures [LAW06,CAR04]. In practice, though, it is rarely achievable to set up a budget decision making process that rests solely on results of rational economic models due to the fact that both the cost and benefit components of the cost/benefit ratio often are too difficult to estimate in the context of security programs [LAW06 and more]. To keep cost-benefit analysis practical, companies take modified approaches to planned security fundings which fall into three categories: expert judgments, algorithmic estimation, and estimation by analogy.

The first class of models relies on accumulated experiences of a team of experts coupled with benchmarking data provided by an industry trend researching firm, like Gartner, Aberdeen, Vista, Delloite & Touche, Ernst & Young. Consolidation of expert judgments may be facilitated by external risk management consultants.

The second class of models relies on the application of a set of mathematical formulas (mainly from the field of financial accounting) to quantify either the cost component or the benefit component of the cost-benefit relationship. While cost elements appear to be easier for companies to get in quantitative terms, benefits may be only partially quantified. A complete quantitative assessment of expected benefits should include data characterizing the scope of company's potential losses (that is, the business impact) from security being compromised and the probability of such compromises. For example, Fidelity is using a cyber threat matrix that positions in a four-quadrant grid the probability of a compromise versus its business impact [DYN05]. Another example is Motorola's quantitative approach to business impact analysis of security lapses that is a part of their security governance concept [BRO05]. However, most organizations barely have valid data collected for this purpose. In practice, for example, security decision

makers in some companies quantify the probability of security breaches without calculating the estimated damage to business due to security being compromised. Other companies' practices include quantifying the estimated potential benefits from preventing those security breaches which translate in business risks without quantifying the probability of these breaches. Yet, in third group of companies, budget decision making rests on qualitative considerations of both the business risk exposure and the probability of such risk's materializing. When elements of the cost-benefit relationship are quantified only partially, decision makers tend to compare potential incremental benefits to incremental spendings (on a variety of security types). Such a comparison results in qualitatively categorizing the payoff from the spendings as high, medium, and low.

The third class of models, estimation by analogy, suggests periodic reevaluation of threat levels, then, adjustment of the security budget of the previous year to derive the next year's one.

Literature indicates, however, that no matter which method is used to get quantitative input into security decision making processes, the size of the budget and the resource allocation decisions are also influenced by a number of organization-specific factors:

- the industry sector the company operates in; for example, highly regulated companies (e.g. the ones from the pharmaceutical sector) or high-risk-visibility companies (e.g. the financial services sector and telecoms) usually spend more [CISCO03].
- the risk affinity of the company and the Chief Security Officer (CSO),
- the position of the organization in the value web; for example, the relationships between a larger final assembler and smaller suppliers are often based on asymmetric cooperation where the smaller companies are highly dependent on the larger companies.
- the level of participation in the value web; how much sharing happens is proportional to how much it would cost to secure it [CISCO03].
- the transaction values executed over vulnerable coordination technology infrastructures; for example employees of partner companies who get hooked up to shared resources by using wireless devises pose extra risk to the networked business.
- the level of maturity attained in security practices. Organizations with mature security processes often spend less on security [GAR06a].
- the level of threat within the organization (for example due to legacy systems developed for use in isolated locations at times when security was not a preoccupying concern),

Our review and analysis also identified circumstances when making a business case for information security comes second to other factors. One example is the case when many IT organizations are using Sarbanes-Oxley as the justification for expenditures that they wanted to make before Sarbanes-Oxley was even an issue [GAR05]. Another example is the case of midsized businesses [GAR06b]. They are persuaded by the use of security solutions by same-size and same-industry peers (especially in highly connected industries such as financial services and healthcare). They are also influenced by the advice of resellers. Auditors and regulators are also becoming an influence on security spending by midsize businesses. Yet, third (and critical!) circumstance leading to upgrading already approved security budgets is a security breach that directly translates in a business risk meaning (i) lost market share, (ii) protracted earning slungs, and (iii) the need for wrenching turnarounds. Such cases indicate a correlation between the amount of expenditure added to the original budget and the severity of the breach [CISCO03]. In severe security breaches, intangible costs of security being compromised may be higher than tangible costs.

The analysis of literature sources was used to understand what are the foundations of a solution that would effectively help decision-makers use credible quantitative input to their budgeting and resource allocation processes. To the best of our knowledge, however, the suitability of quantitative (and partially quantitative) approaches to decision making processes in inter-organizational settings has not been investigated yet. A few authors [AND01,GOR02,GOR03,CAV04,CAR04,GAR06c] have investigated the use of these groups of economic approaches at intra-organizational level. They found that, regardless how budget was treated (as a capital investment or as an operating expense), economically, it pays off to wait for actual security breaches to occur before all the money available for security projects are spent [GOR03]. What they indicate to work well was to first use a NPV model or a ROSI model, and, then, to complement it with an analysis of (i) the dynamic impact of security risk, (ii) the flexibility inherent in most strategic information security investment decisions, and (iii) the dependencies and sequencing constraints typically associated with the implementation of security strategies.

The current three classes of budget estimation models we discussed above do not properly account for these aspects of the decision making processes that today's security professional are confronted with. The inadequate decision-making support these methods offer is due to their built-in assumption that the future business development follows a fixed path [AMR99]. This implies that the methods are only good at capturing the risk of uncertainty, namely the probability that the actual returns would be lower than the forecast. They, however, ignore the rewards, that are the possibilities that the actual returns may be much higher than the forecast. Security funding decision-makers who rely on these methods inevitably fall into the trap of underestimating the potential value of their security projects and, as a result, do not invest enough in uncertain but highly promising opportunities. For example, a business case for information security may well result in a negative number according to a NPV-based appraisal, but it may provide the option to launch other value-added services for secure sharing of dealers' process environments or client interactions in the future.

Yet, networked organizations must be able to make timely strategic choices with reasonable analysis of the information available about security risks and their business impacts. The questions of what types of security a strategy should include and how much of each type should be there must to be answered while finding a way to both recapture the rewards disregarded by the conservative models and protect against the considerable risk of pursuing highly uncertain projects.

Drawing on the results of our literature review, it seems timely and appropriate to consider incorporating options thinking into the decision processes for cross-organizational security spendings. The next section provides a quick rundown of the concept of real-options and explains why we think it best serves the needs of today's networked business' information security decision makers.

3. Real Options Analysis for IT Decision Support

Real Options Analysis [CHI98, KOG03] was first developed as a decision support technique in the area of capital investments. The concept of real means adapting mathematical models used to evaluate financial options to more-tangible investments. Since 1999, most notably through M. Amran and N. Kulatilaka [AMR99], this concept has found its way into the area of appraising IT investments. The core of the real option analysis for IT assets consists of:

- the identification and the assessment of optional components in a project and
- the selection and the application of a mathematical model for valuing financial options that serves to quantify the current value of choosing these components for inclusion at a later time.

Optional components are project parts that can either be pushed ahead or pulled out at a later point in time when new information becomes available to the decision-makers. The option, therefore, is the right but not the obligation to spend a budget or put resources on a project. For example, it is often possible to first implement a data mart, and then later decide to implement a data warehouse.

Next, the decision maker is supposed to choose a model specifically designed for valuing an option and to customize it to reflect the risk aspects of the company's context. For example, the calculus-based Black-Scholes-Merton model or any of the algebra-based (lattice) models by Cox, Ross or Rubinstein [BEN02]. What is important for the decision-maker, however, is to characterize the organization's context in a way analogous to that a financial security could be. The idea behind the customization is to provide the company to assess its simple view of valuation to one that more closely matches the manner in which the company operates.

Insights from practice [AMR99,KUL01] indicate that the real-options-analysis technique enables companies to confidently answer both tactical and strategic questions regarding resource allocation to IT projects. For example, Merck used it to assess the economics of their phase-by-phase ERP implementation tactic in the current quarter to meet requirements in a future quarter. If the initial ERP investment was found to work out well, then Merck's management team could exercise the option to *expand* its commitment to the ERP strategy. Merck noticed that business requirements and opportunities changed in ways that either increased or decreased the importance of what a specific ERP implementation stage delivered. By using real options, Merck's ERP Steering Committee found themselves better able to recognize and avoid throwing resources in stages that no longer have a worthwhile payoff.

The Merck network also used real options to prioritize the ERP package components to implement, such as whether it is more profitable and less risky to start with the HR and the Financial Accounting modules and then to continue with Supply Chain than to get in first the Supply Chain modules and, then, the rest of the ERP application suite. By using the real options concept, the Merck business network created a

situation in which both Merck and their business partners benefited from the upside potential of a shared ERP system while controlling its downside risks. As a quantitative analysis technique, a real-option-based approach is without peer at providing such a type of decision support.

Another example is Amazon.com [KUL01] who focused substantial investments on the development of its secure information infrastructure, customer base, and brand name for its core book business. By doing so, Amazon created a portfolio of growth options to extend its operations into a variety of new businesses, for example in the toy segment due to a partnership with Toys "R" Us, in the segment of new-car-buying services due to "Cadirect". It also co-branded sites with a number of value webs to provide the capability of easy pick-up through US Post Office or FedEx.

Real-options thinking seems suitable for information security strategists because of the field's high stakes and tremendous uncertainty. We think it is worthwhile exploring the use of the real-options concept as a vehicle for security cost-benefit analysis because:

1. Unlike traditional techniques, it comprehends uncertainty and it responds to the dynamics inherent in today's business that drives security requirements and the active decision making required for a cross-organizational security strategy to succeed.
2. It provides interested stakeholders of security projects in the context of a spectrum of possibilities rather than in the context of a single or three (the best, likely or worst case) discrete set-ups, and it facilitates fine-tuning of operational tactics as organizational circumstances unfold over time.
3. It allows managers to make decisions while keeping in mind the trends in their business sector.
4. It allows event-driven incremental expenditures while focusing on organization's critical assets essential to accomplish its mission.
5. It rests on the understanding that not all information assets are of equal value.
6. It allows stakeholders to rationally decide what level of risk the network as a whole, and the parties of the network are willing to assume with respect to the assets they share.

4. Thinking of Security in Terms of Options

Taking an options perspective of information security decision making is not merely applying a new class of mathematical models but re-framing the discussion about information security strategy and spending and resource allocation decisions in terms of options. The first step in re-orienting our way of looking at inter-organizational security strategy, then, is to identify the real options that exist in security investment decisions. Then, we will describe how practitioners can incorporate options thinking into their security strategy evaluation and budget decision-making processes.

Drawing on our literature review, we identify that real options can take a number of forms (Table 1). In Table 1, each option is analogous to a financial option. For example postponing the implementation of a security mechanism is analogous to deferring a financial option.

Table 1: Description of Options

Option	Description
Postpone	Waiting to determine whether to invest in a security mechanism, without imperiling the potential benefits [GO03].
Abandon	Keeping security project resources relatively easily redeployed if project needs to be cancelled.
Scope up	Increasing amount of security mechanisms if uncertainties are resolved favorably.
Scope down	Cutting back on security mechanisms if uncertainties are resolved unfavorably.
Outsource	Deciding on managed security services if service gap is manageable and security costs are reduced [WHI05,MAS06]
Switch	Keeping open to chose alternative security technologies and managed security service providers [WHI05]
Stage	Rolling out a security solution incrementally, slowly expanding to user populations [ABE06, GAR06c]
Growth	Taking advantage of future, interrelated opportunities due to achieved compliancy with SOX or ISO [DYN05].

Each of these options – postpone, abandon, scope up, scope down, outsource, switch, stage, and growth - owes its value to the flexibility it gives the networked organization. Flexibility adds value in two ways. First, management can defer a security investment: because of the time value of money, managers are better off paying the investment cost later rather than sooner. Second, the value of the project can change before the option expires. If the value goes up, decision-makers are better off. If the value goes down, they are no worse off because the do not have to invest in the project.

In what follows, we provide a list of hypothetical examples of the most common types of real options as applied to the cross-organizational information security context for specific purposes, like achieving better timing for an investment, building a small set of security mechanisms that is expandable rather than building a larger set, or learning how much security is needed to assure a certain probability of protection level:

Timing Options. Suppose a big supply chain network considers postponing a security investment until they learn more about the impact of a security breach on partner companies' side. The network needs to know the value of waiting to build the security mechanisms as well as the value of outsourcing security processes until a security threat becomes better understood. It may be that the risk avoided by waiting to invest has a greater value than the cost savings due to buying managed security services from an outsourcing partner. The latter comes from the fact that using managed security services is inherently risky as the client company has little control when quality of service is poor [MAS06].

Staging Options. Suppose a company has to participate in a number of business networks involving partner companies with various levels of trust and needs for cooperation. The company looks for a cost-effective security technology configuration to support a dynamic collaboration environment [DYN05]. The top security management team is reviewing a proposal to implement a data access model that presents semantically consistent view of shared information in a secure way to all partners. The viability of access schema hinges on its coupling with a very effective security model for outside protection from unwanted parties seizing access to any of the partner company's access profiles as well from each partner company's seizing control of other company's access profile. The proposal calls for a full, half-million-dollar rollout at all locations over the next ten months. But the business benefits of the project remain uncertain. The company has the option to invest in the new security mechanisms in stages rather than all at once. The conclusion of each stage will in turn provide further options - for continuing, for postponing, or for abandoning the effort. All these options add value to the proposed project.

Learning Option. Suppose a midsized supplier company joins a major industry leader's network. The company and its partners plan a number of security mechanisms to build a secure foundation for information sharing. Before these mechanisms are actually built, the company's executives can not tell which one will be increasing the company's revenue through e-business and which one will bring an increase in the productivity of the own employees. The company acknowledges that security lapses are management failures more than technical failures and it does not want to get dependent on partners' security management practices over which it has no control. The company made earlier experiences that sophisticated security technologies often can be rendered inefficient due to poor identification of critical information assets, sporadically executed procedures, desperately implemented islands of security technology or lax employees' attitudes towards security within the walls of the own employer. But the company's security decision-makers have an important learning option. They can implement a security mechanism on a limited number of locations in selected business units and then refine their investment and business continuity plans based on what they learn. They can, for example, roll out the most cost-effective security mechanism network-wide worldwide or nationwide and give it a large budget while putting the other - less cost-effective - security mechanisms into where is needed.

This list is illustrative, but it does not reflect the way options actually occur in the realities of cross-organizational security strategy. In a dynamic business environment, an option rarely is spotted in isolation. Instead, it arises as part of a complex bundle. In deciding to implement a new security mechanism, for example, a company will need to weigh the value of the initial timing and staging options, but it will also need to look ahead to the growth, outsourcing, and abandoning options that this mechanism would create. Moreover, one option can take different forms. A staging option, for example, may lead to increased revenues and thus might also be viewed as a growth option. Much of the challenge in taking an options approach to strategy lies in identifying the full set of options security professionals have, disentangling them from one another, and deciding which are the most valuable.

The above examples do not suggest decision-makers use a real-option-based approach as an alternative to the NPV method. In fact, we support the understanding that real options and conservative methods are not mutually exclusive but complementing each other. If security decision-makers see their strategy as being implemented in a security architecture made up of both mandatory and optional components, they also are aware of the fact that the proportion of a security project's value contributed by each component will vary according to the degree of uncertainty associated with the project. If estimation is done in the early phase of a security project, then, due to the uncertainty, the NPV will be expected to be low and the real option value to be high. We do not think that security strategy makers should always run two types of analysis to understand the value of mandatory and optional security architecture components. Self-intuitively, if the NPV of implementing a security mechanism is high enough, determining the budget is easy because its success seems certain and everyone on board sees that it would pay off handsomely. However, in cases of implementing a security mechanism when the NPV number is strongly negative and all its value is uncovered due to the option, then decision makers should most likely reject it, unless they can create an investment structure allowing the security professionals to learn about this security mechanism quickly and cheaply. If the NPV number lies somewhere in the middle between the above two cases, that is, it is slightly positive, then applying the real options concept makes an essential difference. It is this situation, (i) in which decision-makers are often forced to use their gut feel and intuition when determining how much security is enough or which security mechanisms to implement, and (ii) in which real options can bring the logic to support or refute that intuition.

To conclude our analysis, we note that security budget and resource allocation decision making should rely on a few rules of thumb as simple as the ones we have just described in this section.

5. The Research Case for Real-Options Based Cost-Benefit Analysis of Security Decisions

Our literature review and analysis on how to re-think cross-organizational security strategy making in terms of real options points out that it is possible to find arguments which, when assembled, call for a new reward-and-risk capturing quantitative approach to costs and benefits that business networks should consider when determining where and how much to invest in cross-organizational security mechanisms. Although security practitioners and researchers share the importance of investigating cost/benefits relationships in cross-organizational settings, their published works [ABE05, CAV04, CIS02, COY04, GAR05a, GAR05b, GAR06, BER04, BRO05, GOR06, VIS02, VAU02] cite business needs in isolation

and offer isolated "islands" of solutions [CAR04]. We propose the topic of real-options-based security decision support be approached in a disciplined fashion in five phases as suggested by authors who applied real options to other IT areas [BEN02]. These include: the identification of typical security options at strategic and tactical level, the identification of typical classes of risk factors to consider in networked settings, the selection of a suitable mathematical model for valuing the options, the characterization of the security investment context by using the parameters of the mathematical model, and the interpretation of the results of the option analysis. Each phase opens up a number of research questions. The ones that followed immediately out of our literature analysis are presented in Table 2:

Table 2: Research questions for the future

Research areas	Relevant research questions
1. Identification of strategic security options	1.1. What trade-offs are typically assumed in the variety of security options? 1.2. What value and pitfalls are associated with each option?
2.Risk identification	2.1 What security risks are identifiable and where in the network are they located? 2.2. How liability is shared among network partners when security is compromised?
3.Selection of a suitable mathematical model	3. What criteria to use for selecting a suitable mathematical model for valuing options?
4. Characterization of a security investment context	4.1 How to model the decision-making context? 4.2 What assumptions are valid for mapping the characteristics of the context to the parameters of the mathematical model?
5. Interpretation of the results	5.1 What represents a measure of goodness-of-fit? 5.2 How to explain any differences between the empirical evidence and the analytical findings? 5.3. How real options pitfalls can be avoided?

A number of challenges lie ahead in further developing this approach:

1. Customizing Real Options Analysis for security investment decisions requires estimating the risks associated with the currently available security mechanisms and analyzing their interaction. For instance, while using rule-based intrusion detection one could decide to save money by not updating the rules. Then the question arises how long it will take before a new attack inflicts major damage. Even the user of a single PC is often confronted with such decisions, when licenses expire or when updates are announced. We assume that in a complex corporate IT infrastructure, the decisions are much harder to make.
2. Risk measurement at network level proved very difficult [HAR03]. Few studies have tried so far to assess network dynamics because the cross-organizational context is so complex and because it is hard to get access to a networked business to carry out such a research.
3. Security strategy has a cultural aspect. In litigious societies, like North America, firms may share liability when they do not plan for continuity of operations in the event of security being compromised. Therefore, failure to exercise due diligence in security exposes a business network to litigation risks if data, services, or privacy are lost. This means that we need to develop an understanding of how the position of a company in a network determines the scope of its liability, and the litigation risks involved.
3. The current mathematical models used in options valuation require collection and analysis of statistical data about security breaches. Such data may not be easily available for researchers to carry out case studies.
4. The security architecture for a project needs to be built in such a way that optional components are indeed really optional: it is neither necessary nor impossible to add them at a later moment in time. This means that we need an engineering approach that takes adaptability very seriously.
5. It is worth noting that due to the use of Real Options Analysis to a very specific technical domain of IT security, we need very specific technical knowledge as well. The challenges outlined are far from general decision support but instead require us to develop engineering knowledge about compositional design of security architectures and technical advantages and disadvantages (in terms of costs and risks) of different security solutions.
6. Critics say the real-options-based approach is effective only if a company is genuinely prepared to cancel projects after their initial investment. And anybody who has spent any time in the corporate world knows that projects tend to acquire invisible momentum that is hard to stop.

6. Conclusions

Security challenges have always been accompanying the process of externalizing company's operations and a variety of coordination and security mechanisms have been designed to help organizations cope with these challenges. Resolving these challenges in a systematic way requires information security risk be managed based on five cornerstones: an information security organization, IT asset risk inventory, information security policies, including those based on a common policy structure such as ISO 17799, information security architecture, and a business resiliency program. Real options thinking appears to be well suited to assist in predicting what composes a security strategy and how much of it should be present in a cross-organizational setting: it focuses explicitly on flexibility under uncertainty and makes it feasible to link likely changes to be accommodated by inter-organizational and intra-organizational architectures to value creation. The key merit of our approach is in that it recognizes that the ability to postpone, size up, size down, and outsource types of security and aspects of security of certain types is valuable at both the levels of the business network and the partner companies, when there is flexibility associated with security decision making. Moreover, such an approach seems to reflect well the opposing forces of agility and discipline in today's dynamic business networks: agility implies maintaining the flexibility to change direction quickly, whereas discipline and focus imply the opposite—digging in, reinforcing, and securing a space, and refusing to budge or give it up until all the benefits have been reaped. The tension between agility on the one hand and discipline and focus on the other has to be managed creatively and the real-options concept brings the vehicle that security decision-makers need to do this.

Early results of a literature analysis gives us the indication that the specific implication of a real-options-based approach for security decision-makers is threefold: Security architects and CSO staff can use the approach to support the process of road mapping, developing security plans and policies, and auditing their implementation. The approach is relevant to anyone involved in coordination of the processes of shared information asset identification, risk assessment, making sure a proper control environment is up and running, and achieving a balance between the costs and benefits of security controls.

Second, our proposal sheds some light into how systematically to identify interdependencies among security measures of each type making up the security architecture of a networked business. This confronts the issues that security professionals may not leverage the benefits of what each individual project at partner level brings to the value network.

Third, once the interrelations between security measures are known, security strategies have a rational and quantitative approach to sequencing security investments. This immediately addresses the security planning concern of when to do what.

7. References

[ABE05] Aberdeen Group, 2005 Security Survey, Boston MA, 2005.

[AND01] Anderson, R. Why information security is hard—An economic perspective, Proc.of 17th Annual Computer Security Applications Conference (ACSAC), New Orleans, LA, 2001.

[AMR99] Amram, M., Kulatilaka, N.: Real Options: Managing Strategic Investment in an Uncertain World, Harvard Business School Press, Cambridge, Massachusetts, 1999.

[BEN02] Benaroch, M, Managing Information Technology Investment Risk: A Real Options Perspective. Journal of Management Information Systems, 19(2), pp. 43-84, Fall 2002.

[BER04] Bertine H., I. Faynberg, H.-L. Lu. Overview of Data and Telecommunications Security Standardization Efforts in ISO, ITU, and IETF, Bell Labs Technical Journal 8 (4), Winter 2004, pp. 203-229.

[BON05] van Bon, J., M. Pieper, and A. van der Veen. IT Service Management: An Introduction Based on ITIL. Van Haren Publishing, Amsterdam, 2005.

[BRO05] Brown W., F. Nasuti, Sarbanes-Oxley and Enterprise Security: IT Governance and What It Takes to Get the Job Done, The EDP Audit, Control, and Security Newsletter (EDPACS), Taylor & Francis, August 2005,

[BUT02] Butler, S., Security Attribute Evaluation: a Cost-Benefits Approach, Proc. of the 24th Int. Conf. on Software Engineering (ICSE), 2002, ACM Press. pp. 232- 240.

[CAR04] Carali, R., Managing for Enterprise Security, Technical Report of Software Engineering Institute, CMU, Pittsburg, NY, CMU/SEI-2004-TN-046.

[CAV04] Cavusugly H, H. Cavusuglu, Economics of IT Security Management: Four Improvements to Current Security Practices, Comm of AIS, (14), 2004, pp. 65-75.

[CER04] Cerullo V., M. Cerullo, Business Continuity Planning: a Comprehensive Approach, Information Security Journal, Summer 2004, pp. 70-78.

[CHA02] Champy, J., X-Engineering the corporation: the next frontier of business performance (2002) Warner Books, New York.

[CHI98] Childs, P. D., S.H. Ott,. A.J. Triantis, Capital Budgeting for Interrelated Projects: A Real Options Approach, Journal of Financial & Quantitative Analysis, Sep98, 33(3), pp. 305-335.
[CIS02] CISCO Systems, The Return on Investment for Network Security, San Jose, CA, 2002
[COY04] Coy P., Exploiting Uncertainty: The 'Real Options' Revolution in Decision-Making, Business Week, 2004.
[ERN05] Ernst & Young, 2005 Global Information Security Survey, Report Nr. DJ0001, New York, 2005.
[DEL06] Deloitte & Touche Tohmatsu, Global Security Survey 2006, London UK, 2006.
[DOR04] Dornseif M. S. A. May, Modelling the Costs and Benefits of Honeynets, Proc. of Int. Workshop on Security Economics'04.
[DYN05] Dynes, S., M.E. Johnson, Information Security in the Extended Enterprise: Some Initial Results from a Field Study of an Industrial Firm, Proc. of Int. Workshop on Security Economics'05.
[GAR05] Gartner Group, What Your Organization Should Be Spending for Information Security, March9, 2005, ID G00126733.
[GAR06a] Gartner Group, Security as Engineering Discipline: The SSE-CMM's Objectives, Principles and Rate of Adoption, Feb 21, 2006, ID G00138066.
[GAR06b] Gartner Group, Midsize Business Security Spending Plans, Feb 16, 2006, ID G00137654.
[GAR06c] Gartner Group, Information Security Governance at Telia Sonera, Feb 28, 2006, ID G00136835.
[GOR02] Gordon, L. L. Loeb, The Economics of Information Security Investment, ACM Transactions on Information and System Security, 5(4), 2002, pp. 438-457.
[GOR03] Gordon, L., L. Loeb, L. Lycyshin, Information ecurity and Real Options: a Wait-and-See Approach, Computer Security Journal, 19(3), 2003, pp. 1-8.
[HAM03] Hamel, Gary & Valinkangas, Liisa. The Quest for Resilience, Harvard Business Review 81(9), 2003.
[HOM99] Hommel U., G. Pritsch »Marktorientierte Investitionsbewertung mit dem Realoptionsansatz«, in: Finanzmarkt- und Portfoliomanagement, 13(2), 1999, pp. 121-144.
[HUA06] Huang M.-H., Eliminate the Middleman?, Harvard Business Review, 84(3), 2006, pp. 33-37.
[KEL99] Kelly, B. J, Preserve, Protect, and Defend, Journal of Business Strategy, 20(5), 1999, pp. 22-26.
[KOG03] Kogut, B., N. Kulatilaka, Comment: Real Option Pricing and Organizations: The Contingent Risks of Extended Theoretical Domains, Academy of Management Review, 29(1), 2003, pp. 102-110.
[KUL01] Kulatilaka, N., N. Venkatraman, Strategic Options in the Digital Era, Business Strategy Review 12(4), 2001, pp.7-15.
[KUL99] Kulatilaka, N., P. Balasubramanian and J. Storck, Using Real Options to Frame the IT Investment Problem, in: Real Options and Business Strategy Applications to Decision-Making, Risk Publications, Boca Raton, FL, 1999.
[LAK05] Lakshminarayanan V., W. Liu, C.L. Chen, D.Perry, Managing Sequirity Requirements in Practice: a Case Study, Proc. of the 28th Int. Conf. on Software Engineering (ICSE), 2005.
[MAS06] Masuda, B., Managing the Risks of Managed Security Services, Information Systems Security, March/April 2006, pp. 35-42.
[MIC04] Microsoft Executive Circle, Motorola Case Study, 2004.
[OGC, 2000] Office of Government Commerce. IT Infrastructure Library (ITIL). 2000. http://www.itil.co.uk/.
[SBQ01] SBQ, Special Issue on *Return on Security Investment*, Secure Business Quarterly, (1)2, 2001.
[STR98] Straub,D. W., R. J. Welke, Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, 23(4), 1998, pp. 441–469.
[VAU02] Vaughn V., An Empirical Study of Industrial Security Engineering Practices, Journal of Systems and Software, 2002,pp.225-232.
[VIS02] Vista Research, The Weakest Link, The Economist, October 24, 2002.
[WHI05] Whitworth, M., Outsourced Security – the Benefits and Risks, Network Security, Oct 2005, pp. 16-19.