2009 Eigth IEEE/ACIS International Conference on Computer and Information Science

On the singularity of valuating IT security investments

Thomas Neubauer
Secure Business Austria
Vienna, Austria
neubauer@securityresearch.ac.at

Christian Hartl
Secure Business Austria
Vienna, Austria
hartl@securityresearch.ac.at

Abstract

Companies spend considerable amounts of resources on minimizing security breaches but often neglect to implement efficient ones and are not aware whether their investments are effective. Literature provides many approaches aiming to define the value of IT security investments but often can not fulfill the expectation of decision makers in practice, e.g. due to lacking support for considering multiple objectives, business issues or a variety of investment alternatives. This paper identifies criteria for proper IT security evaluation methods from literature and evaluates some selected methods in order to show their applicability in practice. A focus of this evaluation lies on the comparison to methods for IT investment evaluation, in order to answer the question what the difference of evaluating IT investments and IT security investments is.

1. Introduction

Whereas, assessing the return on investment has always been a stumbling block for regular technology investments, assessing the return on investment for IT security investments proved to be more challenging. In contrast to common technology investments, IT security investments do not provide a calculable profit. Instead, they reduce the occurrence and thereby the costs of security breaches (cf. [23]). Researchers (e.g., [8], [9]) agree that due to the increasing interconnectivity and complexity of IT systems, the likelihood of IT security breaches increases. Every new product that is introduced in the IT market, adds a new security twist. The threats are becoming more sophisticated, and the attacks more numerous. Cavusoglu et al. [10] assessed the influence of security breaches on the market value of breached firms with the result that the breached firms lost 2,1 percent of their market value within two days after the announcement. In addition they determined an average loss in market capitalization of $1,65 billion per incident. They concluded that the cost of poor security is very high for investors, as the returns of an IT security investment can affect the organizations strategic drivers, like the brand name. Therefore, IT security investments have to be seen in the scope of organization's strategy.

This paper develops a new view on IT security investments, by reviewing and evaluating the differences between methods for the evaluation of IT and IT security investments in order to support IT managers in better choosing appropriate methodologies for investment selection processes. The comparison will start by contrasting definitions, and approaches to IT, and IT security investments. Followed by identifying, and evaluating challenges of both fields by reviewing existing literature. Based on the identified challenges of both fields we continue with an evaluation and compare the characteristics of approaches for IT investments and IT security investments selection with the aim of evaluating those methodologies by their effectiveness in practice. In the field of IT investment selection we use Cost/Benefit Analysis, the Analytical Hierarchy Process (AHP), Real Option Valuation (ROV) as well as Multi Objective Decision Support System (MODS). Regarding the evaluation of IT security investment methodologies Cost/Benefit Analysis, Defense Trees, Security Attribute Evaluation Method, and Multi-Objective Safeguard Selection Tool (MOST)) are evaluated, with the same criteria used for IT investments.

2. Background

Schechter [28] defines the common term security as "the process of identifying events that have the potential to cause harm (or threat scenarios) and implementing safeguards to reduce or eliminate this potential". Security can be seen as the process of defending an asset against injury or harm. In order to develop an appropriate strategy to prevent events, Threat Scenarios can be used. A Threat Scenario is "a series of events through which a natural or intelligent adversary (or set of adversaries) could use the system in an unauthorized way to cause harm, such as by compromising the confidentiality, integrity, or availability of the system's information" (cf. [28], [2], [19]).

Some authors extend those properties by adding further objectives. Knorr et al. [18] add accountability whereas Soohoo [29] adds authenticity. Herrmann et al. [17] define those three properties as a general definition and subsume under security intellectual property, bindings, privacy and anonymity. To prevent the occurrence of threat scenarios, countermeasures can be defined (synonyms: control, security

978-0-7695-3641-5/09 $25.00 © 2009 IEEE
DOI 10.1109/ICIS.2009.90

measure, safeguard). A countermeasure is "a policy, process, algorithm, or other measure used to prevent or limit the damage from one or more threat scenarios" [28].

Approaches for evaluating security investments (and thus selecting countermeasures) can be distinguished into qualitative and quantitative methods [20]. According to Liao qualitative methods require human experts in all of the phases during assessment, including analyzing the threat probability, evaluating the asset value and the vulnerability and estimating the impacts that threats may cause. Quantitative methods (e.g. [28], [29] and [30]) offer mathematical models for calculating risks derived from long-term population data. In addition there are combinations of both approaches (cf. [5], [7]). Soohoo [29] categorizes approaches for evaluating IT security investments using models of the "first" and "second" generation. Whereas models of the first generation (e.g. Risk Trees, ALE-based techniques; cf. [21]) consider security as a binary condition, second generation approaches (e.g. Integrated Business Risk-Management Frameworks, Valuation-Driven Methodologies, Scenario Analysis Approaches, and Best Practice) describe security in relative terms, because the binary view results in the assumption that all quantities are exactly known (e.g. using single point estimates instead of probabilistically weighted or parameterized ranges of values). These models lead to excessive complexity, poor treatment of uncertainty, and data unavailability [29]. Integrated Business Risk-Management Frameworks focus on the bottom line of business impact, without capturing details of computer security interaction. Valuation driven methodologies focus on the asset value leaving the likelihood of the risk definition behind. The disregard of efficiency measures, frequency of security breaches and safeguard costs results in over- or underspending, where both states are economically inefficient. Scenario Analysis approaches develop different scenarios how computer security can be compromised. They have a limited scope on risks and their effects. Best Practice approaches describe policies and safeguards which are implemented in a majority of organizations.

One reason why measuring IT security investments is hard stems from the fact that there is no common definition of security. Accepting the fact that security is not a binary condition results in some further challenges. Decision makers have to ask themselves "What level of risk can I accept?". In order to answer this question we have to regard security in the organizational context considering the following criteria:

- Multiple Objectives: A major precondition for the proper selection of IT security investments is the definition of objectives. Although researches (cf. [28], [2], and [19]) agree that security is commonly referred to as CIA (Confidentiality, Integrity, Availability) there are additional objectives for IT security investments to find (e.g. [18], [29]). So the first challenge starts by defining objectives of the IT security investment which depend on the particular environment where the security strategy should be deployed.
- Many Alternatives: Considering the complexity of an IT system and the amount of things that can go wrong, determining the acceptable risk level and selecting appropriate safeguards is a challenging task for decision makers. Comparing security designs is challenging because "the strength of the design depends on a relaxed adherence to security engineering design principles" (cf. [7]). Designs that have a risk mitigation to each risk are usually preferred to those that leave gaps for rarely expected attacks.
- Lack of Information: The reliable assessment of information security risks can be more difficult than the assessment of other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing, especially due to the following reasons:
  - Data is limited on risk factors, such as the probability of a sophisticated hacker attack and the costs of damage, loss, or disruption caused by events that exploit security weaknesses.
  - Some costs, such as loss of customer confidence or disclosure of sensitive information are difficult to quantify.
  - Although the costs of hardware and software needed to strengthen controls may be known, it is often not possible to precisely estimate the related indirect costs, such as the possible loss of productivity that may result when new controls are implemented.
  - Even if accurate information would be on hand, it is often out of date due to changes in technology and factors such as improvements in tools available to potential intruders.
- Intangible Costs/Returns: Although security is an organizational problem that must be framed and solved in the context of the organization's strategic drivers, many organizations perform a technology-centric approach. They often regard security as a technical issue where the connection to organization's strategic drivers is neglected.

  A technology centric approach may result in seeing only confidentiality, integrity and availability as objectives. It is clear that IT security may influence the objectives derived from IT investments which are financial, business and strategic performance. By altering this view on risks a new challenge arises. Security strategy must be sufficiently dynamic to keep up with organizational change.
- Time Perspective: When thinking about risk we ask ourselves: What is the probability of occurrence?, What

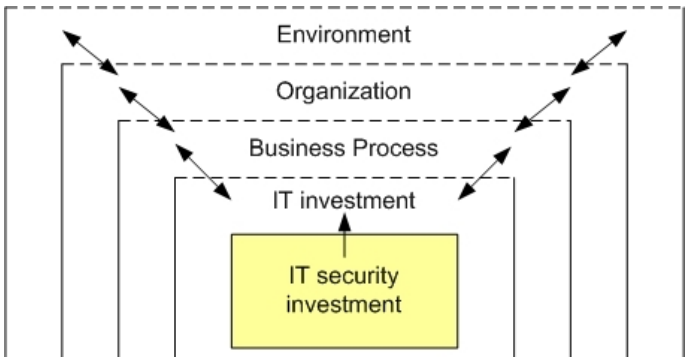

Figure 1. View of technology centric approaches

is the damage that might occur?, When will the risk occur? or When will/should an attack be prevented? It is important to consider the time perspective for risks, and the time value of money in order to allow an appropriate evaluation. If we knew that an attack takes place in three years, we could invest in something else for three years, and invest in the safeguard that prevents the attack at exactly the time the attack occurs.

3. Comparison of Evaluation Methods

This section provides a review of the selected evaluation methods:

- IT investments: Cost/Benefit Analysis, Real Option Valuation, Analytical Hierarchy Process, and Multiobjective Decision Support.
- IT security investments: Defense Trees, Mizzi's Return on Information Security Investment, Security Attribute Evaluation Method, and Multiobjective Decision Support.

Each methodology will be described according to the following criteria:

- Type: Financial Technique/Operations Management technique.
- Aim: This criterion describes on which of the aspects stated in section 2 the methodology focuses. A methodology can have 1 to 5 aims.
- Input/Output Variables: This criterion evaluates the input and output variables of the methodologies. This will show (i) how the challenges are understood in both fields and (ii) if/how methodologies can be used in both fields.
- Advantages/Disadvantages: This criterion evaluates the advantages/disadvantages of the methodologies, by (i) contrasting researchers opinions and (ii) deriving from how challenges are understood and solved.

3.1. IT investment methodologies

Cost/Benefit Analysis addresses only time perspective and intangible costs/returns. Its strength lies in its simplicity, which can give suitable solutions for low risk investments. One of the major challenges lies within estimating the costs and benefits of IT investments. It is assumed for these metrics that cost and benefits are known with certainty. In particular, they do not consider non-financial performance measures, although they can be included if a serious cost and benefit estimation was performed in the first place. Even in this case they give a misleading indication, because intangible costs and returns are downsized to a single value. According to Tallon [31] "The key problem with these evaluation techniques is their treatment of uncertainty and their failure to consider that outside of a decision to reject an investment outright, firms may have an option to defer an investment until a later period". The evaluation of information technology investments is particularly challenging because it is characterized by long payback periods, uncertainty, and changing business conditions (cf. [3]). Therefore, these methods do not consider uncertainty (cf. [27], [4], [14]) and propose Real Option Valuation for managing uncertainty in IT investments.

Criteria	Cost/Benefit Analysis
Type	Financial Technique
Aim	Time Perspective
	Intangible Costs/Returns
Input Variables	Time perspective
	Costs
	Cashflows
	Interest Rate
Output Variables	ROI, NPV, IRR, Benefit/Cost Ratio
Advantage	Time value of money considered
	Simple concept
Disadvantage	Missing "operating flexibility"
	Missing consideration of uncertainty
	Tendency to decide with one criterion
	Only suitable for low risk investments

Table 1. Evaluation: Cost/Benefit Analysis

Real Options are very suitable for IT investments, which depend strongly on market positions and aspirations. In fact, up to 60 percent of IT investments depend on its market position and aspirations [11]. They concentrate on the strategic planning phase of an IT investment, which leads to flexibility and increased responsiveness, by considering multiple forms of risk and incomplete information. According to Gardner [15] and Davis [13] determining the input variables for Real Options is extremely difficult. In addition they emphasize the high level of mathematics, which is too sophisticated for most organizations. One of the key problem of Real Options might be their assumptions deriving from financial options for IT investments [31]. Some researchers (e.g. [26]) conclude, that Real Options lead to over-valuation, because

they do not consider implementation time. This could lead to the insight that determining the correct input variables is vital for a sophisticated Real Option valuation.

Criteria	Real Options Valuation
Type	Financial/Operations Technique
Aim	Time Perspective
	Intangible Costs/Returns
	Lack of Information
Input Variables	Present value of expected cash flows
	Investment Cost
	Time until opportunity dissolves
	Interest Rate
	Project Uncertainty (volatility)
Output Variables	Option Value/Flexibility Value
Advantage	Time value of investment
	Multiple forms of risk, incomplete information
	Flexibility and increased responsiveness
	Adoptable to various decision making problems
	Suitable for medium/high risk investments
Disadvantage	Determining input variables is difficult
	High level mathematics
	Tend to overvaluate projects
	May be inappropriate for IT investments
	Iindividual strategic factors are not included

Table 2. Evaluation: Real Options

The Analytical Hierarchy Process (AHP) is adoptable to various decision making problems (cf. [6] for an example). Therefore the decision maker can individually adopt AHP to almost any specific decision making problem. This is basically done by translating strategies into objectives and measures. In addition AHP includes financial and non-financial methods, considers relationship among factors, generates statistics to confirm decision analysis, supports hierarchical planning through many organizational levels. It is the first methodology in this evaluation, which directly aligns IT investment decisions to the organization's strategic drivers.

Criteria	Analytical Hierarchy Process (AHP)
Type	Financial/Operations Technique
Aim	Time Perspective
	Intangible Costs/Returns
	Lack of Information
	Multiple Objectives
Input Variables	Criteria (Objectives)
	Alternatives
Output Variables	"Best Alternative" according to weighted objectives
Advantage	Translation of strategies into objectives
	Financial and non-financial methods
	Considers relationship among factors
	Adoptable to various decision making problems
	Suitable for medium/high risk investments
Disadvantage	Complex (due to pairwise comparison of all factors)

Table 3. Evaluation: Analytical Hierarchy Process

Multi Objective Decision support directly addresses the challenge "Many Alternatives" in a way, which non of the others is capable of. It considers the aspect, when we have to decide among alternatives, e.g. with similar functionality. The multiobjective methodology proposed by [25] changes the way of thinking of "Should I invest in A or B or C?", to "Should I invest in A and/or B and/or C?". This creates a portfolio of investment alternatives, where in addition individual dependencies, and properties of alternatives can be considered. Furthermore it addresses "Lack of Information", where compared to AHP, less a-priori information is needed, because the decision maker can individually change/set boundaries, in order to see how these changing effect the solution space. The proposed model is strongly linked to the organization's strategy, (business process, multiple objectives, and resource constraints).

3.2. IT security investment methodologies

The model presented by Bistarelli et al. [5] is a combination of a quantitative and qualitative approach. They use financial methods comparable to NPV, and combine them with attack trees. An attack tree is an example for scenario based qualitative analysis. It is an analytical way to describe how attacks against a system can be performed. For each safeguard the Return on Security Investment is calculated. In addition to Return on Security Investments (ROSI) this approach implements measures like, Return on Attack (ROA) [12], and Annual Loss Expectancy (ALE). One of the major disadvantages of this model is the missing consideration of interactions between safeguards.

Criteria	Defense Trees
Type	Quantitative Method/Financial Method
Aim	Intangible Costs/Returns
Input Variables	Single loss expectancy
	Annual rate of occurrence
	Risk mitigated
	Expected gain from attacker
	Costs of safeguards
	Costs of an attack
Output Variables	Return on Security Investment (ROSI)
	Annual Loss Expectancy (ALE)
	Return on Attack (ROA)
	Expected gain from attacker
	Costs of an attack
Advantage	Combination of qualitative and quantitative method
	Combination of ROSI and ROA
Disadvantage	Lack of empirical data for SLE and ARO
	Interactions between safeguards are not considered

Table 4. Evaluation: Defense Trees

Table 4 compares Mizzi's [22] quantitative approach with the approach proposed by Bistarelli et al. [5].

In line 1 Mizzi [22] defines the potential annualized loss of a threat as Total Annualized Loss and [5] defines it as Annualized Loss Expectancy. There are mainly two differences:

Mizzi [22]	Bistarelli [5]
1. $L_t = L_I + \frac{I*t}{365}$	$ALE = SLE * ARO$
2. $CTB < (L_I + A(t))$	$ROA = \frac{GI}{cost\_before\_S + loss\_caused\_by\_S}$
3. $ROSI = \frac{L_t}{3}$	$ROSI = \frac{(ALE*RM)-CSI}{CSI}$

Table 5. Evaluation: Comparison of two quantitative ROSI methodologies

- Mizzi calculates the Total Annualized Loss depending on the time the system is down. Bistarelli et al. do not consider the down time of a system directly. Their calculation is based on the *Single Loss Exposure*, which includes the downtime of a system as loss.
- Bistarelli et al. define the *Annualized Rate of Occurrence (ARO)*, whereas Mizzi [22] does not use any kind of probability estimates.

The second line lists the *Motivation to Attack* from Mizzi and the *Return on Attack* from Bistarelli et al. Mizzi calculates the Motivation to Attack based on the gain of the attacker over time, and assumes that if the cost to break are higher than the expected gain, then the attacker would not compromise the system. This is an example for a binary view on security. It directly considers the safeguard to prevent an attack in the calculation. Line 3 shows the Return on Investment. Mizzi [22] states that the investment into security should not be more than one third of the expected loss.

Criteria	Mizzi's Return on Security Investment
Type	Quantitative Method/Financial Method
Aim	Intangible Costs/Returns
Input Variables	Annual costs to fix vulnerabilities
	Initial safeguard costs
	Annual maintenance costs
	Instantaneous loss
	System down time
	Information asset value
	Recovery costs
	Costs to exploit vulnerabilities
	Costs of damage
Output Variables	Security Expenditure
	Total Annual Loss
	Annual Damage
	Motivation to Attack
	Annual costs to break
Advantage	Considers a variety of criteria
Disadvantage	Only objective considered is information asset protection
	Binary view on security
	Lack of underlying facts

Table 6. Evaluation: Mizzi's Return on Security Investment

Butler [7] combines a qualitative (scenario analysis) and quantitative method (Economic Indexes) in order to develop a Cost/Benefit approach. Butler uses a Multi-Objective Risk assessment phase, using different unit values for estimating the relative importance of each type. She uses the Security Attribute Evaluation Method (SAEM) to evaluate security investment alternatives. With this implementation she addresses the challenges Lack of Information, Intangible Costs/Returns, and Multiple Objectives. The key advantage of this methodology lies in the implementation of the *Swing Method*, which is similar to AHP, a methodology which transforms subjective measures into weights.

Criteria	Security Attribute Evaluation Method
Type	Quantitative/Qualitative Method
Aim	Intangible Costs/Returns
	Lack of Information
	Multiple Objectives
Input Variables	Individual outcome attributes
	Outcome attribute values
	Relative ranking of outcome attributes
	Frequency of attack
	IT security categories (Protection, Detection, Recovery)
	Risk Mitigation of IT security alternatives
	Individual Objectives (Factors)
	Safeguard costs
Output Variables	Threat Index
	Best alternative according to specified criteria
Advantage	qualitative and quantitative methods
	Combination of ROSI and ROA
	Multi-Objective Risk assessment phase
	Sensitivity analysis
Disadvantage	Estimating effectiveness of safeguards

Table 7. Evaluation: Security Attribute Evaluation Method

Strauss and Stummer present a Mulitobjective Decision Support System for IT Security investments selection. This approach helps IT managers in their attempts a given risk by evaluating and selecting portfolios of security measures. It proposes attractive portfolio candidates with respect to the decision-maker's preferences. They demonstrated their model by a case study that evaluates the risk of hacking into a Local Area Network (LAN) in an academic environment. Their model consists of 4 phases: In phase 1 a general risk analysis is carried out, the search for security measures commences and alternative security activities are screened. In phase 2, the solution space of all feasible and efficient measures are determined. In phase 3 a rough selection of portfolios using a quad tree to establish attractive areas is performed. In phase 4 a neighborhood search identifies alternatives that may match the decision-maker's preferences even more closely.

4. Differences between IT and IT security investments evaluation

This section contrasts the methodologies evaluated in the previous sections. Table 9 compares the characteristics of these approaches using the criteria defined in chapter 2.

	IT investment methodologies				*IT security investment methodologies*			
Challenge(s)	CBA	ROV	AHP	MODS	Mizzi	Def. Trees	SAEM	MODS
Many Alternatives				X				X
Lack of Information		X	X	X			X	X
Intangible Costs/Returns	X	X	X	X		X	X	X
Multiple Objectives			X	X			X	X
Time Perspective	X	X	X					

Table 9. Challenges addressed by Methodologies

Criteria	Multiobjective Decision Support
Type	Quantitative/Qualitative Method
Aim	Intangible Costs/Returns
	Lack of Information
	Multiple objectives
	Many alternatives
Input Variables	Individual objectives
	assets, vulnerabilities, threats
	ARO (frequency)
	Safeguard interactions
	Risk mitigation of security alternatives
	Safeguard costs/benefits
Output Variables	Pareto efficient portfolios
Advantage	combination of qualitative and quantitative method
	Multi-Objective decision support
Disadvantage	Estimating effectiveness of safeguards

Table 8. Evaluation: Multiobjective Decision Support

The first two methodologies directly compared are *Cost/Benefit Analysis* with *Defense Trees*, because both are based on the *Return on Investment* metric.

Criteria	Return on Investment	Return on Security Investment
Challenge(s)	Intangible Cost/Returns	Intangible Cost/Returns
	Time Perspective	
Formula	$ROI = \frac{Benefit}{Costs}$	$ROSI = \frac{(ALE*RM)-CSI}{CSI}$
Input	Costs	Costs
	Benefits	Risk Mitigated
	Time	Annual Loss Expectancy

Table 10. Evaluation: ROI and ROSI

Both metrics result in a Cost/Benefit ratio (while a ROI value above 100% is considered as profitable, a ROSI value above 0 is considered as profitable). A ROI calculation has to include tangible/intangible costs and benefits and the time value of money. In contrast, ROSI is using a risk value which is mitigated by the IT security investment (safeguard). The value of this mitigation depends on the value of the underlying asset. This value is derived from the ALE, that defines costs which regularly (annually) occur. Investing in safeguards results in minimizing those costs, which is the benefit of the investment. The challenging part of this calculation, which is similar to ROI, lies in calculating the ALE. This variable depends on two criteria, which are difficult to estimate: The impact, which occurs from a successful attack, and the probability of a successful attack. One further difference lies within the consideration of the time value of money that is only included in ROI calculation. The reason for this lies within the lack of information *when* the benefit of safeguards is realized.

Compared to common Cost/Benefit analysis, Real Option valuation considers a project's uncertainty in form of volatility. It requires more than the cashflow, because it calculates the option value considering multiple cashflow expansions. The input variables in IT security investments differ more than those used in IT investment evaluation methods. While IT investment methodologies require the same variables (benefits, costs, cashflow, time, interest rate) or (benefit criteria, set of alternatives), the input variables for IT security differ more from each other.

The valuation of IT investments is often strongly linked to business process. In contrast a suitable IT security investment depends on assets, vulnerabilities, and threats, and additionally (i) affects the execution of the according business process(es) for a period of time, and (ii) results in negative effects on the strategic performance of the organization, depending on the type of the damage (Confidentiality, Integrity, Availability, Authenticity).

This results in different planning of IT and IT security investments: While decision makers of IT investments are concerned how they can speed up business processes or change existing business processes using IT systems in order to improve the strategic performance of the organization, decision makers of IT security investments have to think about the various effects, which can go far beyond the delay of existing business processes. For example if an attacker hacks into the costumer database of a bank and gets the personal identification number (confidentiality) of the costumers, this would most probably not have any effects on the business processes, but have effects on the *costumer satisfaction*, and further may result in a serious loss of money. This difference in thinking about IT and IT security investments leads (i) to more input variables, (ii) to more complex IT security investment methodologies, and (iii) to a higher amount of proposals of IT security investment methodologies .

This aspect leads to *Real Option Valuation*. While ROI and ROSI or Multiobjective Decision Support for IT and IT security investments can be directly compared (AHP

can be used in both fields), there is not a comparable IT security investment methodology regarding Real Option Valuation . The question which arises from this aspect is "Is it possible to adopt Real Option Valuation for IT security investments?" The most obvious problem is the difference in thinking about *the time perspective* of uncertainty and risk. For example, when thinking about IT investments somebody is considering buying a PC and a printer. In the classic NPV approach he would calculate the NPV by the rate of return when investing in the PC and printer in the present. The real options approach modifies this thinking in: First he invests in the PC and two months later he defines the option of buying a printer depending on how much pages he actually needs to print and the future prices of the copy shop nearby. It is obvious that this thinking has a (flexibility) value. When thinking about IT security investments the situation turns out being different. When a burglar wants to steal our PC, we would have to consider a time perspective: When is the best time to invest in a better door which holds the burglar off our home? To answer this question we would have to know *when* the burglar most probably would try to steal the PC and if the costs for the new door are reasonable compared to buying a new PC. Gordon [16] states it this way "Although this wait-and-see approach toward information security expenditures may seem unwise on the surface, there is a rational economic explanation for such an approach under the appropriate conditions."

5. Conclusions

Managers regularly have to cope with a wide spectrum of potential risks and, thus, the decision of selecting the most appropriate set of security safeguards. The complexity of finding an "optimal" security level is further increased as decision makers have to deal with multiple, often opposing, objectives, as well as uncertainty about the future. As a result, overspending is one of the major corporate problems and decision makers are in demand of methods for efficiently evaluating the optimal level of security investments. The major aim of this paper was to develop a new view on methods for the evaluation of IT security investments, by reviewing and evaluating the differences between IT and IT security investments and methods for its evaluation in order to support IT managers in better choosing appropriate methodologies for investment selection processes. Regarding the research question posed at the beginning, this paper showed that IT and IT security evaluation methods have major differences in their level of diversity. In other words, the input variables in IT security investments methods differs more than those of IT investment methods. While IT investment methodologies usually require the same variables such as benefits, costs, cashflow, time, interest rate, the input variables for IT security investment methods show a much higher diversity. This fact shows that due to its complexity, its variety of definitions and thus a wider field of potential solution approaches the field of IT security investments is more contentious than IT investments. It was further shown that complexity is primarily a result of a higher level of uncertainty.

Acknowledgment

This work was performed at Secure Business Austria, a competence center that is funded by the Austrian Federal Ministry of Economics and Labor (BMWA) as well as by the provincial government of Vienna.

References

[1] M. Amico and Z. Pasek, "A new methodology to evaluate the real options for an investment using binomial trees and monte carlo simuation," *Proceedings of the Winter Simulation Conference*, pp. 351–359, 2003.

[2] M. Andrews and J. Whittaker, "Computer security," *IEEE: Security & Privacy Magazine*, vol. 2, pp. 68–71, 2004.

[3] I. Bardhan, S. Bagchi, and R. Sougstad, "A real options approach for prioritization of a portfolio of information technology projects: A case study of a utility company," *Proceedings of the 37th Hawaii International Conference on System Sciences*, 2004.

[4] M. Benaroch, "Managing information technology investment risk: A real options perspective," *Journal of Management Information Systems*, vol. 9, pp. 43–84, 2002.

[5] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," *IEEE-Proceedings of the First International Conference on Availability, Reliability and Security (ARES 06)*, 2006.

[6] L. Bodin, L. Gordon, and M. Loeb, "Evaluating information security investments using the analytic hierarchy process," *Communications of the ACM*, vol. 48, pp. 79–83, 2005.

[7] S. Butler, "Security Attribute Evaluation Method: A Cost Benefit Approach", Proceedings of the International Conference on Software Engineering, 2002.

[8] K. Buzzard, "Computer security - what should you spend your money on?" *Computer & Security*, vol. 18, pp. 322–334, 1999.

[9] R. Caralli and W. Wilson, "The challenges of security management," *CERT Coordination Center*, 2004.

[10] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," *International Journal of Electronic Commerce*, vol. 9, pp. 69–104, 2004.

[11] D. Craig and R. Tinaikar, "Divide and conquer: Rethinking IT strategy," *McKinsey on IT*, vol. 3, pp. 4–13, 2006.

[12] M. Cremonini and P. Martini, "Evaluating information security investments from attackers perspective: The return on attack," *4th Workshop on the Economics on Information Security*, 2005.

[13] G. Davis, "Estimating volatility and dividend yield when valuing real options to invest or abandon," *The Quarterly Review of Economics and Finance*, pp. 725–754, 1998.

[14] E. Clemons and B. Weber, "Strategic information technology investments: Guidelines for decision making," *Journal of Management Information Systems*, vol. 7, pp. 9–28, 1990.

[15] L. Gardner, "Using information generated by a discrete event simulation to evaluate real options in a research and development environment," *Proceedings of the Winter Simulation Conference*, pp. 2040–2047, 2000.

[16] L. Gordon, M. Loeb, and W. Lucyshyn, "Information security expenditures and real options: A wait-and-see approach," *Computer Security Journal*, vol. 19, pp. 1–7, 2003.

[17] G. Herrmann, "Security and integrity requirements of business process - analysis and approach to support their realisation," *Proc. CAisE: 6th Doctoral Consortium on Advanced Information Systems Engineering*, pp. 36–47, 1999.

[18] K. Knorr and S. Röhrig, "Security requirements of e-business processes," in *I3E*, pp. 73–86, 2001.

[19] C. Landwehr, A. Bull, J. McDermott, and W. Choi, "A taxonomy of computer program security flaws," *ACM Computing Surveys*, vol. 26, pp. 211–254, 1994.

[20] G.-Y. Liao and C.-H. Song, "Design of a computer-aided system for risk assessment on information systems," *IEEE 37th Annual 2003 International Carnahan Conference on Security Technology*, pp. 157–162, 2003.

[21] R. Mercuri, "Security watch - analyzing security costs," *Communications of the ACM*, vol. 46, pp. 15–18, 2003.

[22] A. Mizzi, "Return on information security investment. are you spending enough? are you spending too much?" *ITtoolbox Security*, 2005.

[23] M. Al-Humaigani and D. Dunn, "A model of return on investment for information systems security," *Department of Electronics and Computer Technology*, 2004.

[24] T. Neubauer, C. Stummer, and E. Weippl, "Workshop-based multiobjective security safeguard selection," *IEEE-Proceedings of the First International Conference on Availability, Reliability and Security*, pp. 366–373, 2006.

[25] T. Neubauer and C. Stummer, "Extending business process management to determine efficient IT investments," *Proceedings of the 2007 ACM Symposium on Applied Computing*, pp. 1250–1256, 2007.

[26] H. Nembhard and M. Aktan, "Effect of implementation time of real options valuation," *Proceedings of the Winter Simulation Conference*, pp. 1600–1605, 2002.

[27] R. Kauffman and X. Li, "Technology competition and optimal investment timing: A real options perspective," *IEEE Transactions of Engineering Management*, vol. 52, pp. 15–29, 2005.

[28] S. Schechter, "Computer security strength & risk: A quantitative approach," Ph.D. dissertation, Harvard University Cambridge, 2004.

[29] K. SooHoo, "How much is enough? a risk-management approach to computer security," *CRISP*, 2000.

[30] C. Strauss and C. Stummer, "Multiobjective decision support in IT-risk management," *International Journal of Information Technology and Decision Making*, vol. 1, pp. 251–268, 2002.

[31] P. Tallon, R. Kauffman, H. Lucas, A. Whinston, and K. Zhu, "Using real options analysis for evaluating uncertain investments in information technology: Insights from the ICIS 2001 debate," *Communications of the Association for Information Systems*, vol. 9, pp. 136–167, 2002.