December 2007

Return on Security Investments - Design Principles of Measurement Systems Based on Capital Budgeting

Jan Brocke
Liechtenstein University

Christian Buddendick
University of Münster

Gereon Strauch
University of Münster

Return on Security Investments – Towards a Methodological Foundation of Measurement Systems

Jan vom Brocke[1], Gereon Strauch[2], Christian Buddendick[2]

[1] HILTI Chair for Information Systems, Liechtenstein University
Fürst-Franz-Josef-Strasse, Principality of Liechtenstein

[2] European Research Center for Infomation Systems (ERCIS)
University of Münster, Leonardo-Campus 3, Germany

jan.vom.brocke@hochschule.li
{gereon.strauch/christian.buddendick}@ercis.de

Abstract:

IT-security has become a key topic for nearly every company nowadays. To safeguard security, investments in technical and organizational infrastructures have to be made. The efficiency and effectiveness of these investments can often be hardly determined due to the invisibility of their benefits. When implementing IT-security measures, the predicted outcome, e.g. prevented losses, is uncertain in two ways. First it is not certain that one measure and the corresponding investment will prevent a certain risk to occur in the future and second the seriousness of the prevented incident is hard to calculate. In research and practice the calculation of ROSI (Return on Security Investments) is recommended. A vital discussion about different approaches to calculate this ratio can be observed. Within this article we argue that existing approaches lack of a sound theoretical base for calculating this ratio. We therefore apply principles of capital budgeting to present a framework to enable decision support when investing in IT-security measures. This framework comprises means of simulation in order to take the uncertainty of the investment situation into account. By sensibility analysis and Risk-Chance profiles decision makers can incorporate their individual risk preference in a specific situation.

Keywords: Risk Management, Information Systems Security, IT-Governance, Economics of IT-Security, Return on Security Investments (ROSI)

Introduction

IT-Security has become a vital factor for companies nowadays. The importance of this topic in practice can be read of the over proportional rise of spending for IS security budgets in comparison to all IS budgets (BSI 2000, p. 122). The question of economic efficiency is mostly neglected when planning and implementing IS security measures (BSI 2000, p. 154). The general necessity of profitability analysis is emphasised in later works, but the existing insights in this field of research can be characterised as “vague”, “useless” or without a relation to concrete recommendations for action (Peltier 2001, p. 5). As an indicator of economic efficiency of IS security measurements, a number of specific challenges become apparent. The contribution to profit or loss of one single security measure cannot be evaluated in an isolated way, because they are normally part of a package of measures (Soo Hoo 2000, p. 18). Decisions concerning IS security measures are intended as or perceived to be broad investment decisions (Soo Hoo 2000, p. 18). For such a long-term-examination, direct and indirect in- and out-payments, have to be considered (Grob 1993). There are problems with the quantification of the in-payments, while it is easier to identify direct out-payments of an investment in IS security measures. The in-payments, as they mainly prevent future damage, may never result in positive returns (Rodewald 2005, p. 140; McCumber 2005, pp. 192-196). In addition to that, there are interdependencies to other parts of the information system. To regard the economic efficiency of IS security measures the adoption of a broad and multi-periodic view is needed.
Based on a literature review, we first give an overview on existing approaches to calculate the return on security investments. These findings are applied in order to derive the characteristics of the decision situation and their corresponding requirements for decision support. We then introduce a framework for calculating the return on security investments on a capital budgeting base to meet the derived requirements. Within this framework, relevant factors are taken into account neglected in traditional approaches, for example tax payments and specific interest rates. This framework includes means of handling uncertainty by applying simulation methods as well. To demonstrate this framework a calculation of the return of security investments for an example by means of different spreadsheets is displayed. We then conclude with a brief summary and an outlook on future research.

Overview on Approaches to Calculate the Return on Security Investments

In the following, the approaches presented in the literature and their identified requirements are examined. An established approach is used to calculate the reduction of the expected loss. Investments in IS security measures give no immediate return, but help avoid unwanted incidents and prevent loss. This approach became popular due to the 1979 publication of the “Guideline for Automatic Data Processing Risk Analysis” by the National Bureau of Standards. The top figure, Annual Loss Expectancy (ALE) is generated out of the sum of the expected annual loss traced back to security holes (Mercury 2003).

$$ALE = \sum_{i=1}^{n} S(E_i) \cdot F_i$$

$S(E_i)$ Monetary loss caused by event E_i
F_i Probability of E_i

The ALE-concept was used in the 80s in America, mainly because of its endorsement by the National Institute of Standards and Technology (NIST). The phase-out of these projects led the concept to fall into oblivion (Nowey et al. 2005, p. 17). Soo Hoo names the main reasons for the failure of the ALE concept: an exaggerated level of detail and high complexity of the model, the strong dependence of the model on a completed data pool and the inherent presumption and that all tables are deterministic and well-known (Soo Hoo 2000, pp. 7-9). Other authors criticized the lack of empirical data on the expected loss (Mercury 2003).
The second generation approaches (Soo Hoo 2000, p. 9) resulted out of the recognition that ALE is impracticable. These can be characterized by a reduction of complexity compared to the ALE concept. Exemplarily, the Integrated Business-Risk Management Framework, pure value based methodologies, scenario-analysis and best practice approaches should be named. The non-technical Integrated Business-Risk Management Framework deals with the IS security risks analogous to common business-risks (operational, financial, etc.). This is inadequate to the specifics of the problem. Value based methodologies focus only on the possible amount of loss of one event without a consideration of the incidence rate, so that a total quantification of the risk is impossible. Scenario-analysis focuses only on one or on a small number of threats and does not allow an evaluation to have broad investments. The Best Practice approach as a standardized procedure does not allow the consideration of individual specifics. None of these approaches is suitable for decision support, because none quantifies the benefit of IS security investments or regards important variables, like business impact or interest rates (Wang 2005). Important aspects are not considered in the following approaches, as, e. g. those of Gordon and Loeb (2002) or Cavusoglu, Mishra and Raghunathan (2004). The model of Cavusoglu, Mishra and Raghunathan focuses e. g. only on decisions about intrusion detection systems. Parameterizing these models is very expensive (Soo Hoo 2000). For these reasons no decision support is possible. The approaches did not gain any significance for measuring IS security investments. Thus, there is still

demand for a suitable method to evaluate economic efficiency. One key figure for economic efficiency, used in practice, is the Return on Security Investments (ROSI). This approach aroused great interest for two main reasons: On the one hand the ROSI offers, through a pretended analogy to the Return on Investment (ROI), a solid and well-known basis for investment decisions (Mayer 2004, p. 2, Peltier 2001, p. 254) the other hand, the feigned clear statement and simplicity of the key figure is emphasized (Nowey et al. 2005, p. 21).
There is not any standardized definition of the ROSI: next to the usage of different names for the variables and the utilization of different input tables, ROSI is computed as an absolute value (Berinato 2006) or a quotient (Mayer 2004, p. 2; Sonnenreich et al. 2005, p. 1). Normally the computation as an absolute value is favored (Nowey et al. 2005, p. 20):

$$R - S + T = ALE$$
$$R - ALE = ROSI$$

ALE Annual Loss Expectancy
R Recovery Costs (Sum of the annual costs to recover the loss out of the incidents)
S Savings (Sum of avoided loss)
T Tool Cost (Costs of security measures, based on Total Cost of Ownership)
In addition to this ROSI can be computed as a quotient:

$$ROSI = \frac{R - ALE}{T} = \frac{S - T}{T} \quad (4)$$

Both variants of the ROSI-concept are based on the ALE-concept, which is combined with the classic TCO-concept for IS security investments. Therefore, the ROSI-concept adopts all critical aspects of the two concepts. On the one hand the critics of the ALE approach which are discussed above: Critical for a profit measurement of security measures is that only the direct costs of a measure and the alteration of the expected loss go into the calculation. Indirect costs caused by changes of the productivity through a modification of the processes are neglected. Furthermore the main disadvantages of the classical TCO-method, such as the non-observance of tax- and interestpayments (vom Brocke 2007, p. 73 f) count for this approach as well. The ROSI does not fulfil the claim to be comparable or compatible to the ROI. On the one hand in the absolute value form presented above, the reference value of the ROI, the average cost of capital, can not be consulted.
Soo Hoo tries to improve the ROSI-concept by regarding investment decisions as decisions between different security guidelines (Soo Hoo 2000, p. 18). A security guideline is a bundle of many security measures. Soo Hoo compares them to each other, regarding the “Net Benefit” (Soo Hoo 2000, p. 18). A quantitative valuation of a security investment shall be reached by the “Net Benefit”, with consideration of additional costs, benefits and the changed ALE.
Only one period of time is considered in all of the above described approaches (Soo Hoo 2000, p. 49; Gordon and Loeb 2002; Mayer 2004). Either the mean costs are used or constant (and therefore quite problematic) parameters are assumed. It is not possible to represent the complex decision situation in an adequate way with the help of these approaches. Other approaches of cost-benefit analyses (CBA) (Butler 2002; Gordon and Loeb 2006; Landoll 2006, p. 372; Mercuri 2003) use classical but oversimplifying methods, like the Net present Value (NPV) and the Internal Rate of Return (IRR), which usually do not consider taxes and may lead to wrong decisions. Especially because of the mentioned background of complex approximation and evaluation problems of IS security investments, it is incomprehensible that tax and interest are not considered. This oversight leads to an unrealistic examination of investment decisions. The very important decision between purchase, leasing or outsourcing can not be made without regarding tax and interest payments. Criticizing such approaches is—especially in the IS controlling field—not unusual (Kaplan 1986, p. 85)

Deriving Requirements for Decision Support

The decision-making situation of an IS security investment is affected not only by the direct but also by the indirect payments, related by the investment. Next to the variation on the expected loss, all effects on other application systems and business processes of a company, based on factual and temporal interdependencies, have to be taken into account (Neubauer et al. 2005). It is essential to regard the derivative payments as tax and interest, because of the long-term horizon. To underline the importance of considering these payments, one should take the decision between purchase, leasing or outsourcing into account. This decision is often driven by effect resulting form, different tax or interest rates. Taxes have to be considered because of the ability to attribute costs of negative incidents to the taxes. It can be more efficient to contend with the risk than to invest in security measures. According to this, a main requirement for decision models for IS security investments is that all relevant, direct and indirect payments in the relevant period of time are adequately considered. Firstly, all relevant environmental conditions have to be modelled. They determine the in- and out-payments, and furthermore the framework of the investment. Solely the tax rate is displayed here, for simplification. Depending on the chosen alternative,

the decision maker can influence the in- and outpayments and the expected loss. Table 1 gives an overview of the relevant payments of a decision about IS security investments.

Table 1. Relevant payments of IS security investments

Point of time / Kind of payment	t=0	…	t=n
Direct outpayments of the investion			
e. g. hardware			
e. g. software			
e. g. training			
e. g. licences			
e. g. maintenance			
…			
Additional outpayments			
e. g. loss of productivity			
e. g. less motivated employees			
e. g. loss of flexibility			
...			
Additional inpayments			
e. g. 1st level support			
e. g. better image (higher sales via internet)			
…			
Expected loss *(with and without IS security investment)*			
Derivative Payments			
Taxes			
Interest payments			

The chosen investment alternative has impact on the probability of an incident and on the amount of loss. To evaluate the investment, the difference between the expected loss with the investment (with-case) and without the investment (without-case) is of high relevance. The additional in- and out-payments should be refined as well. Thus, the input factors, which determine the payment, become more transparent on another level of aggregation. The connection between different alternatives of investment, possible reductions of out-payments and additional in-payments, should be mentioned. With the help of security measures, out-payments, for example in the field of user support, can be reduced. Next to this, additional in-payments should be accounted; a higher level of security (e. g. SSL encryption in an online shop) can result in an increase of customers.

On the other hand, not only the out-payment for the acquisition, but also all direct and indirect ou-tpayments that follow, must be regarded. This can result out of a reduced productivity, for example. More indirect out-payments, related to the investments in IS security, have to be regarded, too. Customers can be distracted from their purchase by complicated order processes, for example.

For an IS security investment, all relevant tables and their relationships—as shown here—have to be identified. In order to enable decision support, all relevant data have to be integrated in one long-term calculation. In the following section we will introduce an approach based on established investment controlling methods that is suitable for this situation.

Framework for calculating the return on IS-Security-Investments

Development of a framework

One established method of investment controlling that matches all of the above derived requirements is VOFI (Visualization of Financial Implications). Parallel to the consideration of all relevant aspects, the correct illustration and calculation of the several periods and the corresponding payments have been identified as a basic requirement for a decision support concept for IS security investments. Established methods of investment appraisal should be accessed. Instead of classical methods for investment computation NPV or IRR, which are applied in this context from time to time,(Butler 2002; Gordon and Loeb 2006; Landoll 2006, p. 372; Mercuri 2003) VOFI (Visualization of Financial Implications) is used. VOFI allows a complete, standardized and transparent visualization of the investment and provides a correct evaluation, even within multiple periods (Grob 1993, p. 50ff.). Special advantages of this investment appraisal tool are the great transparency, which is required due to the complexity, uniqueness and expandability of each investment.

All relevant in- and out-payments (cp. 3) have to be consolidated to one cash flow series. In addition, the reduced expected loss has to be taken into account. In a separate table the series of payments without the investment (without-case), should be aggregated. The series of payments is transferred to the VOFI. A VOFI is a collection of all relevant payments in one spreadsheet. Next to this, VOFI considers—contrary to other approaches—tax and interest (Grob 1993). The VOFI of the investment is shown in table 2.

Table 2. VOFI of the investment

Period	**t=0**	**t=1**	**…**	**t=n**
Series of payment **Internal funds**				
Overdraft credt + credit intake - redemption - debit interest				
Financial investment - reinvestment + disinvestment + creditor interest				
Tax payment - payment + refund				
Net funding				
Balances On overdraft credit On financial investment				
Net balance				

Interest and interest rates can be considered as differentiated in VOFI. Different types of credits and investment conditions, with different interest rates, maturity and kinds of repayments can be taken into account. Different means of financing the project can be regarded simultaneously. With those finance instruments, the series of payments is balanced so that a net funding of zero occurs. The series of payments, calculated with the interest payments, earnings and the deprecation, results in the tax base (table 3) to be multiplied with the tax rate. If the tax base is negative, loss compensation with the rest of the company will result in a tax refund for the current investment. The tax rate can be calculated for every company regarding the specific circumstances, e.g. different tax rates for subsidiaries in different countries.

As every investment situation, investments in IT-security are facing the problem of uncertainty as well. Uncertainty can occur in different ways in these decision situations. For example the probability of a risk to occur cannot be predicted ex-ante. Other uncertain factors comprise the effectiveness of specific security means and the amount of money to be spent in future periods.

Traditional risk ratios (e.g. Mean, Variance) are seen as an insufficient means to summarize varying cash flows from multiple aspects. The risk-chance-analysis (Hertz 1964) is an approach to examine the uncertainty of the decision problem by simulation. In doing so, multiple factors of uncertainty are modelled with distributions, and the distribution of the target figure is evaluated within a simulation run. The so far described scenario servers as a calculation system, as the cash outflows and the simulated cash inflows in the VOFI are summarized to financial ratios. The result of the simulation run includes e.g. the distribution of the accumulated value of the investment or the resulting return on security investments for specific measures. The distribution of the target ratio is transformed into a so-called risk-chance-profile. Risk-Chance-Profiles (Hertz 1964) make it possible to read off the probability when a target figure is greater than or equal to a critical value.

Table 3. Computation of the depreciations and the taxes

Period	**t=1**	**…**	**t=n**
Calculation of depreciation Book value in January - depreciation			
Book value in December			
Calculation of tax payment Net payment - Interest payment + Interest earning - Depreciation			
Tax base			
Refunds Payments			

The balance on financial investment of the last period is the terminal value of the investment. This value should be compared to all terminal values of the VOFIs alternatives. If there is only one investment, the terminal value, with the investment (with-

case), has to be compared to the status quo (without-case). To do this, a VOFI is to be created with the unchanged expected loss and an alternative usage of the internal funds with a standard opportunity interest rate. The net terminal value of the investment is the difference between the terminal value of the investment and the terminal value of the opportunity (the second-best solution) (Grob 1993). The investment should be realized when the net terminal value is positive.
Constitutive different bundles of security measures can be compared with regard to their terminal value. To enable a broad decision support, not only the resulting terminal values can be compared, but also the specific RPCs of each investment alternative. In the following section we will introduce an example to illustrate a typical IT-security investment situation within which the framework is utile to calculate the return on security investments.

Application of the framework by an example

In the following, the approach described above will be demonstrated on the basis of an example. This example gives a brief overview on the mode of operation of the framework. Some assumptions are made in order to simplify the decision situation which can be vanished in real applications of this framework. The example is abutted to a case described by Mayer: a company with 70,000 employees plans the introduction of new ID cards, based on certificates (Mayer 2004, p. 4f). The planning horizon and the expected useful life of the investment are added up to four years. Historical data show that a loss of 3.4 million euro occurred every past year because of offences. An expert study tells that the sum of annual loss will increase by 10% per year, if the company keeps the status quo. Another study shows that in comparable companies 80% of the loss is generated by attendance of the employees. It is expected that with the introduction of certificate-based ID cards, especially through better assignment possibilities, the attacks on the information systems, along with the attendance of the employees will be reduced by 75%. Overall, this leads to an expected loss of 1.36 million euro in the first year. It can be assumed that there will be less first level support (e. g. due to forgotten passwords), which will result in savings of 150 euro per user per year. The support assumes that these savings will only approach 50% in the first year and be fully realized starting with the second year. The introduction of the new ID cards creates outpayments of 11 million euro in t=0 for hard- and software. Furthermore, the management assumes 1.5 million euro for integration, 0.3 million euro for testing and 0.2 million euro for consulting and initial training courses. During the whole useful life, an out-payment of 1 million euro per year for attendance, service and support is calculated. Two employees support the whole project during the entire time (out-payments = 100,000 euro per year). To finance the project, 7 million euro of internal funds is allocated. The debtor interest rate is 8%, the creditor interest rate 5%. The internal funds could be used for another investment and create an interest rate of 7%. The company assumes a constant tax rate of 55%. The initial out-payment for hard-and software and all other out-payments in t=0 can be activated and will be depreciated linearly over four years. With these data, the series of payments (table 4) can be calculated.

Table 4. Series of payment of the example investment

Point of time / Kind of payment	t=0	t=1	t=2	t=3	t=4
Personal		100,000 €	100,000 €	100,000 €	100,000 €
Hard and software	11,000,000 €				
Consulting and integration	11,000,000 €				
Testing process	300,000 €				
Training	200,000 €				
Attendance, service and support		1,000,000 €	1,000,000 €	1,000,000 €	1,000,000 €
Expected loss		1,360,000 €	1,496,000 €	1,645,600 €	1,810,160 €
Savings 1st level support		- €	5,250,000 €	10,500,000 €	10,500,000 €
Series of payment	-13,000,000 €	-2,460,000 €	2,654,000 €	7,754,400 €	7,589,840 €

With these data the VOFI and all auxiliary calculations can be computed (table 5 and 6).

Table 5. VOFI of the investment

Period	t=0	t=1	t=2	t=3	t=4
Series of payment	-13,000,000 €	-2,460,000 €	2,654,000 €	7,754,400 €	7,589,840 €
Internal funds	7,000,000 €				
Overdraft credît					
+ credit intake	6,000,000 €				
- redemption		464,500 €	2,782,522 €	2,7252,978 €	
- debit interest		480,000 €	442,840 €	220,238 €	
Financial investment					
- reinvestment				2,424,895 €	5,257,488 €
+ disinvestment					
+ creditor interest					121,245 €
Tax payment					
- payment				2,356,289 €	2,453,597 €
+ refund		3,404,500 €	571,362 €		
Net funding	0 €	0 €	0 €	0 €	0 €
Balances					
On overdraft credit	6,000,000 €	5,535,500 €	2,752978 €		
On financial investment				2,424,895 €	7,682,383 €
Net balance	**-6,000,000 €**	**-5,535,500 €**	**-2,752,978 €**	**2,424,895 €**	**7,682,383 €**

Table 6. Computation of the depreciations and the taxes

Period	t=1	T=2	t=3	t=4
Calculation of depreciation				
Book value in January	13,000,000 €	9,750,000 €	6,500,000 €	3,250,000 €
- depreciation	3,250,000 €	3,250,000 €	3,250,000 €	3,250,000 €
Book value in December	9,750,000 €	6,500,000 €	3,250,000 €	0 €
Calculation of tax payment	**55%**	**55%**	**55%**	**55%**
Net payment	-2,460,000 €	2,654,000 €	7,754,400 €	7,589,840 €
- Interest payment	480,000 €	442,840 €	220,238 €	
+ Interest earning				121,245 €
- Depreciation	3,250,000 €	3,250,000 €	3,250,000 €	3,250,000 €
Tax base	-6,190,000			
Refunds	3,404,500 €	571,362 €		
Payments			2,356,289 €	2,453,597 €

The terminal value of the investment is 7,682,383 Euro.

Table 7. VOFI of the investment

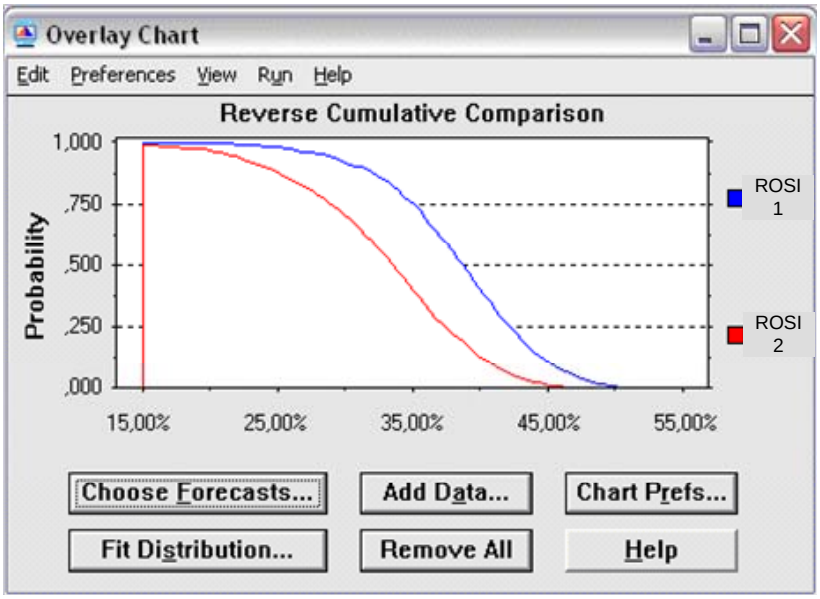
Period	t=0	t=1	t=2	t=3	t=4
Series of payment		-3,400,000 €	-3,740,000 €	-4,114,000 €	-4,525,400 €
Internal funds	7,000,000 €				
Overdraft credît					
+ credit intake					
- redemption					
- debit interest					
Financial investment					
- reinvestment	7,000,000 €				
+ disinvestment		1,309,500 €	1,503,749 €	1,719,417 €	1,958,709 €
+ creditor interest		490,000 €	398,335 €	293,073 €	172,713 €
Tax payment					
- payment					
+ refund		1,600,500 €	1,837,916	2,101,510	2,393,978 €
Net funding	0 €	0 €	0 €	0 €	0 €
Balances					
On overdraft credit					
On financial investment	7,000,000 €	5,690,500 €	4,186,751 €	2,467,333 €	508,624 €
Net balance	**7,000,000 €**	**5,690,500 €**	**4,186,751 €**	**2,467,333 €**	**508,624 €**

The terminal value of the without-case is 508,624 euro (cp. table 7). The net terminal value—difference of the terminal value of the investment (TVI) and the terminal value of the opportunity (TVO)—of the investment is:

$$TVI\text{-}TVO = 7{,}682{,}383\ € - 508{,}624\ € = 7{,}173{,}759 \quad (5)$$

The positive net terminal value of 7,171,759 € will lead to the recommendation to invest in these security measures.
In addition to the comparison of the net terminal value TVI and TVO the return on security investments for different alternatives with respect to the uncertainty can be compared. Therefore some assumptions on the distribution on relevant variables have to be made. For example an assumption regarding the tax rate of future periods or the outpayments for each alternative. In the example case, a return on security investment of 33.4% (38.6%) for alternative 1 (2) has been computed. It is assumed that the uncertainty regarding the outpayments in future periods can be modeled by standard normal distributed variable. Simulation experiments can be applied to display the change of the return on security invesments based on this distribution. As a result the probability of this return can be compared for both alternatives. In this case a variation of the number of outpayments does not affect the decision suggestion. In every case the return on security investments of alternative 2 is higher than the one of alternative 1. The overlay chart of the cumulative comparison is displayed in figure 8.

Table 8. RPC for



The assumption of distributed variables can be made for other elements of the calculation too. Depended on the elements and their distributions situations may occur where alternative 1 is recommended.

Summary and Outlook

With this paper we have introduces a framework for calculating the return on security investments on a capital budgeting base. This framework can be applied by decision makers in order to evaluate the efficiency and effectiveness of IT-security measures. A review on existing literature has shown that most of the actual approaches for measuring this return are insufficient. Either they neglect important variables or they do not take the long term implications of investments into account. Based on the identified requirements we have introduced a framework comprising VOFI as a central method for calculating the return on security investments. In order to handle the uncertainty typical for investment situations, we proposed simulation methods. These methods enable the use of different distributions for variables of an IT-security investment. These Findings can be merged into Risk-Chance-Profiles (RPC) in order to compare different alternatives. We demonstrated the application of this framework by an example.
Further research will focus on two different aspects of this framework. (1) Further body of research will be conducted in order to identify relevant variables which drive the return on security investments. Therefore practical cases will be compared and data mining methods applied to gain insights in the field. (2) Practical implementations of this method should deliver findings on the adequacy and utility of the proposed framework. These findings will contribute to the further development of the framework.

References

Berinato, P.: Finally, a real return on security spending, http://www.cio.com/archive/021502/security.html [11/24/2006].

Bundesamt für Sicherheit in der Informationstechnik (BSI). *Kosten und nutzen der IS-Sicherheit, Studie des BSI zur Technikfolgen-Abschätzung*, 2000.

Butler, S. "Security attribute evaluation method: a cost-benefit approach," *Proceedings of the 24th International Conference on Software Engineering*, W. Tracz (ed.), Orlando, FL, 2002, pp. 232–240.

Cavusoglu, H., Mishra, B. and Raghunathan, P. "A model for evaluating is security investments," *Communications of the ACM* (47:1), 2004, pp. 87-92.

Gordon, L. A. and Loeb, M. P. "The economics of information security investment," *ACM Transactions on Information and System Security* (5:4), 2002, pp. 438 - 457.

Gordon, L., Loeb, M. P. "The economics of information security investement," *ACM Transactions on Information and System Security* (5:4), 2002, pp. 438 - 457.

Gordon, L., Loeb, M. P. "Budgeting process for information security expenditures," *Communications of the ACM* (49:1), 2005, pp. 121-125.

Grob, H. L. *Capital budgeting with financial plans*, Vahlen, München, 1993, pp. 50-80.

Hertz, D. B. "Risk Analysis in Capital Investment." Harvard Business Review (42:1), 1964, pp. 95-106.

Kaplan, R. P. "CIM-Investitionen sind keine Glaubensfragen," *Harvard Manager* (9:3), 1986, pp. 78-85.

Landoll, D. J. *The security risk assessment handbook: a complete guide for performing security risk assessments*, Auerbach Publications, Boca Raton, 2006, p. 372.

Mayer, B. *Rosi – Return on Security Investment. Eine notwendige Rechnung*, http://www.it-daily.net [05/02/2006].

McCumber, J. *Assessing and managing security risk in IT systems: a structured methodology*, Auerbach Publications, Boca Raton, 2005, pp. 192-196.

Mercury, R. T. "Analysing security costs," *Communications of the ACM* (46:6), 2003, pp. 15-18.

National Institute of Standards. *Guideline for automatic data processing risk analysis*, 1979.

Neubauer, T., Klemen, M. and Biffl, S. "Business process-based valuation of IT-security," *Proceedings of the seventh international workshop on Economics-driven software engineering research*, K. Sullivan (ed.), St. Louis, MO, 2005, pp. 1- 5.

Nowey, T., Federrath, H., Klein, C. and Plößl, K. „Ansätze zur Evaluierung von Sicherheitsinvestitionen. Sicherheit 2005", *Beiträge der 2. Jahrestagung des GI-Fachbereichs Sicherheit, Lecture Notes in Informatics (P-62)*, 2005, pp. 15-26.

Peltier, T. R. *Information security risk analysis*, Auerbach Publications, Boca Raton, 2001, pp. 5, 254.

Rodewald, G. "Aligning information security investments with a firm's risk tolerance," *Proceedings of the 2nd annual conference on Information security curriculum development*, M. E. Whitman (ed.), Kennesaw, GA,2005, pp. 139-141.

Sonnenreich, W., Albanese, J. and Stout, B. "Return on security investment (ROSI). A practical quantitative model," *Working paper*, New York, 2005.

Soo Hoo, K. J., (2000): "How much is enough? A risk management approach to computer security", Consortium for Research on Information Security and Policy (CRISP), Stanford.

vom Brocke, J., (2007): Service Portfolio Measurement (SPM), A Decision Support System for the Management of Service-Oriented Information Systems, Enterprise Service Computing from Concept to Deployment. R. Qiu (Editor), Hershey, PA, USA 2007, pp. 58 - 90.

Wang, A. J. A. (2005), Information security models and metrics, Proceedings of the 43rd annual southeast regional conference - Volume 2, pp. 178-184.