

METHODOLOGIES FOR EVALUATING INFORMATION SECURITY INVESTMENTS - WHAT BASEL II CAN CHANGE IN THE FINANCIAL INDUSTRY

Christian Locher, University of Regensburg, 93040 Regensburg, Germany,
christian.locher@wiwi.uni-regensburg.de

Abstract

The New Basel Capital Accord (Basel II) will include operational risk to the calculation of necessary regulatory capital in financial institutions after year-end 2006. Most of the banks have already developed sophisticated risk management frameworks helping to quantify and manage operational risk. Information security has direct impact on operational risk, but risk managers consider Information Systems (IS) related risks not enough by now. This problem mainly depends on the variety of methods used by security managers to evaluate systems security and to develop security concepts. Even little efforts would enable information security officers to quantify the benefits of information security investments using operational risk quantification methods. The security community has not yet addressed this opportunity. The article discusses models used for decisions about security investments known from the field of security economics and accounting and illustrates the problems by applying these models. Based on a general operational risk management framework of a bank, this article introduces a new approach using accepted risk management methods.

Keywords: IT security, risk analysis, investments, return on security investment

1 INTRODUCTION

Information security products are subject to a fast technical improvement. Nevertheless, this technical development is often not turned into a higher level of information security. A representative survey (N=500) by the German BSI (Bundesamt für Sicherheit in der Informationstechnik) shows that 20% of German IT security experts think their organisation is vulnerable because of insufficient controls. The annual CSI (Computer Security Institute) IT-security study (N=530) also shows that the performed countermeasures are often not adequate to mitigate the changing threats (Gordon et al. 2004). This leads to the finding that information security is more an organisational than a technical topic. Although the financial sector is very sensitive to security issues, the official cases of security breaches in banks are astonishing¹ - and we can expect a large number of unreported cases. One important point is that only few companies are planning security investments in a particular manner. Therefore, security investments are more or less event-triggered. An outcome of (Aberdeen Group 2004) is that 125 of 210 companies did not or not consistently track security investments. On the other hand, the biggest challenges for security officers were inadequate staffing and resources (63%) and funds for unforeseen, but necessary security programs (63%). Although many companies see security as a very important issue, only few are performing enterprise-wide self-assessments, i.e. a comprehensive management view of information security-related risk does not exist. Hence, what is demanded both by financial or IS controllers and security officers in companies are methods for evaluating security investments in order to make security affordable, accountable and economically. This article aims at the problem, that the benefit of most security investments is ignored by common financial analysis methods. Therefore, in the field of security economy methods have been developed which try to close this gap but lack integration in financial analysis methods. It is shown that Basel II may cause a fundamental improvement of financial analysis methods by considering risk as an accountable measure. In the end, the methods known from security economy may be unnecessary. The article is structured as follows: Section two starts with an introduction to financial performance measurement of projects in general, the influence of Basel II on financial performance measurement and an operational risk measurement method. In section three, methods for determining security needs and building concepts are reviewed under an economic point of view. Methods for valuing and deciding about security investments are shown in section four. An example using some of the introduced models is presented in section five.

2 EFFECT OF BASEL II ON THE VALUATION OF INVESTMENTS

Basel II has major effects on the financial industry. Not only credits must be priced risk-oriented, internal risks are treated the same way. Basel II will include operational risk in the calculation of necessary regulatory capital. This has effects on the internal performance measurement methods in a bank. In section 2.1 common performance measurement models are introduced. The part of Basel II concerning operational risks is introduced briefly in section 2.2 and in section 2.3 the influence of Basel II risk measurement approaches on accounting models is shown. One popular risk measurement approach – the Loss Distribution Approach (LDA) – is explained in section 2.4.

¹ e.g. security breach in home banking application (Deutsche Bank 24, 2000); ability to steal confident client data (Deutsche Kreditbank, 2003); Worm 'Code Red' causes cash dispenser breakdown (Bank of America, 2003); Nimda Worm crashes network (Deutsche Bank, National Australia Bank, 2001).

2.1 Valuation of investments based on financial performance measurement methods

Performance measurement methods are divided into static and dynamic methods. Both concepts are distinguished in residual concepts (e.g. income - cost) and profitability concepts (e.g. profit/capital). The cash flow return on investment (CFROI) concept as a static profitability measure plays an important role to measure the profitability of a business unit, company, or project. It relates cash flows to the capital invested:

$$CFROI = \frac{\text{inflows} - \text{expenses}}{\text{capital}} \quad (1)$$

A project or business unit is profitable if the CFROI is greater than a pre-defined return on capital. If a manager wants to consider more periods, he/she needs to use dynamic concepts like net present value (NPV). The NPV is a dynamic approach. It is calculated by discounting all expenses and inflows caused by the project during expected n lifetime periods. Suppose E_t being all direct inflows of period t , A_t all expenses and i the internal rate of discount. The NPV of the investment is calculated as follows:

$$NPV = \sum_{t=0}^n (E_t - A_t) \frac{1}{(1+i)^t} \quad (2)$$

A project is profitable, if the NPV exceeds zero (i.e. the investment is at least as profitable as an alternative investment). The strengths of both methods are that investments are fully comparable within all organisational units having the same measurement policy. The NPV has advantages within pre-investment analysis while ROI concepts are best for the ongoing assessment of investment profitability. All models consider only cash flows and neglect other aspects like strategic value of an investment.

2.2 Risk and economic capital as new decision variables in enhanced economic frameworks

Banking business heavily relies on outside capital. A financial institution has to cover potential losses with at least 8% own resources (regulatory capital, C_{Basel}). When losses from operational risk are added to the losses from market and credit risk (what is the intention of Basel II), banks have to cover additionally operational risk following this formula (Basel Committee on Banking Supervision 2004):

$$C_{\text{Basel}} = \frac{\text{equity capital}}{\text{risk assets credit risk} + (\text{market risk and operational risk}) * 12.5} \geq 0.08 \quad (3)$$

According to Basel II, technology, organisational defects, human beings or external events can cause operational losses. IS-related risk is part of operational risk in banks, but attempts to integrate security risk are still at the beginning for three reasons: Even in banks, security risk is not assessed to an adequate extend, security risks are distributed over several risk categories with emphasise on availability and security risks are often not measured quantitative.

Because regulatory capital is limited to the total amount of a bank's own resources, it should be used wisely: On one hand, it restricts the amount of business of the bank, on the other hand the gap between used capital and available capital should be minimised to maximise earnings on capital. Basel II will allow banks to use indicator based operational risk measurement methods (with gross income as indicator) and advanced approaches. It forces larger and internationally active banks to use advanced measurement methods (e.g. the loss distribution approach shown in section 2.4) and "an allocation of economic capital for operational risk across business lines in a manner that creates incentives to improve business line operational risk management." (Basel Committee on Banking Supervision

2004) Risk adjusted performance measurement is necessary to derive internal measures from these requirements.

2.3 Influence of Basel II on financial accounting methods

To fulfil the demand from section 2.2, risk sensitive methods like the RARORAC (risk adjusted return on risk adjusted capital, derived from the ROI concept) must be used.

$$RARORAC = \frac{\text{inflows} - \text{expenses} - \text{expected loss}}{\text{regulatory capital}} \quad (4)$$

A project is profitable, if the RARORAC is greater than a pre-defined value. It is also possible to define a risk-adjusted NPV. It considers alternative investments of the saved regulatory capital using the specific return on equity i_{ROE} and changes in expected loss for financial pre-investment analysis (Locher et al. 2004).

$$NPV = \sum_{t=0}^n ((E_t + \Delta \text{expected loss} + \Delta \text{regulatory capital}_t * i_{ROE,t}) - A_t) \frac{1}{(1+i)^t} \quad (5)$$

A project is profitable if the NPV is greater than zero. E_t and A_t incorporate all monetary aspects, while $\Delta \text{expected loss}$ and $\Delta \text{regulatory capital}$ are measures for changes in risk structure. These two effects are output of the measurement method explained in the next section.

2.4 Measurement of operational risk and capital adequacy: The Loss Distribution Approach

The Loss Distribution Approach (LDA) is the best-known approach to risk measurement and regulatory capital calculation. Although there are many variations in use, they all base on the core model shown in this article. The LDA enlarges the risk definition of the expected loss (risk = frequency x damage) to the understanding of risk as a function of two independent random variables (risk = f (frequency, damage)), what is known from financial risk management or from assurance practice. This understanding is much more comprehensive, because it stresses that losses can occur randomly in frequency and severity in accordance to characteristic distributions. Given this, the expected value covers only a smaller part of all possible loss scenarios and never catastrophic losses, which are intended to be covered with a bank's equity capital. The LDA divides a bank into logical organisational units and operational risk into risk categories (see table 1).

| Business Unit/ Risk Category | BU ₁ | BU ₂ | BU ₃ | ... | BU _n | ∑ RC |
|---------------------------------|---------------------|---------------------|---------------------|------|---------------------|--------------------------|
| RC ₁ | L ₁₁ | L ₁₂ | L ₁₃ | ... | L _{1n} | L(RC ₁) |
| RC ₂ | L ₂₁ | L ₂₂ | L ₂₃ | ... | L _{2n} | L(RC ₂) |
| RC ₃ | L ₃₁ | L ₃₂ | L ₃₃ | ... | L _{3n} | L(RC ₃) |
| ... | ... | ... | ... | ... | ... | L(RC _j) |
| RC _m | L _{m1} | L _{m2} | L _{m3} | ... | L _{mn} | L(RC _m) |
| | L(BU ₁) | L(BU ₂) | L(BU ₃) | | L(BU _n) | ∑ Operational Risk |

L_{mn} VaR of losses in RC_m in BP_n

Figure 1. Risk categories, business units, and aggregation of operational loss

Within each category all similar risks are gathered, for example “internal fraud” will contain all risks or losses that are caused by deliberate or unintentional acts from employees (Basel Committee on Banking Supervision 2004). The parameters and distributions are determined separately for every business line/risk category combination. After aggregating the two distributions, an individual loss distribution for every category and organisational unit is computed. Input data for the distributions are experts’ opinions, internal loss records, and external data. The Value-at-Risk (VaR) is a risk measure. This is originated from financial risk management and expresses the value, which will – within a particular confidence level (e.g. of 99.9%) – not be exceeded. The loss between the expected loss and the upper confidence limit is called unexpected loss. A detailed overview over the method is given in (Alexander 2002).

The overall VaR at a confidence level of 99.9% has to be covered with equity capital following formula (3). It is obvious, that the accuracy of the method raises the more historical data is available from the loss database, and the less it depends on experts’ opinions. On the other hand, historical data may cause too high/low operational risk data in a fast changing environment, so experts’ opinion will always play an important role for input data adjustment in rapidly changing environments. Figure 1 gives an overview over the calculation of regulatory capital using the LDA.

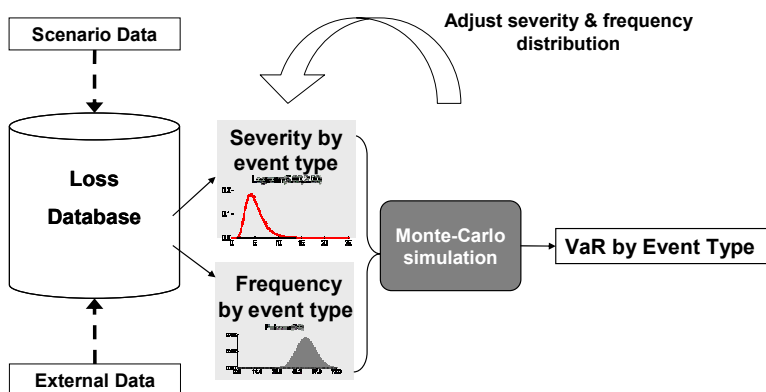


Figure 2. Overview of risk quantification using the LDA

At this point, we leave the macro level of operational risk management and go into the micro level of information security risk management. In practice, security management is quite independent from operational risk management, what leads to different risk measurement methods. On the macro level, the overall IS risk is interesting, because it reflects the value of information assets and business impact of IS risk, on the micro level it is interesting how single threats and vulnerabilities are interacting and form the overall IS risk. Risk discussed in section two is risk of monetary loss. Risk discussed in the next section is mostly seen as risk of successful attacks. Bringing these two views together has not been achieved neither in practice nor in theory. Nevertheless, Basel II will force this, because it demands an enterprise risk management framework and therefore more methodical integration is needed.

3 MANAGEMENT OF INFORMATION SECURITY RISKS

Information security risks are the risk that the firm’s information and information systems are not sufficiently protected against many kinds of damage or loss (Straub & Welke 1998). Security risks are not only a technical problem; even more, they arise from the socio-technical information system of a firm, consisting of humans interacting with technical systems. This work does not distinguish in security and safety aspects, because it has a clear business focus and from that perspective, it makes no difference if the loss is caused either intentional or unintentional (Dierstein 1990). Losses from security risk can be caused by a lack of organisation, human failures or fraud, technical failures or external events (BSI 2001) and are classified as financial, technical, ecological, social, psychological

or other (Ekenberg et al. 1995). There are various models helping security managers to protect a firm's information, for example baseline protection approaches (BSI 2001), vulnerability analysis approaches (Vossbein 1995) and risk analysis approaches (Pfleeger & Pfleeger 2003, Gerber & von Solms 2001, McEnvoy & Whitcombe 2002). These models are reviewed with consideration of integration aspects into operational risk management, the ability to order investments according to their relevance and economic aspects.

3.1 Baseline protection approach

The baseline protection approach concentrates on the analysis of threats (BSI 2001). A threat is "a set of circumstances that has the potential to cause loss or harm" (Pfleeger & Pfleeger 2003). Many firms did not install integrated security architectures. The low security level often depends on the lack of knowledge about the implemented products and their security-related configuration. The BSI baseline protection approach uses different dimensions for safeguards (architecture layers like infrastructure, organisation, personnel, hardware & software, communication, etc.) and for threats (causes such as human error, force majeure, organisational shortcomings, etc.). All threats and safeguards are listed in catalogues. A secure system is achieved if all threats have been eliminated with adequate safeguards.

Advantages and disadvantages: The baseline protection approach helps to protect a firm's IT against threats by defining standardised safeguards for low to middle protection needs. By applying the baseline protection, the majority of systems reach an adequate amount of protection. The baseline protection approach is also often criticised. Individual IS infrastructures are hard to consider and the rising size of the catalogues makes it hard to implement. Its partial use may hinder a firm from building homogenous security architecture. It is too technical and it is always at least a little step behind the actual threats and technical developments. The baseline protection approach does not consider any economic aspects (Warren & Hutchinson 2003) and helps not to establish priorities in safeguard planning.

3.2 Vulnerability analysis approach

Vulnerabilities are weaknesses in a firm's IS architecture (Vossbein 1995, Pfleeger & Pfleeger 2003). The definition covers organisational and technical aspects. Vulnerability analysis targets on analysing the vulnerabilities and implementing controls to minimise the existing vulnerabilities. Starting from a normative policy or idea of a secure system, the security analyst has to identify possible gaps. Vulnerability analysis is mostly based on system specific or policy-based checklists. A secure system is achieved if all vulnerabilities are eliminated.

Advantages and disadvantages: The advantage of the vulnerability analysis is the fact, that it is highly standardiseable and modulariseable. It is easy to perform, but it struggles with the same problems like the baseline protection approach. Each change in technical architecture, organisational regulations, etc. may cause changes in the checklists. The checklist concept may also cause security managers not to think actively. According to the baseline protection approach, the vulnerability analysis approach does not consider economic aspects but expressing the criticality of a vulnerability is possible. (Vossbein 1995)

3.3 Risk analysis approach

The risk analysis approach bases on the assumption that structure, organisation and milieu of the IS organisation and type of the processed information are very heterogeneous. For that reason, every firm has very different security requirements. Information has completely different protection needs that cannot be satisfied with standard controls. For that reason, the need of safeguards has to be determined with detailed risk analysis. The risk analysis approach considers both, vulnerabilities and threats. If both come together, a risk arises. Additionally, it considers the consequences of a risk (i.e. loss, harm)

on a firm's assets. The basic structure of a risk analysis is to select the parts of the architecture (technical or organisational) which should be assessed, then to analyse the protection needs, analyse threats, vulnerabilities and business impacts and then to determine adequate countermeasures. For low protection needs, risk analysis is often combined with the baseline or vulnerability analysis approach. Risk analysis methods differ in mainly aspects: The approach to structure the problem (Zbigniew 1997), the measurement method, and the definition of impact.

For structuring the problem, often simulation-based or scenario analysis methods are applied. The amount of risk is calculated usually by multiplying probability and damage ($R=p \times d$) to compute the expected loss. To simplify the calculation, often an ordinal or semi-metric scale is used. The loss model is vital for comparing risks and losses – astonishingly there is no accepted model for loss calculation. Different model range from fully accountable results (e.g. Basel II loss model) to embracing approaches incorporating reputation losses, temporary share drops and other qualitative variables (this issue is discussed further in section 4.1).

Aim of the methodology must be a maximum of objectivity and long-time reliability of the results. Historical data is the premise for experts' knowledge, which mainly bases on a projection of historical risk perception and experience to the future. The problem is, that only a low percentage of all security breach attempts (e.g. 65% of security breaches successful, 2.6% of them detected in (U.S. General Accounting Office 1996)) are recognised. One of the tasks of security officers is, to get better data quality by improving the identification techniques and policies. A further point is the data need of methods and the information need of different stakeholders. For example, business units do not need the amount of security breach attempts absolutely. For quantifying the business impact of server downtime, it is only necessary to determine the successful security breaches leading to monetary loss in history.

Advantages and disadvantages: Risk analysis is the only method for security planning which considers vulnerabilities, threats, and business impact for valuing security risks. However, there is a large variety of methodologies for risk analysis. Many are either business oriented or technology oriented. Most of them demand a great deal of the risk analysts, because they give no advice in performing the risk analysis, e.g. definition of losses, segregating relevant parts of the IS architecture etc. Risk analysis extends the other methods with a formal cost-benefit-model for security planning with the means to eliminate unprofitable controls (Baskerville 1993). Because – as stated in section 1 – a corporate risk assessment for security risks is often not performed, it is very difficult to state an improvement of security after the security investment has been implemented.

4 VALUATION OF INFORMATION SECURITY INVESTMENTS

4.1 Applicability of value categories on security investments

How are IS investments traditionally measured and why do security investments resist that kind of measurement? The value of IS investments consists of strategic and operative intangible value and tangible value. Businesses often focus on the short term ROI and neglect the strategic value if IS investments (Kohli & Devaraj 2004). A survey performed by (Bacon 1994) showed that monetary aspects are kept in the background if strategic value could be demonstrated. Despite common IS projects, security projects often do not have any distinctive strategic value. In this case, the relevancy of financial evaluation criteria dominates in Bacon's survey with 75%. Unfortunately, security projects often do not have any financial value. Hence, what is needed by security officers, are methods helping them to determine the value of security investments better than with the methods shown in section 2.1.

Risk mitigation seems to be an appropriate means for measuring the performance of IS investments. To determine the risk, top-down and bottom-up approaches can be used. The advantages of the top-down approaches are that gathering and analysing information is quite easy. On the other hand, the

concepts help to quantify post-incident loss, not potential losses and do not help security managers to implement controls internally. In addition, a reasonable statement about the impact is difficult, because the complex capital market does react on many different variables and after one or two days the impact of the incident cannot be proved anymore (see (Garg et al. 2004, Cavusoglu et al. 2004)). The model proposed by Ramachandran & White (2004) is derived from the Business Value Complementary (BVC) model introduced by Barua et al. (1995) that has been designed for evaluating the business value of e-commerce systems. It orients clearly on the business objectives of a company and focuses on the perception of security issues for different stakeholders. For example, a higher security level for a transaction system could highly increase the customer satisfaction. The model is interesting, because it shows managers the effects of a possible investment. But the accountability (as demanded by the practitioners) is still a problem, because financial factors are part of the model, but at the end the question arises, e.g. how much of the increased customer satisfaction can be assigned to a security investment (the difficulties in measuring customer satisfaction set aside). The bottom-up methods try to find out which potential security deficits exist and what controls should be implemented. Most of the traditional risk analysis methods are bottom-up approaches, the risk analysis method shown in section 5.2 is a top-down analysis, because it does not orient on threat scenarios but on business impact.

4.2 Value of security investments in security economy

Financial performance measures do not consider security-specific data (e.g. threats, vulnerability, risk) as a decision variable (Ramachandran & White 2004). As a vehicle, security managers - striving for finding variables to judge the need for a particular investment - developed models discussed in the field of security economics. The first model shown is the common definition of the return on security investment (ROSI). The risk mitigation effects show the benefit of a security investment (Pfleeger & Pfleeger 2003):

$$ROSI = \text{monetary risk mitigation} - \text{cost of control} \quad (6)$$

A security investment is judged to be profitable, if the risk mitigation effect is greater than the expected costs. The formula helps for decisions about one investment, not setting priorities in more alternatives, because it lacks the relation to the capital employed. As a result, the marginal cost of security is in the hand of the decision maker. The understanding of loss (in literature expected loss is used, consideration of unexpected loss would be possible) and loss effects are not defined in the method. ROSI would lead to proper results, if the risk mitigation effects were calculated properly with scenario analysis and expected values. It has been matured in various models trying to consider qualitative variables. But it is doubtful, if variables like *criticality factor*, *exposure factor*, *vulnerability factor* (Microsoft Corporation 2003) help to improve the ROSI concept: The criteria cannot be expressed objectively (and should be already considered in e.g. damage costs or business demands) and therefore the advantage of quantification is weakened by the use of qualitative variables.

Cavusoglu et al. (2004) introduce a solution based on game theoretical considerations. The data input bases on risk (and behaviour) analysis and business considerations. They argue that information security has to do with the behaviour of attackers and defenders. Thus, approaches need to be used, which take into account the goals of the involved parties. Game theory enhances traditional decision theory by considering possible behaviour patterns of both parties (attackers and defenders). They use the method for determining a proper configuration level of an Intrusion Detection System (IDS) by building a game tree consisting of all possible strategies of attackers and defenders. The decision resulting in an optimum of benefit is the best investment. In general, it can be criticised that the method implies an intentional attacker. It is doubtful, if this approach could be applicable for example on worm attacks of the last time (which resemble more a new type of vandalism, not of deliberate acts). However, this approach may help security managers to plan security investments in a limited scope of application.

The model introduced by Ramachandran & White (2004) does not deliver a decision framework for the model. For this, that model cannot be considered further in this article.

4.3 Recommended approach for financial institutions

4.3.1 *Definition of loss*

In this article, loss is defined as a purely accountable measure. This is for four reasons: (1) Intangible effects of loss are often not durable and difficult to separate from other effects, (2) accounting methods must use reliable data to be accepted, (3) quantifying financial loss of operational risk is hard enough and can be fulfilled in the clear borders of Basel II and (4) this does not exclude to take into account intangible/unaccountable loss effects in the management of information security. Information security risk will be underestimated this way (Cavusoglu et al. 2004), but it is more checkable and reliable. The Basel Committee defines legal liability, regulatory action, loss or damage to assets, restitution, loss of recourse, write-down and further considerations (e.g. for external consultants, not for internal labour) as components of operational loss. Banks are free to use broader definitions for internal purposes, e.g. including internal labour or overtime supplements.

4.3.2 *Process model for the measurement of security needs and impact*

ROSI concepts have been developed because of the defects of common accounting models. Risk analysis was introduced as a possible method for giving appropriate data input. Because of the advances of Basel II, methods for building security concepts and the corresponding decision models in security economy should be reviewed again, and security managers should try to integrate into the methods developed by the operational risk function. The effects are the consideration of risk effects and the ability to integrate in common accounting concepts. The subject to risk analysis are the applications used by the business units because they are in the centre of contractual agreements between the IS department and the business units. The risk analysis is performed best top-down scenario oriented, e.g. business units have to quantify costs of unavailability in dependence on the duration, costs of loss of confidentiality, while the IS department must quantify costs of loss of integrity and the probability of these security issues. This results in the business impact of security risks and allows to determine the influence of security on the necessary regulatory capital charge and the expected losses. Based upon this data, a security manager is able to work out a security plan bottom-up.

5 CONSTRUCTION OF A SAMPLE SCENARIO: CONTINUITY OF A PARTICULAR APPLICATION SYSTEM WITHIN BANK

In this section, a simple example will be given to explain the different results of some methods for evaluating a security investment. In section 5.1 the example is constructed and explanations are given. The results are figured out in section 5.2. In section 5.3 the result are discussed and differences worked out briefly.

5.1 Description of the example

A bank has to analyse the effects of discontinuity of an application on operational risk. Therefore, it has collected data about the frequency of this event. The analysis returns the following distribution of the random variable number of loss events (D) during the last year.

| | | | | | | | | | | | | |
|--|-----|----|----|----|---|----|----|----|---|---|----|----------|
| Losses per day (i) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Σ |
| Number of days (n) | 314 | 30 | 5 | 5 | 2 | 3 | 3 | 2 | 0 | 0 | 1 | 365 |
| Number of events ($D = i \times n$) | 0 | 30 | 10 | 15 | 8 | 15 | 18 | 14 | 0 | 0 | 10 | 120 |

Table 1. Distribution of loss events caused by security issues

The mean of D is derived from the database with $\bar{d}=0.3288$. Since the severity S of historical losses has not been recorded very well, the risk managers and security managers agree, that the typical value of S will be 1,000. The expected maximum value is $S=100,000$. Ten loss events have been collected and measured in history. These damages, combined with experts' opinions, are used for estimating the parameters of S , which is assumed to be Lognormal distributed. The mean value of a single loss is $\bar{s}=11,887$ €, the parameters are estimated with $\mu=7.93$ and $\sigma=1.35$ (figure 3).

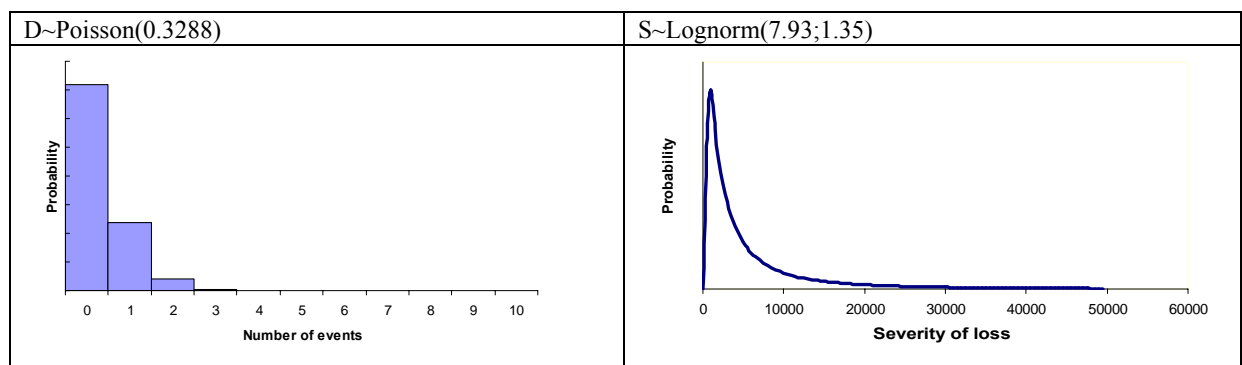


Figure 3. Probability functions for frequency and severity of the event

The analysis of causes shows that 60% of unavailability is caused by problems in the change management organisation when updating software and hardware (including misconfiguration, opening security holes). Adequate change processes could result in lowering D by 30%. Therefore, the countermeasure has only effects on D . The costs of the countermeasure are 250,000 € for organisational improvement and consultancy in the first year with no costs for 4 years. For both scenarios, an aggregate loss distribution must be computed with a Monte Carlo simulation. The simulation has to be repeated for several times to minimise exceptional results (for this case it has been repeated 20.000 times to determine the mean VaR per year).

The VaR on a 99.9% confidence level for one year is computed without countermeasures 1,984,939 € and with countermeasures 1,460,374 €. Therefore the countermeasure will reduce the VaR by 524,465 €, what will result in a capital reduction of the same amount. An additional assumption is that the bank's targeted return on equity (i_{ROE}) is 0.25, the alternative interest rate for the NPV (i) is 0.08.

5.2 Utilising the data for decisions

The data computed above is used in the decision models from the sections 2.1, 2.3 and 4.3 (because of the limited space, only the results are shown in the following). It is now interesting what the decision using a particular model will be and what how comprehensible the data is, i.e. how high the acceptance and usefulness of data is in financial accounting.

| Decision bases on | Result | Decision |
|-------------------|--|----------|
| NPV | $K_0 = -250,000 \text{ €} + \sum_{t=1}^4 (0 - 0) \frac{1}{1.08^t} = -250,000 \text{ €}$ | NO |
| ROSI | $[(11,887 \text{ €} * 0.3) * 120 * 4] - 250,000 \text{ €} = 1,711,728 \text{ €} - 250,000 \text{ €} = 1,461,728 \text{ €}$ | YES |
| Adj. NPV | $K_0 = -250,000 \text{ €} + \sum_{t=1}^4 (240,524 + 524,465 \text{ €} * 0.25) \frac{1}{1.08^t} = 980,920 \text{ €}^2$ | YES |

Table 3. Computed results for the ROSI and NPV methods in a five year period

5.3 Interpreting the results

The results show the divergence of the results. The improved ROSI and the BVC model could not be considered because of the additional information needed. The game theoretical approach was not applicable, because this was not a defender-attacker game. The CFROI and the RARORAC were not used because this was a pre-investment analysis. Left are the NPV, the ROSI approach, and the risk-adjusted NPV. The NPV leads to the dismissal of the project because it considers only monetary in- and outflows but no risk effects. The ROSI works fine for an internal check of the profitability of the project. The risk-adjusted NPV leads to the same decision, but enhances the ROSI methodology with three features: (1) It works with discounted cash flows and therefore is compatible to accounting methods, (2) it includes both expected and unexpected losses used for risk measurement in Basel II and (3) works with a clear definition of risk and loss effects in banks and therefore builds a clear framework for the measurement of investments.

6 CONCLUSION

This article observes information security from an economic point of view and shows the lack of existing methods to evaluate information security investments from this point. The presented solution framework shows that without adequate performance measurement systems, it is hard to prove the benefit of security investments. The solution also shows, that not only an efficient cost allocation mechanism is needed (e.g. to transform information security in a profit centre) but also efficient risk allocation techniques need to be applied in order to make information security a subject for business units. However, the article also shows that the first step to investment analysis is proper risk analysis (with respect to statistical basics) and the definition of basic terms and policies. Further research will have to be done to find methods to segregate relevant IS architecture parts, the procedure of measuring the business impact and the allocation mechanism of risk to the business units to establish a comprehensive risk management framework for information security-related risk.

References

- Aberdeen Group (2004). Security Spend Management. A Benchmark Report.
<http://www.aberdeen.com>.
- Alexander, C. (2002). Statistical models of operational loss. In: Operational Risk - Regulation, Analysis and Management (Alexander, C. Ed.), Prentice Hall, London.
- BSI (2001). Bundesamt für Sicherheit in der Informationstechnik: IT Baseline Protection Manual.

² The capital effects result in savings of 184,274 €.

- Bacon, J.C. (1994). Why companies invest in information technology. In *Information Management - The evaluation of information systems investments* (Willcocks, L. Ed), pp. 31-47. Prentice Hall, London.
- Barua, A. and Whinston, A.B. (1998). Complementarity Based Decision Support for Managing Organizational Design Dynamics, *Decision Support Systems*, 22, pp. 45-58.
- Basel Committee on Banking Supervision (2004). *International Convergence of Capital Measurement and Capital Standards*. Bank for International Settlements, Basel.
- Cavusoglu, H. et al. (2004). Economics of IT Security Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems*, pp. 65-75.
- Dierstein, R. (1990). The Concept of Secure Information Processing Systems and Their Basic Functions. 6th International Conference and Exhibition on Information Security, Espoo (Helsinki), Finland, May 23-25.
- Ekenberg et al. (1995). A Cost Model for Managing Information Security Hazards. In: *Computers & Security*, 14, pp. 707-717.
- Garg, A. et al. (2004). Quantifying the financial impact of IT security breaches. In: *Information Management & Computer Security 2003*, Vol. 11, Nr. 2, pp. 74-83.
- Gerber, M. and von Solms, R. (2001). From Risk Analysis to Security Requirements. *Computers & Security*, p. 577-584.
- Gordon, L.A. et al. (2004). *2004 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute, San Francisco.
- King, J.L. (2001). *Operational Risk - Measurement and Modeling*. John Wiley & Sons. Chichester et al.
- Kohli, R. and Devaraj, S. (2004). Realizing the business value of information technology investments: an organizational process. In: *MIS Quarterly Executive* (1:3).
- Locher, C. et al. (2004). Towards a Risk Adjusted Controlling of Strategic IS Projects in Banks in the Light of Basel II. *Proceedings of the Thirty-Seventh Hawaii International Conference on System Sciences (HICSS-37)*, January 5-8, Big Island, Hawaii.
- McEnvoy, N. and Whitcombe, A. (2002). Structured Risk Analysis. In (Davida, G. et al. Ed.) *Lecture Notes in Computer Science : Infrasec 2002*. Springer, Heidelberg.
- Microsoft Corporation (2003). *Securing Windows 2000 Server*.
<http://www.microsoft.com/downloads/details.aspx?FamilyId=9964CF42-E236-4D73-AEF4-7B4FDC0A25F6&displaylang=en>
- Pfleeger, C.P. and Pfleeger, S.L. (2003). *Security in Computing*. Prentice Hall, Upper Saddle River.
- Ramachandran, S. and White, G.B. (2004). Methodology To Determine Security ROI. In: *Proceedings of the Tenth Americas Conference on Information Systems*, New York.
- Straub, D.W. and Welke, R.J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, December.
- U.S. General Accounting Office (1996). *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. U.S. Government Printing Office, Washington, DC.
- Vossbein, J. (1995). *Konzepte auf der Basis von Schwachstellenanalysen*. Oldenbourg, München/Wien.
- Warren, M. and Hutchinson, W. (2003). A security risk management approach for e-commerce. *Information Management & Computer Security*, 5, p. 238-242.