A Closer Look at Information Security Costs
Working Paper

Matthias Brecht[1] and Thomas Nowey[2]

[1] University of Regensburg, Germany
[2] Krones AG, Neutraubling, Germany

Abstract. Economic aspects of information security are of growing interest for researchers as well as for decision makers in IT-depending companies. From a business perspective cost-benefit-justifications for information security investments are in the focus. While previous research has mostly focused on economic models for security investments or on how to quantify the benefits of information security this paper aims to take a closer look at the costs for information security.
After providing the reader with basic knowledge and a motivation for the topic, we identify and describe the problems and difficulties in quantifying an enterprise's cost for information security in a comprehensive and comparable way with the lack of a common model of information security costs being the most prominent one.
Following, this paper discusses four approaches to categorise and determine information security costs in an enterprise. Starting with the classic approach frequently used in surveys, we continue by describing three alternative approaches. To support research on information security costs we propose two metrics. We conclude with inputs for future research, especially for an empirical analysis of the topic.

Keywords: Information Security, Costs, Economics of Information Security, Cost Model

1 Introduction

Applying methods from microeconomics and business administration to the field of information security has become popular. One important aim of that kind of research is to get a quantitative perspective on information security. In general the advantages of quantification are its accuracy, objectivity, and comparability. In addition, quantification is the basis for calculations and statistical analyses. Nowadays also security investments have to be compared with other investments and cost-benefit-analyses of security investments have to be performed, answering Kevin J. Soo Hoo's question of how much is enough [18]?

So far most research has focussed on economic models for cost-benefit-evaluation and on decision rules. When it comes to data the focus was mainly on the provision of data for the quantification of IS-risks respectively the benefits of information security. In the following we want to take a look at the other side of the balance sheet - information security costs.

Being able to accurately determine security costs is a prerequisite for any cost-benefit-calculation. Another important field of application for a cost model for information security is benchmarking between different companies. This could foster e. g. the comparison of the percentage of the (IT-) budget, or the absolute budget that is spent on information security. To the best of our knowledge until today there is no suitable or applicable model for information security costs in commercial enterprises available. A cost model could be used by e. g. CISOs, budget planners, financially responsible staff or managers as a common basis for communication and for decisions.

The remainder of this paper is structured as follows. Section 2 provides a brief overview over related work. Following in section 3, this paper presents challenges in quantifying information security costs. In section 4 we analyse existing approaches to categorise security costs and present two new approaches to the topic. In section 5, a conclusion of this work as a whole and promising topics for future work are presented.

2 Background and Related Work

Since Ross Anderson has shown the importance of economic aspects for information security research in [3] the topic has been further developed in various directions reaching from behavioral theory to risk management. In the context of this paper it is especially important to consider approaches with a cost-focus that have an application in business administration and risk management.

2.1 Cost-Benefit-Evaluation of Information Security

After a time in which the often cited fear, uncertainty, and doubt (FUD) strategy had been used to sell investments in security (cf. [5]) practitioners as well as researchers are now looking for methods that allow for quantiatively founded cost-benefit-evaluations of information security. To identify costs or benefits of security measures it is necessary to determine both the expected damage before and after a security measure has been taken and the costs for this measure.

In [35] the author points out that information security professionals need to to articulate the value of their activities in business terms. He states that especially during bad economic times, only security initiatives that are able to demonstrate clear business value will be funded. However due to a lack of comparable historical data, security staff must continuously work to evolve alternative mechanisms to capture and articulate the business value of measures. At a project level a possible approach could be to analyse the expected risk reduction, quantifiable financial return or other expected improvements.

[18] states that information security management needs analytic, decision-focused and quantitative techniques to address many of the failings of previous modeling paradigms and to answer the question: How much is enough? During the last decade this changed and IT security management is now increasingly based on economic principles. This also means that a balance between costs and

benefits of IT security is demanded (cf. [27], [28], [32]) and that investments in security have to be geared to the principle of economic efficiency. This includes that in the case of an economic revision they have to withstand the then applied measures. Starting with the idea of a Return on Security Investment (ROSI) several concepts have been developed to support the decision for or against an information measure. On way to do this is to apply the concept of Net Present Value (NPV). [10] developed a NPV-Formular for information security investments:

$$NPV = -I_0 + \sum_{t=1}^{T} \frac{\Delta E(L_t) + \Delta OCC_t - C_t}{(1 + i_{calc})^t} \tag{1}$$

$$\begin{aligned} mit \\ I_0 &= \text{initial investment for security measure} \\ \Delta E(L_t) &= \text{reduction in expected loss in } t \\ \Delta OCC_t &= \text{reduction in opportunity costs in } t \\ C_t &= \text{cost of security measure in } t \\ i_{calc} &= \text{discount rate} \end{aligned}$$

The presented model returns a positive or negative value and thus advises an enterprise to make a security investment or not. The cost of a security measure is treated as a single value without advising how it could be determined. Besides that most of the ROSI-approaches are aimed at single security measures and do not consider information security management.

[16] provide security related cost-benefit guidelines for companies. The authors present analyses and answers to questions like what is the right amount of money to spend and where to invest, but also explains the role of risks in the allocation of resources, strategies to minimise the impact of incidents, and an approach to articulate business values to ensure future funding. In addition, [29] emphasizes the importance of risk management in today's ISM and guides through the different phases of risk assessment and cost-benefit-analyses.

While [26] propose a hierarchical model to assess the security risks of IT, [15] developed an economic model to determine the optimal level of investment in information security, [18] provides a decision analytic framework to evaluate different IT security policies. From the point of view of our research these suggestions all have one major shortcoming: they treat security investments as a black box (see [7]).

2.2 Cost of Cyber-Crime

In the approaches mentioned in section 2.1 the term information security costs always refers to the necessary investments for information security measures. Contrary to that sometimes also the costs caused by a lack of information security – mostly referred to as cost of cyber-crime – are denoted as information security costs.

Although not in the focus of our research it is worth to take a look at this area since the difficulties in quantifying are similar. costs of information security related research This is shown in several cyber-crime surveys. [12] show the discrepancy between several studies that tried to determine the costs related to cyber-crime. The Federal Trade Commission (FTC) estimated the losses due to identity theft in 2004 at $ 47 billion ([8]), in 2006 at $ 15.6 billion ([9]), and in 2008 at $ 54 billion. The huge drop in 2006 seems odd and leads to the assumption that these estimates are extremely noisy. In addition, during the last two years alone, claims can be found that show or predict losses or damages due to cyber-crime from $ 560 million to $ 1 trillion (cf. [21], [20], [36], [2]).

This reveals the difficulties in finding consistent and comparable values and measures for information security related costs. [12] point out that with the existing lack of consistency there remains a large room for interpretation.

2.3 Surveys on information security costs

As shown above in section 2.2 surveys on cyber-crime show a great variety in estimated costs or losses. A similar phenomenon can be recognized when looking at surveys on information security costs.

Every year, several different information security spending surveys are performed, where at least partly surprising results can be found:

- [37] finds that almost 70 % of respondents spend less than 7 % of the overall IT budget on information security, an increase of companies that outsource the entire information security function by 80 %, and 55 % of respondents out of medical practice use either part-time or external staff to handle security.
- [31] states that the security portion of IT budget is expected to rise by 12.6 % in 2009, up from 7.2 % in 2007 and 11.7 % in 2008.
- [38] found an increase in the IT security spending of the Bush administration in 2009 of $ 646.8 million. Agencies as a whole would spend 10.3 % of their IT budget on information security. Spendings for cyber-security were planned to be increase by 73 % since 2004.

Standards or universally accepted conventions e. g. for structures of IT costs are to the best of our knowledge not available.

2.4 Definitions

Especially due to the growing importance of economic values for any enterprise, it is increasingly important to measure the efficiency and effectivity of security measures (cf. [22]). This makes it necessary to identify costs and benefits. [23] defines costs in the context of ISM as the evaluated use of resources in monetary terms. The same author states that the benefits of security management are often expressed as the avoided damaged. Before a security measure is introduced an objective estimation of these two values is used to decide whether it will be deployed or not. Afterwards, the decision that was made should be revisable and comprehensible.

For the purpose of this article it is necessary to define the term information security costs more precisely. We identify four main interpretations of the term (see figure 1):

1. The costs that are caused by information security incidents.
2. The costs for managing information security.
3. The costs that are related to information security measures.
4. The costs of capital that are induced by information security risks.

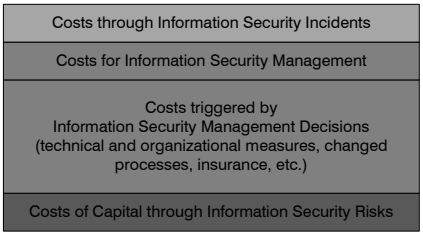

Fig. 1. Four Aspects of Information Security Costs

This paper will focus on the two middle layers. Therefore for the remainder of this paper we define the scope of information security costs as follows:

> The term information security costs refers to costs that are associated with all kinds of measures or activities – including technical as well as organisational aspects – within an organisation that are aimed at reducing information security risks for its information assets.

2.5 Costs of Quality

Well established standards for information security like ISO/IEC 27001 require a management system approach for information security. In this regard there is an analogy to the field of quality management. Some companies even integrate both fields in integrated management systems. Since quality management has a long history it should be worth taking a look at approaches for quality costs.

In [34] the authors give an overview over the field of Cost of Quality (CoQ). They point out that most companies have implemented the so called prevention-appraisal-failure (P-A-F) model stemming from [11] that divides CoQ in three subcategories: the cost for failure prevention, the cost for failure approval plus the cost induced by failures. Besides the P-A-F-model there are numerous approaches for categorising CoQ. The choice of the appropriate model depends on factors like purpose, situation, environment and individual needs [34].

According to [34] companies that adopt CoQ concepts improve their quality while reducing the cost for quality. Yet the authors also point out one main

difficulty in assessing CoQ: Since most CoQ measurement methods are activity oriented they do not mesh traditional cost accounting that is more expense oriented. Consequently there is no standard procedure for determining and categorising data on quality costs.

3 The Challenges in Quantifying Security Costs

It is widely agreed that quantifying the benefits of information security measures is hard (see for example [30]). In this section we present multiple issues that underline that also the quantitative determination of costs related to information security has to overcome some serious challenges.

3.1 Information Security as a cross-functional Task

During the past decade we have seen a development from it-security to information security. Information security covers all activities to protect the confidentiality, integrity and availability of an organization's information assets. Therefore it is widely agreed that inforamtion security is more than just technical measures. Providing information security is a cross-divisional task that encompasses technical (e.g. hardware, software) as well as organisational (e.g. employee trainings, processes) aspects. With information security awareness becoming more ande more important virtually every employee in a company can do her bit to provide information security.

This cross-divisional nature is a huge challenge for categorising and analysing information security costs. On the one hand information security costs can not be easiliy mapped to one single category of traditional cost accounting. On the other hand it is not easily possible to define what part of the costs of a measure are directly accountable to information security.

Even in the case of an investments, which costs are closely related to information security, such as very strict programming guidelines or the operation of a firewall, it may be hard to determine that part of the investment that may be accounted to information security. Programming guidelines are used to improve the security of a company's products, but in a case where employees write hundreds or thousands of lines of code (LOC) a day no one can tell what amount of time is really invested into security. Also, a hardware firewall is definitely a security product, but if it can also act as an e-mail gateway, are really all related costs accountable to security?

The aforementioned examples show one of the problems that occur during the management of information security; it is hard to determine if a task is an information security task or if it is another task with some part concerning security.

Another problem is revealed when we look at the focus of information security management. Information security management is a systematic, long time, cross-divisional task with the aim of protecting a company's assets and goals (cf. [17]). Since expenses for security are in general made to meet the goal of long-term

security, security products are usually very complex. Often, the initial costs (e. g. purchase price of the product, the product's introduction, operation, but also security-related adaptations of business processes) may only account for a fraction of the overall costs. This does not only mean that the decision for or against security investments need to be considered carefully, but also makes the determination of the actual costs of a security measure much harder.

3.2 Divergent Goals of Cost Quantification

Organisations have different reasons and goals for quantifying costs in general and information security costs in particular. Each of the information needs may require a different perspective on information security costs to appropriately answer the question. Table 1 provides the reader with a brief overview. Thus a flexible cost model is required that can satisfy different demands by enabling different perspectives on information security costs in the enterprise.

Goal	**Explanation / Implications**
budgeting	providing guidelines of how much may be spent, categorization to provide internal comparability, orientating towards general controlling and accounting guidelines
cost accounting	usually, no special way of dealing with security, main goal is to meet compliance regarding financial aspects
benchmarking	comparability with other organizations, identification of differences, point out different strategies or starting points
risk management	preparation for controlling decisions, determine advantageousness of measure
cost-benefit-analysis of Investments/Projects	economic assessment of certain measures/projects, return on investment analyses, the overall costs of a measure or project need to be identified
surveys / research	identification of trends, tendency towards higher/lower security spending, determination of preferences (technical/organizational measures)

Table 1. Goals of Cost Quantification

3.3 Hidden Costs: e.g. Security-Related Outsourcing

A major challenge in analyzing security costs are what we call hidden costs, i.e. costs that are at the first glance not directly related to a security risk management decision but indirectly caused by it. A good exmaple is the field of outsourcing, where various hidden costs have been identified in the past.

[33] states that the investments in security services will continue to grow steadily over the next years. One of the main reasons the author sees is the

increasing popularity of Managed Security Services (MSS), which changes the market significantly. MSS describe the outsourcing of operation and management of an enterprise's security solutions in order to save money, but this outsourcing relationship has to be managed and its results have to be reviewed and verified. For an overview of IT outsourcing see [24].

[4] identified four often forgotten and hidden costs of IT outsourcing. These costs are categorised into costs that occur during the search for a suitable vendor and the contracting phase, during the transition phase of switching the in-house delivery of a service to another company, or during the transition from the outsourcing partner to another outsourcer or the reintegration of the formerly outsourced service. In addition, also costs for the management of the outsourcing relationship (e. g. monitoring, bargaining, and renegotiation) must not be forgotten.

3.4 Difficulties in Finding the Right Baseline

An additional challenge especially for benchmarking of information security costs is finding the right baseline. As one can see from the facts mentioned in section 3.1, the nature of information security costs makes it unlikely that this kind of costs can be seen as a subset of IT costs and thus be put in relation to the overall IT budget of a company. This procedure may work for IT security costs but in the case of information security costs one will always only be able to cover parts of the overall costs, since IT security can be seen as a subset of information security, regarding only an organization's IT.

While some results show that with the increasing number of security threats and incidents also the budget spent on information security in relation to the overall IT budget rises. Other results show that especially in industries with highly sensitive information, the importance of information security may not have been fully understood. In addition, it seems that in bad economic times other topics that may help companies to increase their profits or strengthen their market position have higher priority (cf. [6]). In general, most of the above shown results use the overall IT budget of a company as the main reference. This is – at least partly – problematic since the costs that are accumulated to the IT budget may be significantly different for several companies or industries. For example, the costs for telephony and mobile telephony are part of the IT costs in some companies while in others they are not.

4 Towards a Model for Categorising Information Security Costs

The challenges identified above lead to the conclusion that a common understanding of information security costs is required. Therefore a common way of categorising and structuring costs in a repeatable and comparable way is required. Building on that basis it becomes possible to identify cost-drivers and to analyse different security management approaches. In the following we present

different approaches to structure information security costs. We will refer to such a categorisation by the term cost model. Thereby we will focus on enabling benchmarking between organizations, but will also take a look at other areas of application.

4.1 Approach 1: The Balance Sheet Oriented Approach

Benchmarking initiatives frequently are driven from the controlling or accounting department. Thus it is quite common to use structures for classifying costs that are oriented towards the chart of accounts. A typical example for that type is the model developed by the consulting firm Gartner[3] for Total Cost of Ownership (TCO)[4] analyses of Information Systems (cf. [13]). Equally for the field of information security Gartner chose an approach that could be called balance sheet oriented.

To cover the costs spent on information security Gartner uses a scheme, which distincts between the four different cost categories presented in table 2.

Cost category	**Description**
Personnel Costs	Includes all personnel costs supporting information security functions
Hardware	Dedicated security hardware (e. g. security gateways, disaster recovery hardware)
Software	License costs of software dedicated to managing security systems (e. g. IAM, endpoint security suites)
Outsourcing/Managed Security Services (MSS)	Costs of monitoring/managing security devices, systems and processes or other costs related to MSS

Table 2. Cost Categories for Information Security used by Gartner [14])

For the year 2011 they found a distribution of the inforomation security budget in 21 % hardware, 29 % software, 40 % personnel and 10 % outsourcing.

In general, this approach is a first step towards the classification of information security costs. The classification in hardware, software, personnel and outsourcing may also be good for IT-related budget planning.

As already shown in section 2 the classification of security costs into hardware or software is problematic, if at all possible.

So, Gartner's approach leads to a situation in which comparability between several industries or even single companies – due to a lack of transparency in the procedural method – cannot be provided. However, this approach allows companies to easily determine their costs in those categories because of existing

[3] http://www.gartner.com

[4] TCO is a financial approach to help managers or consumers to estimate the overall costs of a product over its whole life cycle. It can also be used to determine the economic value of an investment and contains both, acquisition and operation costs.

accounting/budgeting processes. On the other hand, a more detailed analysis of the results of this approach is not possible. Too much information about the creation of reference data is missing or unclear. Thus, a comparability between several companies may hardly be possible. In addition, this approach focusses more on IT-security than on information security.

4.2 Approach 2: The security measure life-cycle approach

Especially when it comes to investment decisions on information security measures, decision-makers have the goal to capture the total cost of ownership (TCO) of a measure. This leads to an approach that not only covers the cost of purchase for a security measure but also other costs within its life cycle. An example of such a categorisation is sketched in [30]:

- costs of purchase
- costs of setup
- costs of operation
- costs of change

This approach is well-suited for cost-benefit-analysis of single measures since it covers all aspects of costs that are connected to the implementation of a security measure. The values can thus be compared to the potential benefits (mainly risk reduction) of a security measure. Likewise the approach can be used for the sel of different security measures.However it is hardly possible to apply this approach to a company's information security management as a whole since it lacks a process perspective and is mainly focussed on IT. In addition, this approach is not suitable for benchmarking between several companies as no reference values are calculated or presented.

4.3 Approach 3: IT-security process oriented approach

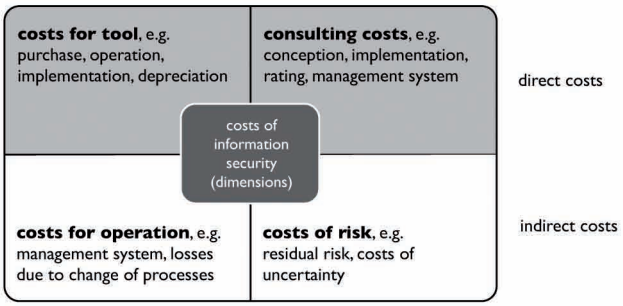

Fig. 2. Dimensions of Information Security Costs (cf. [19])

The categorisation proposed by [19] is depicted in figure 2. It gives a comprehensive picture of costs associated with IT-security activites. The focus is on single security measures though especially costs for operation also cover some high-level aspects like change of processes. The approach covers all of the four cost aspects of section 4.2 in one category (cost for tool) making it more comprehensive. Nevertheless it is still focussed on IT-security.

The categories leave room for interpretation, e. g. some may have the opinion that the complete part of costs for operation should be accounted to the costs for tool section. This and the fact that the categories are not compatible with standard cost accounting models complicate the collection of data.

Another fact that may lead to controversy is mentioning costs of risk as actual costs of information security. [25] states that higher risks, which also means higher uncertainty, leads to higher interest rates for fresh capital. The reduction or elimination of risks, which is a major goal of the management of information security, would lead to lower interest rates and so decrease these costs. In any case information security measures should rather be seen as a means to reduce risks than as a trigger for risks.

All of the models mentioned so far try to categorise costs of information security, but tackle their goal in a completely different way. This is another proof for the need of a universally accepted and applicable cost model to provide comparability and a universal understanding of the topic.

Since providing comparability and several industries or single companies is one of the main goals of cost model we hope to develop, we will propose our own more specific approaches to classify and determine the costs for information security in an enterprise in the following sections.

4.4 Introducing Determinability and Security-Cost-Ratio

This paper introduces two new metrics that should help to describe and determine the cost ratio of a security measure or investment.

Especially when it comes to benchmarking between organisations we are facing the challenge that some of the cost categories may be very unambiguous and easy to determine while others leave much more room for interpretation. Companies should be aware of that fact when interpreting deviations from the benchmark. Therefore

determinability describes how difficult the determination of the related costs is in practice. The value of determination is indicated on a scale from “easy” to “hard”, with intermediate steps of “easy – medium”, “medium”, and “medium – hard”. For example, the determinability of the control “human resource management” is defined as “medium – hard”. With empirical data available we could also analyse the statistical spread.

A challenge that is closely related to the latter is the decision of proportion of a cost category should be attributed to information security.

Information Security Cost Ratio describes the real percentage of the costs that may be accounted to information security. This value is indicated on a scale from "low" to "very high". Intermediate steps are "medium", "high – very high" and "very high".

4.5 Approach 4: The ISO/IEC 27001 oriented Approach

The international standard ISO/IEC 27001 has a high acceptance and distribution in companies around the world. This section will provide an approach or categorising the costs of information security based on the ISO/IEC27001 standard (cf. [1]). The different controls that are relevant for information security are shown and described in table 3.

This approach should provide organizations with possibilities to determine costs of the controls and control areas and guide companies in their decision on how much to invest in which control.

For the support of business decisions like this distinguishing between hardware or software, as suggested in section 4.1, would not provide any help for an organization (cf. section 2.1).

Besides the explanation of the cost aspects, 3 also gives an indication for the values of determinability and information security cost ratio. Some examples are especially noticeable: Within the human resource management, mostly only some parts of certain processes are information security motivated. The determination of these ratios is definitely not easy, but requires a detailed analyses of these processes. The information security cost ratio of "information security incident management" was set to be "very high". This is the case because this control can be seen as very closely related to and almost exclusively motivated by information security management. However if an organisation uses its conventional incident management processes also for information security incidents the information security cost ratio may be significantly lower.

The tasks of managing information security in an organization can be seen as an information security task. And also the technical aspects of this control are usually only information security motivated. Thus, its costs can mostly be seen as information security costs only.

Since there is a lack of related literature, the chosen values derive from the practical experience of the authors of this paper. These values (especially the information security cost ratio) need to be researched in detail and should be subject to future research towards a cost model of information security costs (cf. 5.2).

This discussion reveals that the costs of information security can originate from various different departments or directions. For several controls only parts of the overall costs can be accounted to information security. In addition, one might argue that, for example, the control human resource management and thus its costs can not be seen as part of the IT budget of a company. The same may be true for physical security.

In general, the mentioned controls and related measures could be further classified. For example regarding their main aspects like

Control	**Description**	**Determinability**	**Information Security Cost Ratio (%)**
security policy	Controls to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations	easy	very high
organization of information security	Controls for the organization of an enterprise's information security	medium	very high
asset management	Controls for the management of an enterprise's assets (e. g. (de)classification, related controls)	medium	medium
human resource management	Controls for the reduction of risk of human error, fraud, theft or misuse of facilities (e. g. security motivated training)	medium – hard	low
physical and environment security	Controls to achieve security due to the prevention of unauthorized access, damage and interference to business premises or information	easy – medium	medium
communications and operations management	Controls in order to ensure the correct and secure operation of information processing facilities	medium	medium
access control	Controls to ensure only authorized access to information	medium	high
information systems acquisition, development and maintenance	Controls for security motivated/related costs for purchasing, development or maintenance (e. g. security hardware/software, but also security features of "normal" hardware/software, also related research)	medium	medium
information security incident management	Controls to help dealing with information security incidents (e. g. detection, investigation, resolution)	medium – hard	very high
business continuity management	Controls needed in order to ensuring business continuity or disaster recovery	hard	medium
compliance	Controls to avoid violation of civil law, statutory, regulatory, contractual obligation or any other security requirements	medium – hard	medium
ISMS	The mandatory parts of the Information Security Management System as described in Chapters 4-8 of ISO/IEC 27001, including for example risk management, internal audits, reviews, etc.	easy – medium	very high

Table 3. Overview of Information Security Costs (According to Appendix A of [1])

- organization,
- people
- technology or
- processes.

It goes without saying that it is possible to implement and operate information security measures that are not mentioned in appendix A of the ISO27001 standard. However for the purpose of benchmarking the participants need to agree on a set of common controls.

So far we have only coverd the controls that are part of appendix A of ISO/IEC 27001. The information security management system (ISMS) itself – being obligatory and containing activities like risk management and internal audits – can be found in chapters 4 – 8 of the standard. Even if harder to categorise this part of the standard should also be part of a cost model, e.g. as one block ISMS-costs.

Since the ISO/IEC 27001 standard is well accepted, widely distributed and standardized, this approach is well-suited for benchmarking and research. In addition, due to the fact that management aspects as well as technical and organizational measures are covered, this approach can also be used to provide an organization's security management with an overall view. However, since single security measures cannot be examined in detail, this approach is not suitable for cost-benefit analyses.

4.6 Approach 5: The ISMS-Layers Approach

Our second proposed approach takes the perspective of information security management. To achieve a top-down determination and classification of costs for information security, we suggest an approach that basically consists of four layers, plus basic prerequisites. In contrast to other approaches, like the one distinguishing personnel, software, hardware and outsourcing mentioned in section 4.1, we are looking for an approach that better meets the cross-divisional characteristics and nature of information security. In addition, this approach could easily provide the possibility to compare if an organization, for example, spends too much money on management tasks or too little on a certain type of security measures.

An overview of this approach is shown in figure 3. Next to each of the five layers of this approach, blue circles are located, indicating the ratio of the costs that are directly accountable to information security (information security cost ratio). In the same way as in section 4.5, these are vague, approximate values, set provisorily. These values also derive from the practical experience of the authors of this paper and should be scientifically and comprehensible determined in future research work (cf. 5.2).

Details to each of the layers and their information security cost ratio, in ascending order, are presented in the following paragraphs.

The bottom layer builds the basis of this approach and describes the prerequisites of an efficiently and effectively working information security management.

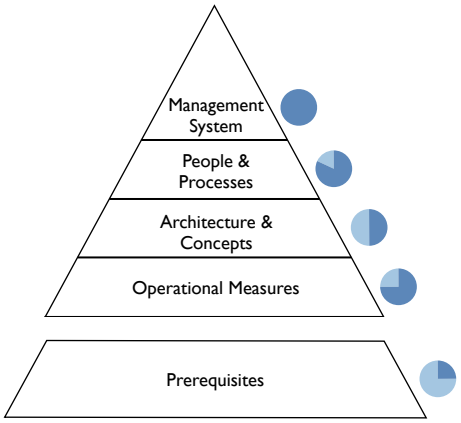

Fig. 3. The ISMS-Layers Approach

Since these prerequisites (e. g. inventory of assets, or the introduction of information ownership) are necessary management tasks to provide security for an enterprise's assets its costs should not be accounted to information security, since this would falsify the results. However information security management is frequently the trigger for providing theses basics or at least it requires the documentation of some additional attributes. As a compromise, we suggest an information security cost ratio of approximately 25 % for this layer.

The second layer is called "Operational Measures"; it consists of what one would typically call information security measures: measures like virus-protection or encryption software. Mostly, measures of this layer are fully and directly accountable to information security. It depends on the control itself, what ratio has to be applied to determine the information security costs. In the case of a firewall that also acts as an e-mail gateway this ratio can be set to a middle to high value. Thus, we suggest a security cost ratio of 75 %.

The third layer of this approach is called "Architecture & Concepts". It consists of concepts like data protection, data leakage prevention, reporting, IDS or providing security in an enterprise's products, enhanced by architecture tasks like encryption, PKI or IdM. In this layer, the line between information security tasks and other tasks with – maybe only partly – security relevant aspects are much harder to draw. On the one hand an identity management infrastructure can clearly reduce information security risks through approval processes and reporting features. On the other hand by enabling automated provisioning of access rights it also helps to reduce it-operations costs. The determination of the information security cost ratio in this layer is quite tricky, however, we suggest a cost ratio of approximately 50 %.

The next layer is called "People & Processes". It deals with security aspects related to people and processes, such as awareness, security related training,

but also the development and implementation of security controls, policies and guidelines. In general, the optimization or adaption of existing processes and services may in some cases have an influence on a process that is easily measurable (e. g. cycle time), in other cases the influence may not be directly measurable (e. g. long-term awareness-campaigns, training activities, changes in processes). Adding up, a very high percentage of the mentioned costs can be accounted to information security, respectively we suggest a value of 80 % to 85 %.

The top layer of this approach is called "Management System". This layer includes the ISMS including risk management, audits, but also costs for information security related audits, and costs for ISMS software. In our opinion, the costs for ISM, security audits and risk management actions are 100 % information security costs. Usually, ISMS software are highly specialized solutions, which only goal is to support the ISMS. There may be some parts where measures of this layer can be of use or beneficial for other departments or business functions, but those should mostly be negligibly, thus a security cost ratio of close to 100 % is suggested.

In general, this approach is best-suited for benchmarking and for research regarding the performance of different strategies in an organization's security management. The advantage of this approach is the fact that areas with a high information security cost ratio are separated from areas with a low one. In practice, this supports comparisons well.

5 Discussion

A cost model is one important step towards a common understanding and comparability of information security costs. Table 4 summarizes the approaches presented in this paper with regard to their adequacy for different purposes. However the analysis above has shown that one single model won't satisfy all information needs. Therefore combined models are needed and future research on the practicability of cost models as well as on the nature of information security costs is required. Those aspects are briefly discussed in this concluding section.

5.1 Conclusion

In our opinion, it could be useful to combine two – or possibly also more – of the approaches that have been presented in this paper with other ways of classification. It is conceivable that, for example, a combination with the four aspects personnel, invest (hardware, software), maintenance and outsourcing/MSS or also possibly with the four aspects mentioned by Gartner in section 4.1 would lead to an improved understanding, comparability and ease of use.

Especially, the results of cost-benefit-analyses can vary widely depending on the related measure. The measure itself can still be classified, for example, with the help of the approach, mentioned in section 4.6, but this is simply not enough for a cost-benefit-analysis. After the classification, the costs of the measure need to be broken down further. In case of an operational measure, the application

	App. 1	App. 2	App. 3	App. 4	App. 5
focus single measure	o	+	o	-	-
focus whole organisation	o	-	o	+	+
it-security centric	+	+	+	o	-
information security centric	o	-	o	+	+
benchmarking	o	-	-	+	+
cost-benefit-analysis	o	+	o	o	-
comparing measures	o	+	o	o	-
compatibility with ex. data sources	+	+	o	-	-
differentiation by determinability	o	-	o	+	+
differentiation by cost ratio	o	-	o	+	+

+ ≙ appropriate, o ≙ partially appropriate, - ≙ inappropriate

Table 4. Adequacy of Selected Approaches for Different Purposes

of a classical TCO approach could already be sufficient. In case of architectural topics like SSO or PKI this is much harder since only parts of the overall costs can be accounted to the acquisition or operation of the security measure. Other aspects like the adaption of internal processes play a much bigger role here and the measure itself might not even be seen as an information security measure. Even in this case, the complexity of ISM increases; tests, audits but also concepts for the introduction of these measures are not seen as measures themselves, but still – additional costs may incur. Similar problems may also occur on other layers.

After application of the combination one would achieve an overview in form of a matrix where the one dimension would describe the information security costs according to the design of an ISMS (cf. 4.6) or according to the classification of costs according to the ISO27001 standard (cf. 4.5). The other dimension would respectively describe the aforementioned four aspects personnel, invest, maintenance and outsourcing. This would lead to a further break down of the costs of the several layers or measures. Detailed research of these combinations should be subject of future work towards a cost model for information security costs.

This section shows several approaches of how to tackle the aim of being able to determine the costs of information security and achieve comparability. The advantages and the aim of the presented approaches have been identified and

visualized. Depending on the aim of its use another perspective, and so also another cost model may be relevant for an organization:

- For budget planning, the most relevant costs for an organization will probably be expenses that have to be paid to externals, e. g. managed services, costs for hardware and software, license costs, consulting (cf. figure 2, section 4.1).
- For the evaluation of a project or the implementation of a certain measure, basically all costs are highly relevant, i. e. TCO.
- For the benchmarking of IT costs, the most relevant costs will probably be costs for operation, maintenance etc., while costs for the introduction or implementation may be less relevant.
- For the benchmarking of information security costs, a differentiated view depending on the build-up of an ISMS may be the most relevant for an organization. This would provide the possibility to compare if an organization, for example, spends too much money on management tasks or too little on baseline architecture projects (cf. section 4.5, section 4.6).

This list represents only a few. As aforementioned in section 3, the topic of cost models in the field of information security has so far mostly been left out of research. The identification of additional purposes for using cost models may be part of research future work.

5.2 Directions for Future Research

Empirical Evaluation of the Results of This Paper The development of a process for determining security costs in a consistent way is a major prerequisite for an empirical evaluation of information security costs. Only if it is clearly described how to measure the values for the different cost categories in a repeatable way, benchmarking can be successful.

As this paper suggests own approaches to determine and classify costs for information security or for certain information security measures, the next step would be to research the results of the presented approaches in practice. An empirical study among CIOs or CISOs could prove or disprove the information security cost ratios provisorily set for the approaches mentioned in section 4.5 and section 4.6, and also give a first impression if the presented approach will really work in practice.

Determination of Information Security Cost Ratios and Determinability Several possible classifications and ways of determination of information security costs have been presented in this paper. Some of these approaches use cost ratios to make the determination of costs easier. The ratios that have been used in this paper derive from the practical experience of the authors. In general this means, that those values are only estimations to present the idea of the real information security cost ratio. The used values for several controls, measures

or ISMS layers can not be seen as proven values. The detailed and scientific determination of these exact values should be the subject of further research.

The same, in general, applies to determinability. With the help a more detailed and systematical research the set values for the determinability of the costs that are accountable to information security. Regarding this issue, the conduct of a survey among several CISOs or Chief Information Officers (CIO) could be an appropriate method to prove or disprove the values provisorily set in this paper.

Determination and Evaluation of Possible Combinations As aforementioned in section 4 the combination of the approaches, presented in this paper with several other aspects (e. g. personnel, invest, maintenance, outsourcing/MSS, or others) may improve the determinability, understanding, comparability or ease of use of the presented approaches. This would lead to a matrix, in which would help to break down the related information security costs even more. This may provide the user of the cost model with the aforementioned advantages. Thus it might be interesting how the combination of these approached with other aspects or classifications affects these characteristics.

Reference Parameter This paper identifies several problems and discrepancies of surveys (cf. 3). One of the identified problems is the appropriate baseline. In the case of information security the IT budget of an organization is a value, often found in literature. This paper shows, that using this value is not applicable for information security costs as only parts of information security measures and costs can be seen as IT measures and thus seen as IT costs. Often also the turnover of an enterprise is used as a reference parameter. A detailed research of the significance, availability and accuracy of reference parameters in the field of information security and its costs may produce interesting results that could be used in future research.

Identification of Differences Between Several Industries After a practical test of the approach that has been suggested in this paper, another topic for future research could be to research possible differences between several industries. A software development company will encounter much higher costs for secure programming than for example a consulting company. On the other hand, a company that mostly focusses on mechanical engineering faces lower costs for security in products than a company that develops wireless access points or other network components. Extensions or adaptions of the cost model to make it more suitable for different industries can be a topic for further research. Especially for companies that do not only apply information security measures to protect their own information assets but that do also implement security in their products a further differentiation between costs for security in "conventional" products (i.e. cars), costs for security products (i.e. smartcards), and costs for measures to secure an enterprise's information, data or internal systems (this also includes ISM) seems to be essential.

References

1. ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management Systems – Requirements.
2. Edward Amoroso. *Written testimony to the US Senate Commerce, Science, and Transportation Committee*, 2009.
3. Ross Anderson. Why Information Security is Hard - An Economic Perspective. In *ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference*, pages 358–365. IEEE Computer Society, 2001.
4. J. Barthélemy. The Hidden Costs of IT Outsourcing. *Sloan Management Review*, 42(3):60–69, 2001.
5. S. Berinato. Finally, a Real Return on Security Spending. *CIO Magazine*, February 15 2002.
6. Capgemini. IT-Trends 2008, 2008.
7. Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. A Model for Evaluating IT Security Investments. *Communications of the ACM*, 47(7):87–92, July 2004.
8. Federal Trade Commission. Identity Theft Survey Report. http://www.ftc.gov/os/2003/09/synovatereport.pdf, 2003.
9. Federal Trade Commission. Identity Theft Survey Report. www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf, 2007.
10. Ulrich Faisst, Oliver Prokein, and Nico Wegmann. Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. *Zeitschrift für Betriebswirtschaft*, 77:511–538, 2007.
11. Armand Feigenbaum. Total quality control. *Harvard Business Review*, 34:93–101, 1956.
12. Dinei Florêncio and Cormac Herley. Sex, Lies and Cyber-crime Surveys, 2011.
13. Gartner. Distributed Computing - Chart of Accounts. http://www.arsys-europe.net/Propalms/Datasheets/Propalms_WhitePaper_Gartner_TCO_Analyse_for_Distributed_Computer.pdf 2003.
14. Gartner. IT Budget: Information Security & Risk Management Spend Metrics. http://www.gartner.com/technology/metrics/it-security-risk-spending.jsp, December 27 2011.
15. Lawrence Gordon and Martin Loeb. The Economics of Information Security Investment. *ACM Trans. IS Security*, 5(4):438–457, November 2002.
16. Lawrence Gordon and Martin Loeb. *Managing Cybersecurity Resources: A Cost-Benefit Analysis*. McGraw-Hill, 1 edition, September 28 2005.
17. Marcus Holthaus. *Management der Informationssicherheit in Unternehmen*. PhD thesis, Universität Zürich, 2000.
18. K. J. S. Hoo. *How Much Is Enough? A Risk Management Approach to Computer Security*. PhD thesis, Stanford University, 2000.
19. Frederik Humpert-Vrielink and Nina Vrielink. Ganzheitliches Sicherheitskosten-Controlling. http://www.kes.info/archiv/online/kostencontrolling.html.
20. SSG Inc. Cyber Crime - The Facts. http://www.ssg-inc.net/cyber_crime/cyber_crime.html.
21. Stuart Kendrick. The Morphing IT Security Landscape. https://vishnu.fhcrc.org/security-seminar/IT-Security-Landscape-Morphs.pdf, November 2010.
22. Gerald Kovacich and Edward Halibozek. *Security Metrics Management: How to Manage the Costs of an Assets Protection Program*. Butterworth-Heinemann, 2006.

23. Martin Kütz. *Controlling der Information Security*, chapter 03710. Number 32. Aktualisierung September 2011 in Praxiswissen IT-Sicherheit: Praxishandbuch für Aufbau, Zertifizierung und Betrieb. TÜV Media - Dieter Burgartz and Ralf Röhrig, 19 edition, 2011.
24. Kim Langfield-Smith and David Smith. *Managing the IS Outsourcing Relationship*, chapter 10, pages 163–188. Advances in Managing Information Systems. Information System Outsourcing. S. Rivard and B. A. Aubert, 2008.
25. Christian Locher. Ein Steuerungsmodell für das Management von IV-Sicherheitsrisiken bei Kreditinstituten. In Otto K. Ferstl, Elmar J. Sinz, Sven Eckert, and Tilman Isselhorst, editors, *Wirtschaftsinformatik 2005*, pages 1207–1225. Physica-Verlag HD, 2005.
26. T. Longstaff, C. Chittister, R. Pethia, and Y. Haimes. Are we Forgetting the Risk of Information Technology. *IEEE Computer*, December 2000.
27. Hannes P. Lubich. IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtung. *HMD, Praxis der Wirtschaftsinformatik*, (248):6–15, 2006.
28. Rebecca T. Mercuri. Analyzing Security Costs. *Communications of the ACM*, 46(6):15–18, 2003.
29. NIST - National Institute of Standards and Technology. Risk Management Guide for Information Technology Systems. *Recommendations of the National Institute of Standards and Technology*, 2004.
30. Thomas Nowey. *Konzeption eines Systems zur überbetrieblichen Sammlung und Nutzung von quantitativen Daten über Informationssicherheitsvorfälle*. PhD thesis, Universität Regensburg, 2010.
31. Jonathan Penn. The State Of Enterprise IT Security: 2008 To 2009, 2009.
32. Norbert Pohlmann. Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen. *HMD, Praxis der Wirtschaftsinformatik*, (248):26–34, 2006.
33. Andreas Schaffry. Die IT-Sicherheitsausgaben bis 2015. http://www.cio.de/knowledgecenter/security/2294879/index.html?r=2616952702416512&lid=152021, November 2011.
34. Andrea Schiffauerova and Vince Thomson. A review of research on cost of quality models and best practices. *International Journal of Quality and Reliability Management*, 23:647–669, 2006.
35. Tom Scholtz. Articulating the Business Value of Information Security. Technical report, Gartner Inc., May 04 2011.
36. New Scientist. Cybercrime Toll Threatens New Financial Crisis. http://www.newscientist.com/article/dn16092-cybercrime-toll-threatens-new-financial-crisis.html, November 20 2008.
37. Tom Sullivan. The Surprisingly Small Percentage Health Orgs Spend on Data Security. http://govhealthit.com/news/surprisinlgy-small-percentage-health-orgs-spend-data-security, November 03 2011.
38. Matthew Weigelt. Security Could Consume 10 Percent of IT Budget. http://fcw.com/articles/2008/02/07/security-could-consume-10-percent-of-it-budget.aspx, February 07 2008.