Journal of Information Assurance and Security 5 (2010) 074-083

# Identifying the Cost of Security

Wouter de Bruijn[1], Marco R. Spruit[2], Maurits van den Heuvel[3]

[1] Master of Business Informatics
Institute of Information and Computing Sciences
Utrecht University – Utrecht, the Netherlands
J.W.Bruijn@rn.rabobank.nl

[2] Center for Organization & Information
Institute of Information and Computing Sciences
Utrecht University – Utrecht, the Netherlands
spruit@cs.uu.nl

[3] Accenture
Amsterdam, the Netherlands
maurits@hillmoor-consulting.nl

***Abstract:*** Organizations know that investing in security measures is an important requirement for doing business. But how much should they invest and how should those investments be directed? Many organizations have turned to a risk management approach to identify the largest threats and the control measures that could help mitigate those threats. This thesis presents a framework to support analysis of the costs and benefits of those control measures. This analysis can be performed by using either quantification methods or by using a qualitative approach. Based on a study of five distinct security areas–Identity Management, Network Access Control, Intrusion Detection Systems, Business Continuity Management and Data Loss Prevention–nine cost factors are identified for IT security, and for only five of those nine a quantitative approach is feasible for the cost factor. This study finds that even though quantification methods are useful, organizations that wish to use those should do this together with more qualitative approaches in the decision-making process for security measures.

***Keywords:*** Risk management, IT Security, Security economics, Quantification methods, Management strategies.

## 1. Introduction: Security Governance

In August 2008 an identity theft scheme was stopped when the United States justice department started prosecuting eleven people involved in the scheme [1]. The criminals targeted nine major U.S. retailers and accessed their network by connecting to the wireless networks used by shops of those retailers. They were able to access the network as it had no encryption or hacked their way in despite the encryption. Once inside they tracked and collected credit card data. By going from city to city, a total of 40 million credit and debit card numbers were stolen. The money made by the suspects was allegedly transferred to bank accounts in Eastern Europe, where a few of the eleven suspects were located. It was unclear how much money exactly was stolen through the identity theft scheme, but the losses for the involved companies could run into well over ten million U.S. Dollars. If the involved retailers had stronger encryption in place for their wireless networks the hackers would have not been able to gather this amount of confidential data. The scheme is a clear example where investments in information security may have reduced the horrendous extent of the security debacle. It is an important requirement for all organizations to keep their information assets secure.

Security is a trade-off, however. A major data breach can cause a company to eventually go under. On the other hand a too restrictive environment where employees cannot access the resources they need to do their job can lead to productivity problems as well. If organizations know the exact costs and benefits of a security measure this will help them in the decision making process. There are methods and approaches that try to do this. Some of the cost factors of a security measure can be quantified. For others, it might be better to have a qualitative approach. But to calculate future costs they will have to make assumptions. If these are wrong, they will base their decisions on false data. Furthermore, for companies, it is not just about one implementation; if a company installs the best firewall out there but outsiders can easily access the wireless network from the parking lot of the building, security still is weak. Executive managers making the decisions will have to realize that making a measure in one area influences the validity of other security measures already taken.

From the outline above it should be clear that making decisions in information security is a difficult task. In the complex environment with a multitude of factors troubling the view, making the right decisions is hard. Many companies resort to baseline measures as presented by standards and best practices. Even though this approach gives a good overview of what is needed in the security strategy, to make the strategy completely fit the organization, the approach should fit the unique aspects of the company. Therefore, a risk management approach is needed. In this approach, organizations analyze risks before deciding on measures that can mitigate those risks. A risk management approach allows them to prioritize the risks and to perform an analysis of the costs and benefits for the right mitigation options. This paper presents a framework that helps organizations identify the costs whilst doing such an analysis and helps them to calculate these costs. This leads to the following research question:

**What aspects of IT security can be made quantifiable and how can the real costs of these aspects be measured?**

Received September 12, 2009

1554-1010 $ 03.50 Dynamic Publishers, Inc.

This paper will continue with a study of the relevant literature, which especially focuses on the economics of Information Security. Also in section 2 the Risk Management approach will be analyzed together with some of the quantification methods. Section 3 gives an overview of the research method. The main contribution of this paper, the 'Cost of IT Security Framework', is presented in section 4. The final sections of this paper discuss the framework implications, present the main conclusions and suggest several opportunities for future research.

## 2. IT Security Decision Making

Decision making in Information Security is hard. The first researcher who tried to define the reasons for this was Ross Anderson. He argues that the incentives for individuals often are wrong [2]. Perfect rational behavior by individuals can have an unintended effect on security overall. Anderson continues in his paper to show that these perverse incentives can be caused by the structure of the IT market and the lack of visibility for buyers. An example of the problem with the market structure is that software companies will aim at the largest market share. It is in their advantage to deliver their product on an emerging market as quickly as possible. That their product is completely secure is of less importance and severe security holes can be fixed later on. The problem of lack of visibility leads to buyers not being able to distinguish good from bad. Akerlof's example of the market for lemons explains why this happens. If sellers can sell two types of products (good and troublesome products), but the buyers do not know which one they are offered, they will buy at an equilibrium price. Therefore sellers will be better off by selling the cheaper to acquire bad products. The same applies to some security markets as buyers cannot see from the box of a product how much security it really gives them [2].

Gordon and Loeb [3] looked at the same problem from the perspective of a company. They created a model that determines the optimal amount to invest to protect a given set of information. They define the benefits of the investments as 'the reduction in the firm's expected loss attributable to the extra security'. Their model shows that for an information set with a higher vulnerability in general more security investments need to be made, but that in some cases companies are better off by investing in protection for lower vulnerable information.

Rosenberg et al. [4] present some of the difficulties management face when attempting to increase security by mitigating risks from outside attacks. Even when looking at two variables of management steeering, they conclude that the results are vastly different when those actions are combined. This reduces predictability of the outcome.

Research on the economics of security has led to several proposals for a Return on Security Investment-model, such as those from Purser [5] and Sonnenreich et al. [6]. All ROSI models are based on the standard ROI model, which divides the expected returns minus the costs of the investment with the cost of the investment. We have seen some of the problems with quantifying security. Each ROSI-model will need to cope with the inaccurate data problem and the fact that security measures usually reduce the risk up to a certain percentage. We look at how one of these models deals with this. Sonnenreich et al. [6] adjust the ROI model by defining the expected returns as the Annual Loss Expectancy (ALE, explained later) multiplied by the percentage of risk mitigated. So if a security control reduces the risks with 75%, this amount of the ALE should be compared to the investment costs. Sonnenreich et al. argue that inaccurate data might not be as bad as it sounds. As long as they are measured by repeatable and consistent metrics it can give the right answers. As an example they use the advertising industry, which uses the potential viewers instead of the actual number of buyers. Even though they are right that such metrics can be used in ROI-calculations, one has to wonder what consistent measures there are to calculate the probability of, for example, a hacker breaking through the firewall. Kabay [7] argues that the statistical methods normally used in reports have limited use in information security. This is due to not all security incidents being detected and even if they are detected, not all are reported. Furthermore, even if accurate statistics are recorded, it does not mean they can be generalized to all systems and organizations. Other ROSI-models have similar approaches.

In conclusion, no Return on Security Investment model should be used single-handedly to decide on security investments. The body of research on the economics of security shows the reasons for this. This supports the use of a risk management approach in organizations. But this also does not mean there is no place for such models. If informed decisions are to be made for security investments, an analysis of the costs and the benefits needs to be made.

Organizations willing to implementing security measures have several approaches they can take in order to decide the right set of measures to take, but for a good fit with the organization it needs to start with an assessment of the most important assets of that organization. This is why many large organizations choose to tackle security with the risk management approach. This enables them to identify and manage risks threatening the organization. Identified risks are assessed and prioritized based on the magnitude of the loss and the probability of occurrence. The risks are then managed by selecting the right controls, depending on the financial implications.

Several standards exist for risk management. Some focus more on IT systems (such as NIST); others are broader (for example COSO ERM). Especially aimed at information security risk management are OCTAVE by Carnegie Mellon University and ISO 27005. Apart from these differences in the scope, they also target different organizations and locations. For example, OCTAVE is mainly used in the United States and targets small to medium-sized organizations. ISO 27005 is a worldwide standard aimed at large organizations. However, in all standards the following basic steps can be found. As a prerequisite for the full process, organizations should have identified what assets are most valuable to them and have defined the criteria. Based on this, the threats to the assets are identified and an analysis of the exact risk is conducted. This is usually called the risk assessment. Once this is done satisfactorily, the right control measure can be taken. Risks can be accepted, avoided,

reduced and transferred. Risk management is a continuous process. An evaluation of the choices made is necessary and can be used as input for the new assessment [8]. For IT security, the risk management approach brings great benefits. By identifying the biggest threats and the costs involved with those threats, the most important measures will be taken first. It also reduces the chance that vulnerable areas are overlooked. If the right measures are selected, companies can prevent security incidents from happening or when they do happen greatly reduce the impact of the event. Purser argues that this is the key point of information security:

*"The information security process adds value to the enterprise by reducing the level of risk that is associated with its information and information systems."* [5]

In the risk mitigation phase organizations will decide what the right measure is to deal with the identified risks, starting with the highest prioritized risks. If an organization is evaluating possible control measures, it will need to perform a Cost-Benefit Analysis (CBA) to see if the control measure is worth taking. The benefits will be the reduction of the risk. This is where the framework presented in this paper will be used. Also, the CBA can be used to compare several options to control the risk. As its name implies, CBA compares the costs with the benefits. With security related issues, the benefit is often defined as the reduction in expected losses. CBA can be qualitative or quantitative. Mercuri [9] describes some of the drawbacks of the quantitative approach. To correctly compare the costs and benefits, the calculation needs to consider the risk-adjusted cash flow using methods such as IRR and NPV. Furthermore, the investment in one security area can influence the risk and benefits in distinct but related areas. When more things are influenced by one measure, quantifying the costs gets harder. A method that was created for risk analysis in the computer industry specifically is Annual Loss Expectancy (ALE) [9]. ALE uses a simple formula in which the cost of an incident occurring is divided by the chance of that incident happening. For example, an incident costing a company $10 million with a 25% chance of occurring would have an ALE of $2.5 million.

An important drawback of such methods is that the data used as basis for the method often lacks empirical validity. Both the costs and the chance of an incident occurring are estimated. Especially if the incident has a large impact and a low chance of occurring, there usually is no data to justify the exact number and a wrong estimate can have a great influence on the outcome. There are some approaches that try to deal with this problem. Blakley et al. suggest calculating the ALE within a certain range [8], but this range can grow big very quickly. Sun et al. [10] propose to incorporate the Dempster-Shafter theory in risk analysis and include it in the Cost-Benefit Analysis. CBA is a bit more useful in such cases but remains highly dependent on the risk assessment. If risks are exaggerated or underestimated, the outcome of any method used will be flawed. We could know these numbers if we have a statistical knowledge base of computer crime, but there are major difficulties in making an accurate knowledge base [7]. The first reason for this is that not all security incidents are detected. The second reason is that even when incidents are detected, not all incidents are reported for systematic data collection. For organizations, disclosing information about security incidents will lead to bad publicity. So they prefer to solve the security problem internally. A third problem is that even when accurate statistics might have been recorded it still does not mean it can be generalized to all organizations and all types of applications, systems, security measures and operations.

Even with the problems quantifying the costs and benefits of security measures, reality is that any implementation will cost money and companies will only invest in areas that bring them benefits that exceed the costs. So even when it is difficult to assess the costs and benefits, some kind of analysis needs to be done. In those areas where a quantitative approach does not cut it, organizations could move to a qualitative approach, such as using classification methods.

Some security projects are not executed because of the reduction in risk they achieve *per se*, but for other reasons. Compliance is an important driver for many security projects. Laws often require companies to show due care in the protection of sensitive data and some laws define rules for the level of security. A CBA can still be interesting to compare mutually exclusive projects that both help the company to be compliant with the law.

## 3. Research Approach

With the research question and the goal to create a framework in mind, the research method aimed to gather knowledge on candidate aspects and methods for the framework. It was chosen to use design science research as its aims to create and evaluate things that help solving identifiable organizational problems [11, 12]. Before being able to define which aspects are quantifiable and which are not, knowledge of the methods available to determine costs was required. The research started with a literature study on information security to gain knowledge on the state of the field and to learn about the different approaches to security economics. The next step was studying methods that can be used to quantify costs. This involved learning about how and when those methods are used, how they fit within the decision making process in information security and what their limitations are. For most methods, sufficient literature and support is available to get a good overview. Mercuri [9] provides a good starting point by giving an overview of methods used to quantify security costs.

Because of the large size of the field of information security, several areas were identified that could serve as a basis to study the field. Those five areas all include measures organizations can take to reduce threats that may have been identified in the risk assessment and have been selected based on the aspects of the security landscape they cover. For each area, the goal was to define the cost factors that an organization should consider when implementing a security measure. These cost factors were compared for all areas and used as a basis for the overall framework. After determining the categories making up the costs for a security measure in an area, a framework was created depicting the cost factors for that area. This includes a description of the factors, how it influences the total costs and the best way to incorporate the

costs (i.e. quantitative or qualitative and if the former, how the full costs can be calculated). Semi-structured interviews were held both to learn about the security areas and get input for both the smaller frameworks and the overall frameworks, as well as to validate the overall framework. Finally, after investigating what the frameworks for the five areas had in common, those aspects were compared and integrated into an overall framework for IT security. After creating the overall framework, a validation process was performed which is described in the discussion (section 5). The following five areas were identified:

- **Identity Management (IdM)**

  IdM focuses on authentication and access management. In many systems, access should be limited to a group of users and there is a need to know who performed which actions. Identity Management provides organizations with the means to do both. It gives a company the ability to provision, de-provision, declare access status and hand out credentials in an automated manner.

- **Network Access Control (NAC)**

  NAC aims to prevent security problems by performing a check on each device that tries to connect to the network. All devices have to authenticate. The check includes information on the definition file of the antivirus and firewall software and a test on the latest updates for the operating system. Admission is only granted if everything is up-to-date, reducing the threat of an infected computer connecting to the network [13].

- **Intrusion Detection Systems (IDS)**

  The idea of using audit trails to monitor threats was first brought up by James Anderson in 1980. It was only later on when networks got more public that IDS got widespread use. It serves three essential security functions; monitor and detect unauthorized activity and providing the information needed for effective countermeasures. [14]

- **Business Continuity Management (BCM)**

  Disasters happen and security incidents occur. BCM tries to reduce the losses incurred by planning and documenting what to do if disaster strikes. Knowing what to do can greatly increase the speed at which the company is back in business. Business continuity is not only dependent on IT related problems, nor can BCM be seen without IT being a part of it.

- **Data Loss Prevention (DLP)**

  The most important technical asset for companies is not the IT infrastructure, but the data held on the IT systems. Losing valuable documents because of a hard disk crash can cost the company much in lost productivity. Losing data due to a security breach can be even more costly. Data Loss Prevention tries to stop this by controlling what happens with sensitive information and by enforcing policies for confidential data.

Those areas were chosen to study parts of the research domain. Some of the main aspects in IT security were combined. It is a good mix between proactive and reactive measures. The goal for Network Access Control for example is to prevent infected hosts from accessing the network. Identity Management is also proactive as it prevents unauthorized access. Intrusion Detection Systems on the other hand are clearly aimed at detection and allows security personnel to respond to incidents. Business Continuity Management has a bit from both sides: the goal of BCM is to prevent large losses from occurring after an incident has happened (reactively) by defining a recovery plan beforehand (proactively). Data Loss Prevention tries to prevent private data from leaving the company perimeter and as such has a proactive approach. Some of the areas have solutions that rely on technical measures, such as Intrusion Detection Systems, whereas others have a higher impact on processes or the organization. None of the solutions can be seen solely as a technical, process or organizational measure. An integrative solution is required, which is important as any solution that only addresses one aspect will leave weak points [15].

Another aspect that was checked was whether those areas together embodied all of the core objectives in security. In general these are seen as Confidentiality, Integrity and Availability (the CIA-triad of security). NIST [16] adds accountability and assurance to these three. In table 1 is shown how the security areas relate to these objectives. Assurance should be seen as a control for the implementation of each security measure, instead of something onto which security measures can be mapped. Therefore it was added over the other four objectives.

| **Objective** | | **Area:** | **Prevents…** |
|---|---|---|---|
| **Assurance** | **Confidentiality** | IdM | Unauthorized users from accessing resources. |
| | | NAC | Unauthorized users and unsafe hosts from accessing the network. |
| | | DLP | Confidential data from leaving the organization. |
| | **Integrity** | IdM | Unauthorized users from editing resources. |
| | | IDS | Disturbance of integrity of data. |
| | **Availability** | IdM | Unauthorized users from moving/deleting resources. |
| | | IDS | Missing clues on threats. |
| | | BCM | Downtime if availability is threatened. |
| | | NAC | Unauthorized users and unsafe hosts from accessing the network. |
| | **Accountability** | IdM<br>NAC<br>IDS<br>DLP | All these areas have the option to identify the actions of individual users. |

*Table 1.* Security areas fit with objectives

It should be noted that the selected five areas is not meant to be completely exhaustive for the research domain of IT Security. There are areas that have been left out. For example, vulnerability management is an area which will not be studied, as the economic justification goes over company boundaries

(the costs of discovering vulnerabilities is left at one person or company and many people benefit from it) [4]. Some of the areas also do overlap each other. This mainly is the case between Identity Management and Network Access Control. IdM Is used to create rules for employee access. NAC uses this as a basis to authenticate users on the network, also managing access.

For each of the five areas, literature was studied and domain experts were interviewed. In a more emerging area such as Network Access Control, less literature was available and more experts were interviewed. One of them is an associate professor on the topic of network management at a technical university in the Netherlands, and two presidents of a security company that implements one of the NAC offerings. For other areas, at least one expert was interviewed with a large amount of business experience in the field. Based on the cost factors that were identified in this process, five frameworks were made. There was extensive overlap between the areas. Costs had often to do with the procurement of the product and the required hardware, with the creation of policies and the implementation of the security measure in the organization. Furthermore there were future costs such as maintaining the systems and for administration tasks. Studying those five areas resulted in five frameworks for areas that are all related to IT security, but each giving a limited view of the topic. A common pitfall named in the interviews with domain experts in several of those areas is that these measures are seen as a silver bullet; none of them can reduce all the security risks an organization faces, nor should (a combination of) the areas studied here necessarily be the best way to deal with those risks.

Ideally we would have a single framework that can help us define the costs of a security measure, regardless of the area. This should be done carefully. As stated earlier, those areas differ in their approach (proactive or reactive) and in the security objectives they try to accomplish. That was the reason to study them separately in the first place. Research indicates that in the knowledge elicitation process it is important to use experts from a different viewpoint (stratification) to counteract the clustering effect that comes with using experts of the same expertise [17]. This was incorporated in this research by using experts from several domains, organizations and functions, even though all interviewed experts have a high knowledge of IT security. If the same cost factors are found in most of the areas, then these cost factors will always have to be considered when analyzing a potential security measure. The cost factors identified for each section have been compared with each other. In this comparison it was determined that there was enough overlap to make it possible to create such a framework.

The basis of the process to add cost factors to the overall framework was the ubiquitousness of the cost factor. A supermajority rule was used in the decision making process: each factor that was present in at least 80% of the cases would be added to the framework directly. For others it was a more difficult task and it depended on further study whether these could be added. The following steps were taken to determine which factors should be added to the framework:

- Identified similar cost factors.
- Counted the instances. If at least in 4 out of 5, then it will be added to the framework directly.
- Check for different items but with the meaning closely related.
- Group factors together.

After identifying the cost factors that meant the same, the factors were added to the framework that obeyed the supermajority rule. The next step was to determine what to do with those factors that were left over. The first option here is to look if the meaning and the items making up those cost factors are closely related. If this is the case, they can be put in our framework under one common term. One example of this were the cost factors ‘Policies’ and ‘Plans’. Policies are a cost factor in IdM, NAC and DLP. The creation of plans is present in BCM. Both are about rules and guidelines that should be followed and are made up of the same costs, so they can be put in the framework under one name. Items that still are left over might be grouped together. The framework for each area is made up of cost factors that were deemed important enough for that area. In other areas those cost factors might also be present, but not with the same impact as to warrant the same level of detail. The best example of this is hardware procurement and hardware implementation. These two cost factors are related to each other but convey different costs. For some areas, hardware is not as important as in others and as a result only the cost factor hardware was added. By grouping the hardware procurement and hardware implementation together under the cost factor hardware, this item also has been added to the overall framework. Using this methodology all cost factors could be added to the overall framework.

## 4. Cost of IT Security Framework

The overall framework lists all major cost factors that need to be considered when deciding on the implementation of a security measure. Costs are divided in one-off costs and recurring costs. One-off costs occur in the planning and implementation phase. For some of these costs the amount will depend on the current situation; others will be described as from the ground up. Taken together, these costs are the investment that has to be made once. Recurring costs return each year and as such should be handled differently from one-off costs. These costs can be compared with the costs currently made in order to give an idea if the organization benefits from taking this security measure financially in the long-term. With most security measures this will not be the case, but it should be kept in mind that the first and foremost reason to implement such a measure is to reduce risk.

A second distinction is made between cost factors that can be assessed with a quantitative approach and those where a qualitative evaluation is better. This distinction is visualized with an icon. The cost factors were identified as quantifiable based on the input of the experts for each of the domains. The two categories are treated differently in this framework. For quantitative categories, the field “Costs involved” and the explanation following the framework will explain how the monetary value for these cost factors can be calculated. Those with a qualitative approach will also state what makes up this

cost factor, but will continue with an explanation of what makes it so hard to judge the exact cost. Table 2 presents the 'Cost of IT Security Framework', listing the cost factors for measures taken within IT security along with the ways these costs can be quantified, if possible. It consists of nine cost factors. Five of them come with the implementation of a security measure, four of them are recurring and will result in costs that can be measured on a yearly basis.

| Cost of IT Security Framework | | |
|---|---|---|
| **Cost Factor** | **Description** | **Costs involved** |
| **One-off costs** | | |
| **License** | Licensing costs of the tool or product from a vendor. Only required if using a vendor-based solution. | Costs for the license to use the tool or product. Differs per vendor and the optional components. |
| **Policies** | Policies and plans as developed by a team with expertise and insight in the business. The decisions that have to be made as a result of the security measure are defined here. | Costs of a team of people with insight in the business and people with expertise in policy / plan creation for that area. |
| **Hardware** | Hardware procurement, installation, configuration. | Costs of defining the required hardware, finding the best offerings, procuring and installing the hardware and embedding in the network. |
| **Implementation** | The full process of implementing the security measure. Usually this has impact on the infrastructure and the organization. The implementation of the security measure often is phased and can require a long time. | Costs of employees and consultants that guide the implementation process, the implementation and configuration of the security measure. |
| **Embedding** | The embedding of the implementation in the organization. Employees are needed for the administration and need to be hired or get training. Other employees might also need training or at least be notified of the changes. | Costs for training and creating the required awareness of the new measure, and the hiring or relocating of people to perform administration and monitoring. |
| **Recurring costs** | | |
| **Support** | Support costs from the vendor. With some licensing schemes, a yearly fee has to be paid as well. | Depends on the vendor. |
| **Administration** | Costs for updating and configuring the solution. Reflecting changes in the business in the policies. User support (help desk). | Costs of employees performing these tasks and changes that might need to be made to the business. Compatibility problems might lead to higher costs. |
| **Monitoring** | Monitoring the system. | Costs of employees that do the monitoring and act if needed. |
| **Auditing** | Audits and tests performed to assure the correct implementation and workings of the system. | Costs of employees / auditors that perform this task and tasks that have to be done as a result. |

*Table 2.* Cost of IT Security Framework = Quantitative approach = Qualitative

The first cost factor of the one-off costs is the **licensing** costs. These come with any commercial tool or product that is bought. In many security measures a tool or product is the basis of the implementation. Choosing the right vendor is of high importance, as the tool or product should help the organization to reduce the security risks identified with the risk management approach. Organizations should have a good understanding of the requirements for the product and use that as input for making the choice between vendors. Many vendors allow their customers to choose between several packages and care should be taken to select the right optional components. The pricing schemes vary greatly

between the different security measures and between vendors, but can be requested. As such, organizations can know these costs beforehand. Some security measures do not require a vendor-based solution. This cost factor can be ignored for these measures.

All security measures involve making decisions. These decisions have to be made once a security incident happens or are made to define what users are allowed to do and what not. In any case organizations have to define the rules that form the basis of these decisions and use them to create **policies** and plans. An example of such rules that make up these policies is which employees should have access to what resources. This can also explain why bad policies are a threat to security; a receptionist that can access the financial systems of the organization might be able to change her own salary. Good policies are written by people who have good insight in the organization and have expertise with regard to writing policies for that area. It is unlikely that employees in the organization have both. In most cases, a team needs to be formed that consists of people who know a lot about the organization they work in and of contractors that know what they should look for and can write down the policies. If an organization knows the salary and fees to be paid to those people and the time required for creating the policies and plans, they can calculate the costs coming with this cost factor. However, in some areas it will be very hard to estimate the time required making it unfeasible to quantify the costs.

The next cost factor in the framework is **hardware**. Even though security threats are not solved by throwing more IT at the problem, it often is required to install more hardware or adapt the current IT infrastructure. If decision making is automated on the network, the organization will have to install a policy base on a server. The costs coming with hardware consists of those made in multiple steps. First, it needs to be identified what the requirements are. Second, the hardware needs to be procured and this is normally done by choosing between several offerings on the market. Next is the installation of the hardware, to be finalized by embedding it within the current infrastructure. For some of these steps it might be possible to quantify the costs, but overall it is too hard to know beforehand what the requirements will be and more importantly, how it will fit in with the current architecture. If the complexity of the current IT architecture is high, the costs can grow large very quickly.

One of the one-off cost factors that is underestimated the most is the process of the **implementation** of the security measure. In order for the measure to be effective, organizations need to implement the measure carefully and enforce policies. Most implementations can have such a big impact on the organization that it is recommended to use a phased implementation; first test the measure with a small group of users and slowly grow from there. As the time required for the full implementation process depends on the findings in the first steps and the full process entails a number of organizational changes, it is impossible to make a realistic estimation of the costs.

The final one-off cost factor is the **embedding** of the security measure in the organization. As will be described at the recurring costs, employees are needed for the administration and monitoring. These employees might be available within the organization, in which they will usually require training. They also might need to be hired. Most organizations will know how much it costs them on average to hire a new person, based on previous experience. Furthermore, the employees within the organization often need to learn to work with the changes that come with the new security measure, either by training or by being notified. The basic training for the new employees will need to be updated. Training costs can be calculated once the organization knows how many people need to receive the training and what the costs of the training are.

The recurring costs start with **support** costs. This is usually a part of vendor-based solutions, but sometimes support can also be bought in from an external party. Just as with the licensing, the pricing schemes differs per vendor, but can be learned about by requesting these. With some licensing schemes a yearly rate has to be paid. These costs can also be added to this cost factor.

A large cost factor will be the **administration** of the systems. Changes in the business need to be reflected in the policies and that only makes sense if the systems where these policies are enforced are also updated. The company needs to have employees available to do this as well as give users support. This is only quantifiable if employees are doing this full-time and the organization is able to determine how many of them are needed. Otherwise the organization would need to know the time employees, who do this as part of their work, will spend on the administration. This cannot be known exactly beforehand. Another aspect that makes it hard for the quantitative approach is that as the business grows or changes, the configuration of the security measure has to be adapted. This can lead to great variations in costs from year to year.

Finally, **monitoring** and **auditing** are named as a cost factor. Most systems will produce logs stating events and incidents that happened. These need to be checked and acted to if incidents are spotted. An example is an employee accessing resources on the network he should not be able to access. This can indicate a loophole in the system or in the policies and that should be adjusted. Monitoring is a continuous process with the main purpose to identify incidents and start the appropriate follow-up course of events. Auditing is usually done at an interval and is performed as a check on the right implementation and working of the security measure. It can also include test procedures. The costs for the follow-up actions can not be known before hand.

## 5. Validation and Discussion

The first version of the overall framework went through a rigorous validation process. This started off by comparing the framework with those of the five areas; for each area it was asked whether the cost factors were rightly represented in the overall framework. No changes were made after this process. The next phase in the validation consisted of interviews with experts, making this an approach very similar to the Delphi method [18]. The Delphi method is a technique to acquire knowledge from a large group of experts without the disadvantages of group communication. It uses two rounds of interviews. In this research, for the first round of interviews,

performed to create the framework, the experts were chosen based on their experience in that specific area. The experts invited to participate in the validation process were selected for their overall experience in Information Security. Some were asked because of their business expertise whereas others were interviewed because of their academic background. In the Delphi Method the second round is needed to stabilize the findings until the involved experts agree. This is similar as what was done to validate this research. Expert interviews were conducted until a consensus was reached. Table 3 gives an overview of the experts interviewed with regard to the validation of this research.

| Expert Funtcion | Organization | Validated |
|---|---|---|
| Senior Advisor Operational Risk management | Large financial institute | Risk management approach, position of Cost-Benefit Analysis |
| Senior Executive | Large IT consultancy firm | Overall framework |
| Consultant | Small security consultancy firm | Overall framework |
| Associate Professor | Technical University | Scientific method, Overall framework |

*Table 3*. Experts used in validation process

Several issues were identified during these interviews. Some of the cost factors were so broad that they could be split up in multiple factors. This was the case with 'implementation'. In the first version of the overall framework this was used for costs caused from the installation and configuration of the measure, training, hiring or relocating of staff and changes that had to be made to the organizational structure and processes. It was decided to take parts of the cost factor and move it to 'embedding'. A similar change that was made was separating 'monitoring' and 'auditing'. Both were grouped together under one of those names but neither felt comfortable with the experts and it was concluded that both processes differed enough as to warrant two separate cost factors. This also stresses the point that to ensure the proper working of a security measure, the results need to monitored and audited.

Also discussed was whether the experts agreed that the cost factors could be approached with quantitative methods or not. If this was not possible it was tried to define at which moment in time it would be possible to know the exact costs. Even though some cost factors led to lengthy discussions, in the end the experts agreed that the qualitative cost factors could not be calculated. A good example of a cost factor for which the point of knowing the costs comes much later is hardware. At the point of doing the CBA, organizations will not have defined the exact requirements in a high level of detail. When a security measure is implemented, the organization has to give employees the task to find the performance requirements in discussion with the vendor and compare that with the current infrastructure. Once this process is completed the costs for the procurement of hardware can be requested. But there is even more to it. The installation and initial configuration of the new hardware and the adjustments to the current system can also be quite complex, making it hard to know the exact time required for all hardware to work as planned. In most cases, the full costs for procuring and installing hardware will only be known in hindsight.

Besides discussing the cost factors the use of the framework was a topic. The main use of the framework is embedded in doing the Cost-Benefit Analysis during the risk management approach. Those measures that can mitigate the identified risks are analyzed. The goal of the CBA in the risk mitigation phase should be to find out if the benefits of the studied control measure are worth to pay the price that come with the measure. One of the main findings in this research is that whilst some of the cost factors coming with IT security measures can be quantified, for others it is unfeasible to make a realistic estimate of the exact costs at the time of doing a CBA. In considering an implementation, five of the nine cost factors cannot be quantified. This has an impact on the possible routes to take when analyzing a security measure. It makes it impossible to quantify the total cost of the solution. Organizations have several options in choosing how to tackle this problem. They can try to get a grasp of the total costs by using quantitative methods for cost factors where this is feasible and qualitative where this is not the case. With the time required to gather all data and measure the quantitative costs, organizations can also opt to skip quantification methods even when it would be feasible to use such methods for the cost factor. Instead, they can use qualitative methods that can be used for quicker analysis. Either way, by using the framework presented in this paper the organization will know which cost factors need to be considered. Not being able to quantify the total costs is not as bad as it may sound. It is at least as hard to quantify the benefits of a security measure. Organizations would need to know the Annual Loss Expectancy (ALE) of the original situation and the ALE after the IT security measure has been implemented. The benefit is the costs saved in the new situation, which can also be defined as the prevented losses. Just as with the cost factors; it is very hard to calculate the ALE for all measures correctly [7]. So even in analysis of the benefits a qualitative approach might be better.

The problems with quantification of both the costs and benefits make it highly unlikely that organizations can define the exact amount of prevented losses against the exact costs beforehand. This should be realized when trying to quantify this and not base there decisions solely on the quantitative analysis. But this does not mean there is no value in trying to quantify the costs. In trying to assign a value to them, organizations can get a better idea of the benefits, advantages and disadvantages of a solution, leading to better results of the decision making process [5].

A second use of the Cost of IT Security Framework, outside of the risk management approach, can be found when updating the implementation of a security solution. This might be needed due to changes in the business and as a result of problems found in monitoring and auditing. If the required changes are large enough to warrant careful analysis it can be made a project on its own. Organizations should start such a project with an analysis to see whether the updates are really worth implementing. This analysis can use the Cost of IT Security Framework. Licensing costs are often not required, but the other cost factors have to be studied and compared to

the recurring costs in the current situation. If the required changes come with high costs and only show a low improvement in security, then organizations might be better off to not implement the solution and stop the project here. If the organization is better off with the changes, it will start to plan and implement those changes, which after the implementation will have influence on the running of the security solution.

## 6. Conclusion and Future Research

This paper presented a framework to be used by organizations during a Cost-Benefit Analysis of an IT security measure. The framework focused on the cost factors. For each of the cost factors it was determined whether they could be quantified. Furthermore, the framework describes for each cost factor what costs are involved. The framework was created by studying five security areas. For each of them, literature in those areas was studied and domain experts were interviewed. The cost factors identified for each area had enough cost factors in common to justify the statement that these have to be considered for IT security in general. The Cost of IT Security framework has been validated by further interviews.

The research question this paper tried to answer was on the quantification possibilities of IT Security. The answer to the question is that it is possible, but only in selected cases. In an ideal world, we would be able to know exactly what would happen when implementing a security measure and we could calculate the exact costs and put the correct value to the benefits. In reality, this is not the case. Five out of the nine cost factors identified cannot be quantified. Some cost factors involve a time consuming process where the total costs depend on the outcome of the first steps. Others have to do with maintenance and monitoring and have costs that can vary per year. Even though not all cost factors can be quantified, it does not mean that there is no purpose in doing so for the cost factors where this is possible. There are methods available that given correct input can produce the numbers. The quantification can be used to give an indication of the total costs. Furthermore, in doing so the organization has to think about the implications of implementing such a measure. This decision making process will lead to a more realistic view when a security measure is actually implemented. Still, care must be taken not to overstate the importance of quantification methods. Organizations should have a weighted approach, using risk management to prioritize those aspects with the biggest impact.

The main use of the framework is within the risk management approach. By identifying the risks and prioritizing them based on impact, the most important risks can be tackled first. For each security measure analyzed to mitigate those risks, during the CBA it should be investigated if it really reduces the intended risk (the benefit of the measure) and whether the cost to do this is acceptable. In analyzing the costs, the Cost of IT Security framework presented here can be used. If organizations have more options and those are mutually exclusive the framework allows for comparing the costs involved. Given the same level of risk reduction, organizations can opt for the measure that is most cost effective. Decision making in security should not be based on a quantitative analysis of the costs of benefits only. It is too hard and time consuming to perform this task, and no guarantees can be made about the correctness of the outcome. But this does not mean there is no place for quantification methods. Some sort of Cost-Benefit Analysis needs to be made, and the outcome of the decision making process can be improved by quantification methods, as long as the limitations are kept in mind.

Opportunities for future research include further study in the role of the Cost-Benefit Analysis for IT security measures. The framework in this paper only looked at the cost factors. The other side of the CBA, the benefits, has been described in this text. Nonetheless, future research could study how this framework could be extended or used as the basis for a method for the full CBA. The scope of the framework has been limited to IT security, so that the areas that were studied had that aspect in common, making it more likely that similar cost factors would be found. Undoubtedly, some of the findings in this paper are valid throughout the full landscape of security. The risk management approach does not only find IT risks, but also many others. Future research could validate the cost factors identified in this framework in information and physical security. Also, the cost factors could be compared against those that make up the costs for IT projects. It would be interesting to see how much IT and security projects have in common. This paper concluded that a Cost-Benefit Analysis is helpful, but the time spent and the way of doing it should fit the type of risk. Decision makers in security would be helped by research that guides them in selecting the right form of CBA.

## References

[1] BBC News. *US cracks biggest ID fraud case,* 2008**.** Retrieved November 9th, 2009 from http://news.bbc.co.uk/2/hi/business/7544083.stm

[2] Anderson, R. “Why Information Security is Hard - An Economic Perspective”. In *Proceedings of the 17th Annual Computer Security Applications Conference*, pp. 358-366, 2001

[3] Gordon, L.A. & Loeb, M.P. “The Economics of Information Security Investment”, *ACM Transactions on Information and System Security*, vol. 5 (4), pp. 438–457, 2002

[4] Rosenfeld, S.N., Rus, I. & Cukier, M. “Modeling the ‘Tragedy of the Commons’ Archetype in Enterprise Computer Security”. *Journal of Information Assurance and Security*,vol 4 (1), pp. 10-20, 2009.

[5] Purser, S.A. “Improving the ROI of the security management process”, *Computers & Security*, vol 23 (7), pp. 542-546, 2004.

[6] Sonnenreich, W., Albanese, J. & Stout, B. “Return On Security Investment (ROSI) – A Practical Quantitative Model”. *Journal of Research and Practice in*

*Information Technology*, vol. 38 (1), pp. 45-51, 2006.

[7] Kabay, M.E. "Understanding Studies and Surveys of Computer Crime", in *Computer Security Handbook*, Bosworth, S., Kabay, E. & Whyne, E. (eds.), Wiley, New York, 2009.

[8] Blakley B, McDermott E. & Geer D. "Information Security is Information Risk Management", *ACM New Security Paradigms Workshop*, 2008.

[9] Mercuri, R.T. "Analyzing Security Costs", *Communications of the ACM*, vol. 46 (6), pp. 15-18, 2003.

[10] Sun, L., Srivastatav, R.P. & Mock, T.J. "An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief", *Journal of Management Information Systems*, vol. 22 (4), pp. 109-142, 2006.

[11] Hevner, A.R., March, S.T, Park, J. & Ram, S. "Design Science in Information Systems Research", *MIS Quarterly*, vol. 28 (1), pp. 75-105, 2004.

[12] March, S.T. & Smith, G.F. "Design and natural science research on information technology", *Decision Support Systems*, vol. 15 (4), pp. 251-266, 1995.

[13] Panjwani, S. & Tan, S. "Assessing Trusted Network Access Control Cost-Benefit Factors", in *Proceedings of the Workshop on the Economics of Securing the Information Infrastructure*, 2006.

[14] Bankovic, Z., Moya, J.M., Aruajo, Á., Bojanic, S. & Nieto-Taladriz, O. "A Genetic Algorithm-based Solution for Intrusion Detection". *Journal of Information Assurance and Security*,vol 4 (3), pp. 192-199, 2009.

[15] Hale, J. & Brusil, P. "Secur(e/ity) Management: A Continuing Uphill Climb", *Journal of Network and Systems Management*, vol. 15 (4), pp. 525-553, 2007.

[16] NIST. "Underlying Technical Models for Information Technology Security". *NIST Special Publication 800-33*, 2001. Retrieved November 9th, 2009 from http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

[17] Sutherland, J. W. "Architecting the future: A Delphi-based paradigm for normative system-building", in *The Delphi method: Techniques and applications*, H. A. Linstone & M. Turoff (eds.), Addison-Wesley, Reading, MA, 1975.

[18] Linstone, H. A. & Turoff, M. *The Delphi method: Techniques and applications*, Addison-Wesley, Reading, MA, 1975.

## Author Biographies

**Wouter de Bruijn** is a MSc in Business Informatics. He received his degree in 2008 at Utrecht University based on his research on security costs. He is currently working on the Data Ware House project at Rabobank and is a reviewer for the European Conference on Information Systems. His research interests include Information Security, Security Economics, Risk Management and Information System Management.

Dr. **Marco Spruit** is an Assistant Professor in the Organisation & Information research group at the Institute of Information and Computing Sciences of Utrecht University. His information systems research revolves around Knowledge Discovery processes to help achieve organisational goals through Data Mining techniques, Business intelligence methods, Linguistic Engineering techniques and Web 2.0 technologies. Additionally, he investigates Information Security models and Cloud Computing frameworks as infrastructural safeguards and enablers for Knowledge Discovery processes. Marco initiated his Knowledge Discovery research agenda while performing his PhD in Quantitative Linguistics at the University of Amsterdam. In 2005 he was awarded an ALLC Bursary Award for this work.

**Maurits van den Heuvel** B.Sc. M.Sc. has studied Business Administration (Technical Academy, Rijswijk, The Netherlands, 1996) and Cooperative Computing (Middlesex University, London, 1999). He has worked for ING and Accenture as a risk management consultant and project manager. Currently he is an independent project manager and consultant on Information Risk Management and Process Improvement.