CITS: THE COST OF IT SECURITY FRAMEWORK

MARCO SPRUIT

WOUTER DE BRUIJN

Department of Information and Computing Sciences, Utrecht University, the Netherlands

corresponding author: m.r.spruit@uu.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 research presents the Cost of IT Security (CITS) 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.

INTRODUCTION

In August 2008 an identity theft scheme was unraveled when the United States justice department started prosecuting 11 people involved in the scheme (BBC News, 2008). 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 suspects allegedly stored the information on compromised web servers and would encode credit card information on blank cards. Those cards where used to withdraw cash from ATM's. The money was transferred to bank accounts in Eastern Europe, where some of the 11 suspects were located. It was unclear how much money exactly was made in the identity theft scheme.

Had the involved retailers stronger encryption in place for their wireless networks, the hackers would have not been able to gather this amount of confidential data. The losses for the involved companies could run into well over ten million Dollars.

The scheme is a clear example where investments in information security would have prevented a much larger loss. It is an important requirement for all organizations to keep their information assets secure.

In order to calculate the cost of future security measures 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. This all makes decision making 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. Many of those standards include an approach based on risk management. In this approach, organizations analyze risks before deciding on measures that can mitigate those risks. In some cases, the chance of an incident occurring is so small that so the organization can decide against any preventive measures. A risk management approach also allows them to prioritize the risks. After those risks are assessed the right mitigation strategy needs to be selected.

To help the decision making process, this research will present a framework which gives an overview of the cost factors that come into play. For some factors influencing the decision, it will be easy to calculate the exact costs. For some others, the time and resources it takes to even come to an imprecise estimate make it unfeasible for the quantitative approach. As the risk management approach to security seems to be the best way of informing executive managers about the risks and the effectiveness of a security measure, this will form the basis of the approach taken in this research.

There has been some attention to the topic of the economics of IT security, but the amount of papers, articles and books available on this topic are limited. Economic approaches to the problem have been tried, some coining the term 'Return on Security Investment', but they have not yet received widespread use. This is partially because most of the models focus on one implementation at a time. The consensus in the field at the moment seems to be that even though an economic approach can lead to better decision making, calculating the exact costs is almost impossible to do (Anderson, 2001 and Gordon & Loeb, 2006b). This all leads to the following question which we will aim to answer in this research:

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

The research question makes clear that some aspects are quantifiable, implying that others aren't, and shows the goal of creating a framework taking all costs into account. In order to create a complete framework, the qualitative aspects will also have to be added to the framework. The focus will be on the quantitative aspects.

RISK MANAGEMENT

Small organizations often will have an ad-hoc approach to IT Security, with the related tasks often being performed by the system administrator. As organizations grow larger a different approach is needed. Organizations use security standards and best practices. Even though this approach gives a good overview of what is needed in the security strategy, to best results are achieved if the strategy completely fits the organization. The approach should fit the unique aspects of the company. This is why in large organizations security is often tackled with the risk management approach (Bojanc & Jerman-Blažic, 2008). Decision makers need information to base their decisions on. They know there are many threats to the business they are responsible for. To successfully handle the risks that apply to their business, decisions are based on an assessment of the risks.

Risk management enables organizations to identify, assess and manage risks (Jones, 2007). It is a way of dealing with uncertainty by assessing the risks and prioritizing them 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 on IT systems, others are broader. Especially aimed at Information Security are OCTAVE by Carnegie Mellon University and ISO 27005. The "Operationally Critical Threat, Asset, and Vulnerability Evaluation" (OCTAVE) standard tries to balance the organizational viewpoint (operational risk) with technology and security requirements. ISO 27005 is the information security risk management standard by the International Organization for Standardization and gives organizations guidelines to improve information security by using a risk management approach.

Even though these standards sometimes presents guidelines and best practices, the main advantage of risk management is that it identifies the unique risks that the organization faces. 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.

In all standards, the following basic steps can be found: Risk Assessment, Risk Mitigation, and Evaluation.

RISK ASSESSMENT

The first step in the risk management approach is to identify and analyze the risks the organization faces. How this is done exactly differs per framework and often also per type of risk. Quantitative risk analysis attempts to calculate the severity of the risk as a function of the potential damage and the rate of occurrence of the risk (Cavusoglu et al., 2004). Qualitative approaches are also common. Usually risks are classified into a limited number of classes such as 'low', 'medium' and 'high'. This allows for much quicker analysis than when a quantitative approach is used (Blakley et al., 2002). Sun et al. (2006) describe some of the methods used in qualitative risk assessments, naming methods such as scenario

analysis, questionnaires, and fuzzy metrics. Once the risks have been identified, organizations need to prioritize those risks which need attention first. This prioritization serves as input for the next phase.

RISK MITIGATION

Starting with the highest prioritized risks, in the risk mitigation phase organizations will decide what the right measure is to deal with this risk. Risk Mitigation can be achieved through any of the following options:

- Risk Acceptance: Accept the potential risk and if possible implement controls to lower the impact if the risk materializes.
- Risk Avoidance: Avoid the risk by eliminating the risk cause and/or consequence. This can mean letting an investment opportunity pass.
- Risk Reduction: Limit the risk by implementing controls that reduce the risk.
- Risk Transference: Transfer the risk by using other options to compensate for the loss, such as purchasing insurance. In such a case, the organization transfers the liability to another party.

In the risk mitigation phase, the different options are compared. If an organization is evaluating possible control measures, it will need to perform a Cost-Benefit Analysis to see if the control measure is worth taking. The benefits will be the reduction of the risk. This is where the framework can be used. Also, the Cost Benefit Analysis can be used to compare several options to control the risk.

EVALUATION

After the risk mitigation stage, it needs to be evaluated whether the choices made in the risk management process were correct. Based on the evaluation the risk assessment step starts again. It is important to recognize that risk management is a continuous process. As the environment around the organization changes and the organization adapts, new risks might emerge and the impact of existing risks will change (Blakley et al, 2002).

The use of the framework presented in this research is limited to the risk mitigation phase and within the mitigation phase can be used to identify the cost factors for controls that would reduce the risk. Nonetheless, Purser (2004) 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." (Purser, 2004)

METHODS

Part of the risk management process is an analysis of the several options for risk mitigation. Most of the standards use Cost-Benefit Analysis (CBA) for this aspect. Based on the risks defined in the risk assessment the company can calculate the costs of each of the options and select the most appropriate one. As its name implies, CBA compares the costs with the benefits. With security related issues, the benefit is often the reduction in expected losses. CBA can be qualitative or quantitative (NIST, 2001).

Mercuri (2003) 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 Internal Rate of Return (IRR) and Net Present Value (NPV), discussed later on in this section. 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) (Mercuri, 2003). 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. In reality, the cost of that risk will never be $2.5 million in one year exactly. It is either zero or $10 million (Blakley et al., 2002).

An important drawback of this and other quantification methods is that the data used as input 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.

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. Kabay (2008) describes that we could know these numbers if we have a statistical knowledge base of computer crime. But he also explains that there are major difficulties in making an accurate knowledge base. 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 can only 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 they will cost money and companies will only invest in areas that bring them the benefits which have a certain worth. So it might be useful to look at methods used for other investment decision.

In corporate finance, the most used method for decision making on investments is Net Present Value (NPV). Brealey, Myers and Marcus (2007) describe it as the “gold standard” of investment criteria. NPV deducts the investment costs from the present value of cash flows coming from the investment project. If the NPV is positive the project has more benefits than it costs and organizations should go ahead with the project. For a project with the goal of reducing risk by implementing controls that improve security, the present value of cash flows will not be a positive one. As stated earlier the benefits are taken to be the prevented losses. By taking the present value (adjusted for the time value of money) of those cash flows companies have a more realistic comparison. One has to wonder though with the toughness of estimating the impact of a potential loss, and without knowing when such costs will be incurred whether an NPV analysis does go into too much detail.

Still, in a study by Gordon and Loeb (2006a), about 25% of the interviewed firms stated that they did ‘usually’ use NPV analysis in the decision making process for information security projects and found

that there is a movement to a higher use of economic analysis, whilst also realizing that companies take more things into consideration when making such decisions:

"Of course, the fact that a firm uses NPV analysis for some information security expenditures decisions does not mean that the firm uses it for all such decisions. Furthermore, even where NPV is used, it does not follow that final decisions are based solely on NPV analysis." (Gordon and Loeb, 2006a)

Some security projects are not done 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 organizations to show due care in the protection of sensitive data and some laws define rules for the level of security. Gordon and Loeb (2006b) call these projects must-do projects, regardless of the results of the NPV. A CBA can still be interesting to compare mutually exclusive projects that both help the organization to be compliant with the law. And even for a must-do project, the organization performing such a project can only reserve the money for it if it knows how much it costs.

There are several economic methods that can help organizations in IT security decision making, but most of them rely on organizations to quantify the costs and benefits of a security measure. Several researchers have tried to find the underlying principles that make this a difficult task. An overview of previous research is presented in the next section.

ECONOMICS OF INFORMATION SECURITY

Decision making in Information Security is hard. The first researcher who tried to define the reasons for this was Ross Anderson. Anderson (2001) argues that the incentives for individuals often are wrong. 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 as 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 (Akerlof, 1970 in Anderson, 2001) 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 bad products. The same applies to some security markets as buyers cannot see from out the box of a product how much security it really gives them.

Gordon and Loeb (2002) 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 sets.

A second finding of the Gordon and Loeb model is that companies should invest at most 37% of the expected loss due to a security breach. However, Hausken (2006) shows that the assumptions made by Gordon and Loeb exclude some classes of security investments. He concludes that in those cases the investment is not capped at 37% and thus can be higher. It is interesting to note that Gordon and Loeb (2006a) applauded Hausken's findings. This shows that the field is developing and improving the body of knowledge on the economics of information security.

Both Schechter (2004a) and Cremonini & Nizovtsev (2006) make the important observation in that security is not just about how secure systems really are but what also matters is perception. In earlier work, Schechter defined a metric called cost-to-break. For an attacker it is worthwhile to spend his resources up to the point that it equals the amount that he can gain. However, what the attacker thinks he needs to spend is based on his belief of the likelihood that he can find a vulnerability, and what he can gain is mainly based on the market price for a vulnerability. Both may be distorted by false perceptions. Schechter suggests that these values and its implications for (software) security are best studied by regression models.

Research on the economics of security has led to several proposals for a Return on Security Investment-model. Two examples of those were created by Sonnenreich et al. (2006) and Purser (2004). 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. Already discussed are 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.

Sonnenreich et al. (2006) adjust the ROI model by defining the expected returns as the ALE 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 a hacker breaking through the firewall. The statistical methods normally used in such cases have limited use in information security (Kabay, 2008).

Purser (2004) attempted to adjust the ROI formula in such a way that it could be used for both normal investments as well as security investments by incorporating the value of change in risk. This value can be calculated using methods such as ALE and CBA. He leaves it to the user to which method is used. He understands the problem of inaccurate data, but his argument for using his Total Return on Investment-model (TROI) can be summarized as: the value is in the process. For Purser, the decision making process in security should aim at reaching the desired risk profile by looking at the results of security measures and developing the security culture. TROI can be used to support this decision making process, both by giving a reasonable answer to the ROI question for security investments and by fostering the discussion and analysis of security measures. However, if an organization already has the right mechanisms in place to foster discussion and analyze the options in the decision making process, then the TROI model does not provide any added value.

Therefore, no Return on Security Investment model should be used solely to decide on security investments. The body of research on the economics of security, partly described at the beginning of this section, 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 and quantification methods can help in that regard (Bojanc & Jerman-Blažic, 2008). In order to support organizations in the analysis of the costs the remainder of this research studies the cost factors in IT security measures.

KEY SECURITY AREAS

Because of the large size of the field of information security, several areas were identified that could serve as a base to study the field. In choosing those areas care was taken to include proactive and reactive security measures and to ensure that the areas attract a high interest from both the business and scientific community.

The following areas were identified: Identity Management, Network Access Control, Intrusion Detection Systems, Business Continuity Management, and Data Loss Prevention.

IDENTITY MANAGEMENT

IdM mainly focuses on authentication. In many systems, access should be limited to a group of users and/or there is a need to know who performed a certain action. Identity Management provides companies with the means to do both things. Satchell et al. (2008) describe some of the basic concepts involved. Koch & Möslein (2005) give an overview of how it is supported by technology and how it improves security. Petterson (2006) describes some metrics which can be used to measure the effectiveness of an IdM implementation.

NETWORK ACCESS CONTROL

NAC aims to prevent security problems by performing a check on each device that tries to connect to the network. The more advanced versions retrieve information on the definition file of the antivirus and firewall software, checks if the latest updates for the operating system are installed and grant admission only if everything is up-to-date (Panjwani & Tan, 2006). Users also need to authenticate before being allowed on the network (Suzuki et al, 2007).

INTRUSION DETECTION SYSTEMS

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, detect and respond to unauthorized activity. As such, it is a reactive approach to computer security (Peddabachigari et al., 2007). IDS attracts a high interest from the scientific community. Abraham et al. (2007) describes some of the techniques that are used in the development. Wei et al. (2001) propose an IDS with a built-in Cost Benefit-Analysis.

BUSINESS CONTINUITY MANAGEMENT

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 with which the company is back in business. Usually, the IT part of BCM is often referred to as Disaster Recovery Planning (DRP). However, business continuity is not only dependent on IT related problems, nor can BCM be seen without IT being a part of it. Therefore, in this research BCM is studied whilst still focusing on the IT costs that come with it. Two papers that have the same approach to this subject are Cerullo & Cerullo (2004), who provide an overview of the planning process, and Lam (2002), who presents an eight step model for BCM.

DATA LOSS PREVENTION

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. Companies can resort to measures such as encryption and backups and can create and enforce policies that help prevent data losses. DLP has not received much scientific attention, but the technologies and policies that are part of DLP solutions have. For an overview of technologies, see the taxonomy by Venter & Eloff (2003).

Each area was studied by interviewing one or more experts and studying literature in the area. This lead to the creation of a framework listing all cost factors in those areas, as well as whether those costs can be quantified or not. The frameworks served as a basis to create an overall framework which will be presented later on in this research.

With the choice of these areas, some of the main aspects in IT security were combined. It is a good mix between proactive and reactive measures (Venter & Eloff, 2003). 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. As Cerullo & Cerullo (2004) state, 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, 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 (Hale & Brusil, 2007).

It should be noted that the selected five areas are not meant to be completely exhaustive for the research domain. 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, the vendor of the application or system needs to update the product and many people benefit from it (Camp, 2006). A study on Vulnerability Management would need to focus on these incentives. There are also more ‘simple’ areas such as anti-

virus and firewalls for which the use has become a de facto standard (and in a way they are included as NAC products often enforce the use). Some of the areas that were chosen 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.

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 (2001) adds accountability and assurance to these three and defines the five objectives as:

- Confidentiality: Private or confidential data should not be disclosed to unauthorized individuals.
- Integrity: Consists of two facets. Data integrity, which means that data is not altered in an unauthorized manner, and system integrity, which means that a system works as it should, i.e. it does not give manipulated responses.
- Availability: Ensures that the systems work and can be used by authorized users.
- Accountability: This is the requirement that actions of an individual can be traced to that individual. It is of importance as for many security measures, compliance is an important driver to implement that measure.
- Assurance: Assure that the other four objectives are met in an adequate way and that security measures are correctly implemented. Not so much linked to individual security measures but more a requirement that any security measure is implemented with due care.

In table 1 it is shown how the security areas relate to these objectives. Assurance has not been added to the table, because it cannot directly be linked to the security measures. It should be seen as a control for the implementation of each security measure, instead of something onto which security measures can be mapped.

Apart from the objectives in table 1, assurance is also an important driver for organizations. It has much to do with compliance. Organizations are required to show due care and due diligence. If they fail to do so, they can be held liable whenever an incident happens resulting in high claims. Most regulations do not state the exact requirements and leave the details to the organizations themselves. Organizations can show they are compliant by meeting the assurance objective through implementing security measures in an adequate way and being able to prove the organization did do what was realistically possible to prevent incidents. The exact laws organizations fall under depend on the type of organization and the location they are active. For example, organizations trading on a stock exchange in the United States have to comply with the Sarbanes-Oxley regulations.

After studying the five areas the authors were able to create 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.

Tabel 1. Security areas fit with objectives

OBJECTIVE	COVERED BY	HOW:
Confidentiality	**IdM**	Prevents unauthorized users from accessing resources.
	NAC	Prevents unauthorized users and unsafe hosts from accessing the network.
	DLP	Stops confidential data from leaving the organization.
Integrity	**IdM**	Prevents unauthorized users from accessing resources.
	IDS	Is aimed at keeping the integrity of data intact.
Availability	**IdM**	Prevents unauthorized users from accessing resources.
	IDS	Monitors and identifies threats.
	BCM	Reduces downtime if availability is threatened.
	NAC	Prevents unauthorized users and unsafe hosts from accessing the network.
Accountability	**IdM**	All these areas have the option to identify the actions of individual users.
	NAC	
	IDS	
	DLP	

Ideally a single framework would be available that can help us define the costs of a security measure, regardless of the area. This may be done by integrating the five frameworks into one overall framework. This should be done carefully. The five 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 (Sutherland, 1975). 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 with security measures. The cost factors identified for each area 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 (Vermeule, 2007; Zhang et al., 2006) 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. The other steps are also based around this supermajoritarian constraint. A supermajoritarian approach was chosen over a simple majority (at least 50%) as the framework is created to list cost factors that should be looked into when studying the costs coming with a security measure. Therefore a high level of consensus is required on the cost factors that were added. This resulted in that for some of the cost factors it was quite straightforward to add them the overall framework, as they were present in (almost) all of the five areas. 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:

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

In the first step, identifying the similar cost factors, the naming was checked. Some of the areas might use different terminology for the same thing. However, with the exception of the implementation factor (9) which each had the name of the different areas, no factors were taken together in this first step. In the second step, all of the factors in the different frameworks were then counted. Those that were named in at least 80% of the frameworks were deemed important enough to add to the overall framework directly. The terms that were added this way were licensing (1), implementation (9) and support costs (14). This does not mean that all security measures necessarily involve licensing costs, but the majority of them they do so this is a cost factor that should be considered. As depicted in table 2, in the five areas studied for this research, only Business Continuity Management did not had licensing costs listed as a cost factor.

Not all cost factors were found in at least four of five areas. Those factors were identified as a cost factor in the area they were identified in, but do not occur in every area. So the next step was to determine what to do with those factors and preferably see if they somehow can fit within the 80% requirement.

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 the framework under one common term. One item that was added this way were policies (2) and plan (3) creation. 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 the same name. Similarly, the cost factors administration (15), adjustment of plans (16), maintenance (17) and vendor lock-in (18) were taken together. The administration is done to keep the system up-to-date and

properly configured. In BCM, the plan adjustments are done for the same reason. Maintenance is part of administering the installed systems and vendor lock-in can lead to higher administration costs in the future.

Tabel 2. Grouping of cost factors

#	***Cost factor***	*Sub factors*	*IdM*	*NAC*	*IDS*	*BCM*	*DLP*
ONE-OFF							
1	**License**	License	X	X	X		X
2	**Policies**	Policies	X	X			X
3		Plans				X	
4	**Hardware**	Hardware procurement		X	X		X
5		Hardware implementation		X	X		X
6		Hardware				X	
7		Adjust systems	X				
8		Infrastructure changes				X	
9	**Implementation**	(IdM, NAC, IDS, DLP) Implementation	X	X	X		X
10		Configuration			X		
11		Test plans				X	
12	**Embedding**	Organizational changes				X	
13		Staff			X		
RECURRING							
14	**Support**	Support	X	X	X		X
15	**Administration**	Administration	X	X			X
16		Adjust plans				X	

17		Maintenance			X		
18		Vendor lock-in		X			
19	**Monitoring**	Monitoring			X		
20	**Auditing**	Auditing	X	X			X
21		Testing			X	X	

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 (4) and hardware implementation (5). These two cost factors are related to each other but convey very different costs. For some areas, hardware is not as important as in others and as a result only the cost factor hardware (7) 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. In table 8, also infrastructure changes (8) has been listed as part of hardware. This is partially true. Some of the changes made have to do with the IT infrastructure, others might have to do with changes to the infrastructure and would fall under implementation. Apart from hardware, also auditing (20) and testing (21) were grouped together, as both are done to assure the correct working of the security measure. In the first version of the overall framework, monitoring (19) was also added in this cost factor, but after the validation interviews it was decided to separate it from auditing. It was also established that in the areas in which monitoring was not named as a cost factor, the processes involved within monitoring were seen as part of either the administration or the auditing costs. That explains why it only comes up once in the five areas, but still has its own costs as to warrant a separate cost factor.

For the implementation cost factor, configuration (10), test plans (11), organizational changes (12) and staff (13) were added. During the interviews it was identified that the implementation traject could be split up in the implementation of the security measure itself and the embedding of the measure into the organization. As all items could be grouped in one of the cost factors, there were no factors left so the option to leave them out did not need to be considered. It could have been that there were items only have small effect on a single or a few area(s) so that the impact on security measures overall is negligible. The supermajority rule proved useful in integration of the five frameworks. As the integration went successful the framework can be presented in this research. The framework lists all 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. 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.

The framework can also be used to compare different solutions of a product. For example, In Identity Management there are solutions that integrate all systems by creating a layer around it, and others that 'merely' have a central application that aggregates the different credentials for users. Even though the user experience is the same, the technical requirements are quite different and as such the costs that have to be attached to some of the cost factors. By analyzing these costs, organizations can look for the solution with the lowest financial impact.

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 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. As this research is aimed at the quantitative cost factors it will not be explained in detail how to tackle these cost factors. However, they do have their part in the total cost of the solution and decision makers will need to consider them when deciding between different options.

CITS: THE COST OF IT SECURITY FRAMEWORK

After combining the cost factors from the five areas now the "Cost of IT Security Framework" can be presented. In the framework all the cost factors for measures taken within IT security are listed along with the ways these costs can be quantified, if possible. The framework can be found in table 3. It consists of nine cost factors. The first five cost factors come with the implementation of a security measure, the final four are recurring and will result in costs that can be measured on a yearly basis. It should be kept in mind that the quantification is done at the time of doing a Cost-Benefit Analysis during the Risk Mitigation phase.

ONE-OFF COSTS

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. This should give the organization a good understanding of the requirements for the product and serve as input for making the choice. 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. Therefore 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.

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 1 – The Cost of IT Security (CITS) Framework  **= Quantitative approach**  **= Qualitative approach**

All security measures involve making decisions. Organizations have to define the rules that form the basis of these decisions and use them to create **policies** and plans. These policies define the reaction when a security incident happens and what users are allowed to do. An example of such rules that make up these policies is which employees should have access to what resources. Bad policies are a threat to security; a receptionist that can access the financial systems of the organization could change her own salary. Good policies are written by people that have good insights in the organization and have expertise in writing relevant policies. It is unlikely that employees in the organization have both. In most cases, a team needs to be formed that consists of people that are knowledgeable about the organization they work in and by 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 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 the **hardware**. Even though security threats are not solved by throwing more IT at the problem (Mercuri, 2002), it often is required to install more hardware or adapt the current IT infrastructure.The costs coming with hardware consists of those made in multiple steps. It needs to be identified what the requirements are and the hardware needs to be procured. 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 steps quantifying costs might be possible, but overall it is too hard to know beforehand what the exact requirements will be.

One of the one-off cost factors that is underestimated the most is the **implementation** process of the security measure. In order for the measure to be effective, organizations need to implement the measure, hire (if needed) people for the administration, train employees 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 is a result of the findings in the first steps and this phase 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 described in the recurring costs, employees will be needed to perform the administration and monitoring. These employees might be available within the organization. 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 needs to learn to work with the changes that come with the new security measure (by training or by being notified) and the basic training for the new employees will need to updated. Training costs can be calculated once the organization knows how many people need to receive the training and how much the training costs. Embedding is closely related to the implementation and is an important factor in making sure that the implementation has the desired effects on the organization.

RECURRING COSTS

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. In most licensing schemes a yearly rate has to be paid. If that is the case 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, which 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.

The third recurring cost factor is **monitoring**. Most systems will produce logs stating events and incidents that happened. These need to be checked and acted upon if incidents are spotted. An example of this is when an Intrusion Detection System detects an anomaly in network traffic and reports an incident. The employees tasked with monitoring the network will be notified and if they can confirm the security breach they will act upon it. Monitoring is a continuous process with the main purpose to identify incidents and start the appropriate follow-up course of events. Organizations might be able to calculate the costs for the employees if they know the time required, but the costs for the follow-up actions cannot be known before hand.

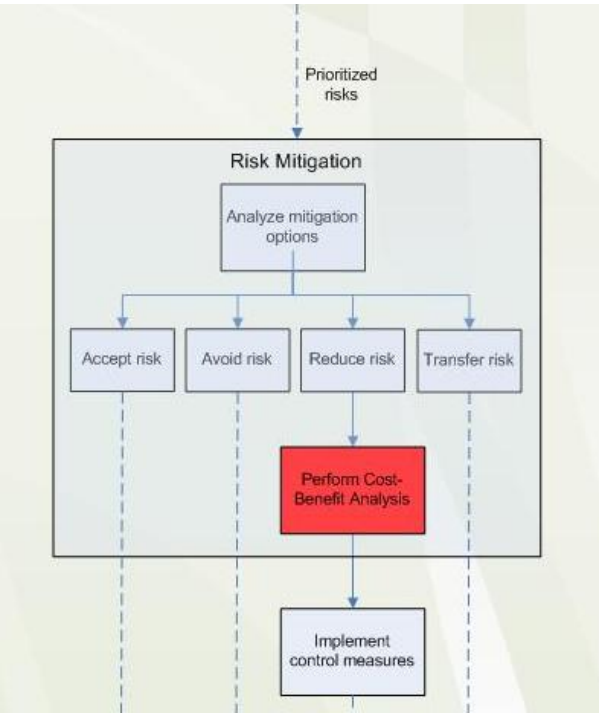
Finally, auditing is named as a cost factor. **Auditing** is an evaluation of the implementation, performed to assure the correct working of the security measure. Auditing is usually done at an interval and is performed as a check on the right implementation and working of the security measure. It can also include test procedures. An example of something that can be found during an audit is that a group of employees have more access than they should have based on their function. This can indicate a loophole in the system or in the policies and that should be adjusted. Audits can be performed by an internal or external auditor.

Relevance

Before looking at how the Cost of IT Security framework can be used, we should look back at the risk management approach. The risk management approach contained three major phases; the risk assessment, the risk mitigation and the evaluation. The risk mitigation phase is modeled in more detail in Figure 1.

The input is the prioritized risks. Those with the largest impact on the organization should be handled first. During the risk mitigation phase, the different options are investigated and the most suitable option is chosen. Among the options is the implementation of control measures. For these measures, a Cost-Benefit Analysis can be made. The framework presented here can help identifying the costs to be considered for the CBA.

Figure 1. Risk Mitigation



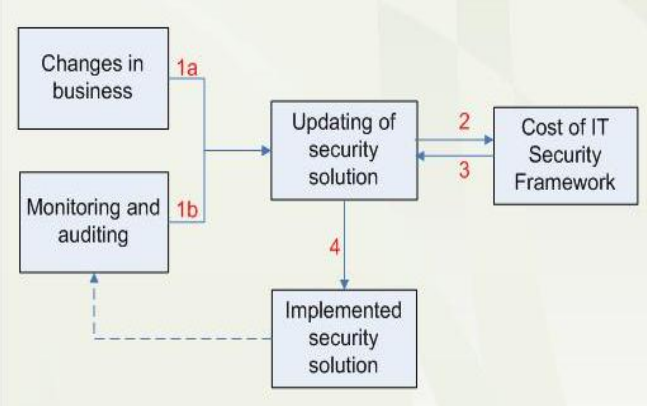
The framework can help any organization in their analysis of the costs in two ways: first of all, the cost factors have been identified, listed and validated. Organizations should look at these cost factors when deciding on an IT security control measure. Secondly, for each cost factor it was stated whether it is possible to use quantification methods.

The goal of the Cost-Benefit Analysis 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 (Jones, 2007). It is clear that in most cases the costs and benefits cannot be fully quantified. Still, whether a measure will bring the right benefits can be studied. Given the risk management approach, it should already have been identified what risks need to be mitigated and what the impacts are of those risks. The security measure tries to reduce the risk. Usually the risks cannot be completely mitigated, but are reduced in either the probability of occurrence or the losses incurred with such risks (Blakley et al., 2002). An analysis on whether the measure really reduces the intended risks and does not add new risks to the organization should be part of the CBA. So an analysis of the costs and benefits can still lead to improved decision-making in IT security, even when it is not feasible to perform a complete quantitative assessment. The framework presented in this research helps organizations to identify the cost factors and quantify those where it is feasible.

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. Figure 2 shows this process. This might be needed due to changes in the business (1a) and as a result of problems found in monitoring and auditing (1b). For easy-to-solve problems not much time needs to be spend in considering whether it is a good idea to make the required changes. But sometimes the required changes will be much larger, involving higher costs and making

it a project on its own. Before starting such a project, organizations can start an analysis to see whether the updates are really worth implementing.

Figure 2. COS framework in updating process



This analysis can use the Cost of IT Security Framework (2). 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 (3), which after the implementation will have influence on the running of the security solution (4).

For some security measures and with the second use as described above, an important part of the analysis is a comparison of the recurring costs. If these are lower after the implementation, then organizations know they will have an advantage in implementing the solution (of course they should still consider the investment costs, but in the long-term there is only money to be gained). However, these are selected cases and in most situations, the benefits of implementing a security measure cannot be found here. This is why a risk management approach is so important, as only that can give organizations a true insight in the risks that are mitigated. The framework could be used outside of a risk management approach, but then organizations will have a hard time defining the benefits.

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 investigated whether the cost factors were rightly represented in the overall framework. No changes were made after this process. For the next phase an approach very similar to the Delphi method (Linstone & Turoff, 1975) was taken. The Delphi method is a technique to acquire knowledge from a large group of experts without the disadvantages of group communication (Roth & Wood II, 1990). This involves a second round of expert interviews which are conducted in order to verify the findings. The experts are interviewed up until a consensus is reached. The authors had a different scope and goal for this second round of interviews. For the first round of interviews, performed to create the framework, the experts

were chosen based on their experience in that specific domain. The experts invited in the second round were selected for their overall experience in Information Security. Some of the experts had an academic background, whereas others were interviewed because of their business expertise. The goal of the validation interviews was to verify the identified cost factors as well as the research method and the approach taken to the Cost-Benefit Analysis.

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 added 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. For all other cost factors, the experts agreed on those factors being included in the framework. They also found that the nine cost factors in the overall framework included all costs that come with a security measure.

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.

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 Cost-Benefit Analysis. In considering an implementation, five of the nine cost factors cannot be quantified. This 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 qualitative methods it still is possible to give an indication of the total cost. For example, if the current network infrastructure is known to be very complex, then we also know that making large changes to the network will lead to high costs. These costs cannot be known exactly, as the time required to make these changes is very hard to estimate. But these costs will be higher when compared to a simple network infrastructure. Together with the quantitative costs, this can then be taken into account in the analysis (Pras et al., 2004). 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.

In order to put a correct value in an analysis of 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. The problem with this is the same as with the cost factors; it is very hard to calculate the ALE for all measures correctly (Schechter, 2004b; Kabay, 2008). This suggests that in analysis of the benefits a qualitative approach will be better. This should also fit with the approach and goals of the risk assessment. If an organization groups risks based on their impact in high, medium and low in such assessment and their goal is to reduce all risks that are classified as high to at least medium, then they can focus on controls that reduce risks with a high impact.

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. Organizations trying to use quantification methods should realize 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 (Purser, 2004).

The use of quantification methods should also depend on the type of risks. If compliance is the main driver for an IT Security measure, it will often be a must-do project. A CBA can be done to quickly analyze the involved costs or to compare projects. But the decision to go ahead with the project is not depending on the outcome, and as such it does not require the same attention as when it does. For a project which is easy to implement, the time required to do a detailed CBA might take longer than the project itself. Organizations should adjust the requirements for the CBA to the type of risk and security measure.

A question that organizations might find interesting is that if it is not possible to define the exact costs coming with a cost factor before the measure, when will they be able to quantify the costs of a security measure? The first qualitative cost factor in the framework is hardware. The main reason for not being able to quantify the cost at the time of doing a CBA is that the hardware costs are dependent of what adjustments and new hardware is needed. For this the current infrastructure must be compared to the requirements posed by the security measure. The exact requirements are not always known until the first phase of the implementation is completed. At the point of doing the CBA, organizations will not have defined the exact requirements in a high level of detail. In most cases, the full costs for procuring and installing hardware will only be known in hindsight.

For the implementation cost factor, the main reason that makes it unfeasible to quantify the costs for that beforehand is that the length and implications of the full implementation process depends on the outcome of the first phase, as well as the changes that need to be made because of the hardware cost factor and the final version on policies. Once all of this is known, organizations can use the experience of the vendor or consultants to estimate the total length of the implementation and the costs coming with that.

Three of the qualitative cost factors are recurring costs. Sometimes these will vary on a yearly basis, depending on how the business evolves and other changes that have to be made. In those cases organizations will only be able to say what the costs are on average when they can draw from experience. But if these costs are more or less constant, then organizations might be able to do this earlier. For administration and monitoring the organization can use the expertise of the vendor or consultants to make realistic estimates of the time and number of employees required to perform such tasks. Based on this, the costs for most activities can be calculated. As for administration some of the costs are with updating the solution, this depends on how often changes are required. This cannot always be known beforehand and in such a case, organizations can only know the exact costs when they have build up a few years of experience.

The analysis of the costs could be helped if it is known how much the cost factors that can be quantified contribute to the total costs of the security measure. This is similar to the metrics that Sonnenreich (2006) suggests to use for his ROSI-model. These have limited use in Information Security. For the overall framework it is not possible to add a certain percentage to the cost factors. In an area for which new hardware needs to be procured the costs for that factor will be much higher compared to the other costs than those areas which do not require many changes to the hardware infrastructure. This might be possible if the scope is limited to one area of Information Security, but even then it can be quite difficult. There are not many metrics available that give a good overview of the costs (Petterson, 2006). Future research could try to define those, but it will be hindered by many of the problems identified by Kabay (2008) on building up a statistical knowledge base for computer crime.

CONCLUSIONS

This research presents the Cost of IT Security Framework to be used by organizations during a Cost Benefit Analysis of an IT security measure. The CITS framework focuses on the cost factors. For each of the cost factors it was determined whether they could be quantified or a qualitative approach would be required. Furthermore, the CITS framework describes what costs are involved for each cost factor.

The Cost of IT Security Framework was created by studying five security areas. For each of them, literature in those areas was studied and domain experts were interviewed. This has led to a framework listing all cost factors for that area. These frameworks had enough cost factors in common to serve as the basis for creating the overall framework. This justified the statement that the cost factors listed in the Cost of IT Security framework have to be taken into account when analyzing a security measure. This overall framework has been validated by further interviews. As only the overall framework went through this validation process, it is recommended to use this even when analyzing a security measure which falls in one of the five areas.

The main research question which the authors 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. Nine cost factors were identified. The framework shows that five out of nine cost factors identified

cannot be quantified upfront. These are the costs, for hardware, implementation, administration, monitoring and auditing. The reasons for this vary. The cost factors hardware and implementation involve a time consuming process consisting of multiple phases, where the exact costs to be made depend on the outcome of the previous steps. Some of the recurring costs, administration, monitoring and auditing, are cost factors for which the costs can vary per year and often are dependent on modifications that have to be made to the system as required by business changes.

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. 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. Using this in the decision making process will lead to a more realistic view of the implementation of the security measure. There are several methods available that can be used for quantification, such as Annual Loss Expectancy and Net Present Value. For the full process, an attempt at a Return on Security Investment can be undertaken. Still, care must be taken not to overstate the importance of quantification methods. In doing a Cost-Benefit Analysis, what is the purpose of calculating the exact costs when the monetary value of the benefits is not known? Organizations should have a weighted approach, using risk management to prioritize those aspects with the biggest impact and adjusting the analysis based on the type of project.

This research also identified the preferred way of decision making in IT security. The main use of the 'Cost of IT Security 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 the security measure really reduces the intended risk (the benefit of the measure) and whether the cost to do this is acceptable. In analyzing the costs, the framework presented here can be used. If organizations have more options and those are mutually exclusive, then 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.

Another important advantage of risk management is that it has an evaluation phase. This evaluation will lead to a new risk assessment, based on the situation as it is at that moment. This is important, as how secure the organization is depends on the total picture instead of single security measures. By continuously evaluating the situation gaps in the current security infrastructure of organizations can be identified earlier.

Decision making in security should not be just based on a quantitative analysis of the costs and benefits. It is too hard and too time consuming to perform this task, and no guarantees can be made about the right outcome. But this also 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 for that can be improved by quantification methods, as long as the limitations are kept in mind and the bigger picture is not forgotten.

REFERENCES

Abraham, A., Grosan, C. & Martin-Vide, C. (2007). Evolutionary Design of Intrusion Detection Programs. *International Journal of Network Security.* Vol. 4 (3), pp. 328-339.

Anderson, R. (2001). Why Information Security is Hard - An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference*, p.358.

BBC News (2008). *US cracks 'biggest ID fraud case'***.** Retrieved November 15th, 2008 from http://news.bbc.co.uk/2/hi/business/7544083.stm

Blakley B, McDermott E. & Geer D. (2002). *Information Security is Information Risk Management.* ACM New Security Paradigms Workshop.

Bojanc, R. & Jerman-Blažič, B. (2008). Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces* . Vol. 30 (4), pp. 216–222.

Camp, L. J. (2006). The State of Economics of Information Security. *A Journal of Law and Policy for the Information Society.* Vol. 2 (2), pp. 189-205.

Cavusoglu, H., Mishra, B. & Raghunathan, S (2004). A Model for Evaluating IT Security Investments. *Communications of the ACM*, Vol. 47 (7), pp. 87–92.

Cerullo, V. & Cerullo, M.J. (2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management.* Vol. 21 (3), pp. 70-78.

Cremonini, M. & Nizovtsev, M. (2006). Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies. *The Fifth Workshop on the Economics of Information Security*. University of Cambrige, England.

Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D.R. & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security.* Vol 4 (3), pp. 224-274.

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

Gordon, L.A. & Loeb, M.P. (2006a). Budgeting Process for Information Security Expenditures. *Communications of the ACM.* Vol 49 (1), pp. 121-125.

Gordon, L.A. & Loeb, M.P. (2006b). *Managing Cybersecurity Resources: A Cost-Benefit Analysis*. McGraw-Hill, New York.

Kabay, M.E. (2008). *Understanding Studies and Surveys of Computer Crime*. Retrieved September 26th, 2008 from http://www2.norwich.edu/mkabay/methodology/crime_stats_methods.pdf.

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers.* Vol. 8 (5), pp. 338-349.

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

Jones, A. (2007). A Framework for the Management of Information Security Risks. *BT Technology Journal.* Vol. 25 (1), pp. 30-36.

Lam, W. (2002). Ensuring Business Continuity. *IT Professional*. Vol 4 (3), pp. 19-25.

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

Koch, M. & Möslein, K. M. (2005). Identities Management for E-Commerce and Collaboration Applications. *International Journal of Electronic Commerce.* Vol. 9 (3), pp. 11-29.

Mercuri, R.T. (2002). Computer Security: Quality Rather than Quantity. *Communications of the ACM.* Vol. 45 (10) pp. 11-14.

Mercuri, R.T. (2003). Analyzing Security Costs. *Communications of the ACM.* Vol. 46 (6), pp. 15-18.

National Institute of Standards and Technology (NIST) (2001). *Underlying Technical Models for Information Technology Security*. Retrieved september 26th, 2008 from http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf.

Panjwani, S. & Tan, S. (2006). Assessing Trusted Network Access Control Cost-Benefit Factors. *Proceedings of the Workshop on the Economics of Securing the Information Infrastructure*.

Peddabachigari, S., Abraham, A., Grosan, C. & Thomas, J. (2007). Modeling Intrusion Detection System Using Hybrid Intelligent Systems. *Journal of Network and Computer Applications.* Vol 30 (2007), pp. 114-132.

Petterson, G. (2006). Introduction to Identity Management Risk Metrics. *IEEE Security and Privacy*. Vol 4 (4), pp. 88-91.

Purser, S.A. (2004). Improving the ROI of the Security Management Process. *Computers & Security* 23 (7), pp. 542-546.

Roth, R.M. & Wood II, W.C. (1990). A Delphi approach to acquiring knowledge from single and multiple experts. *Proceedings of the 1990 ACM SIGBDP conference on Trends and directions in expert systems*. Pp. 301-324.

Satchell, C., Shanks, G., Howard, S., & Murphy, J. (2008). Identity crisis: User perspectives on multiplicity and control in federated identity management. *Behaviour & Information Technology*.

Schechter, S. (2004a). Toward econometric models of the security risk from remote attacks. *Third Workshop on the Economics of Information Securit.y.* Minneapolis, MN.

Schechter , S. (2004b). *Computer Security Strength & Risk: A Quantitative Approach.* Harvard University.

Sonnenreich, W., Albanese, J. & Stout, B. (2006). Return On Security Investment (ROSI) – A Practical Quantitative Model. *Journal of Research and Practice in Information Technology*. Vol. 38 (1), pp. 45-51.

Sun, L., Srivastatav, R.P. & Mock, T.J. (2006). 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.

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

Suzuki, S., Shinjo, Y., Hirotsy, T., Itano, K. & Kato, K. (2007). Capability-based Egress Network Access Control by using DNS server. *Journal of Network and Computer Applications,* Vol. 30 (4), pp. 1275-1282.

Venter, H. S. & Eloff, J. H. P (2003). A Taxonomy for Information Security Technologies. *Computers & Security.* Vol. 22 (4), pp. 299-307.

Vermeule, A. (2007). Absolute Majority Rules. *British Journal of Political Science.* Vol. 37 (4), pp. 643-658.

Wei, H, Frinke, D., Carter, O. & Ritter, C. (2001). Cost-Benefit Analysis for Network Intrusion Detection Systems. *Proceedings of the CSI 28th Annual Computer Security Conference.*

Zhang, J., Hsee, C.K. & Xiao, Z. (2006). The majority rule in individual decision making. *Organizational Behavior and Human Decision Processes.* Vol 99 (1), pp. 102-111.