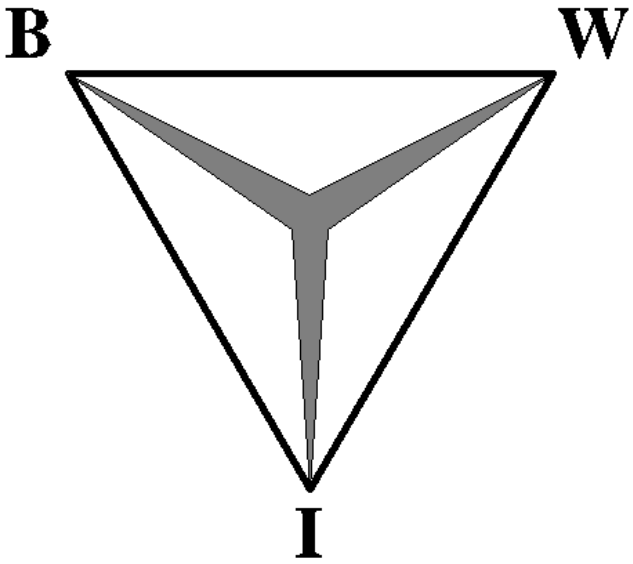
Information Security
Risk Analysis and Decision Modelling



July 2002

In cooperation with:
Deloitte Touche Tohmatsu
Orlyplein 50
1034 DP Amsterdam

Gert Braun
BWI-paper
Vrije Universiteit
De Boelelaan 1081a
1187 HV Amsterdam

Preface

As one of the last parts of the BWI[1]-study at the Faculty of Exact Sciences of the Free University (VU) in Amsterdam, the so called BWI-paper is written. In this paper the student must clearly assess an existing problem, using existing literature.

This paper, as the title implies, is about information security. The term information security is seen in its broad view and includes IT (systems) security as well. This paper has been made during the start of an internship at Deloitte Touche Tohmatsu (DTT) in Amsterdam. DTT offered an internship about the ROI (Return On Investments) of IT-security measures. During talks about the assignment, the idea came up to start with the BWI-paper during the first month.

During this first month I did a lot of reading on the subject, looking at the different perspectives people have when it comes to information security (and there are a lot!). When finishing the first draft, I had a lot of help from both my counsellors, Bert Kersten (VU) and Coby Peeters (DTT), who reviewed it and made comments. Also my other colleagues at DTT provided me with interesting insights into the subject. Last but not least, the persons I personally talked to (which are mentioned in the bibliography). I would like to take this opportunity and thank them all for their support.

I have enjoyed writing this paper and I am happy to receive any comments and/or questions you might have.

Gert Braun
gdhbraun@cs.vu.nl or
gbraun@deloitte.nl (till end 2002)

1 BedrijfsWiskunde & Informatica, which is best translated as Business Mathematics & Computer Science

Abstract

Information security is an ancient concept, but with the increased use of electronic information systems in the last decades, the need for securing these electronic systems has increased. This paper identifies the important elements of information security. We look at the differences in qualitative and quantitative analysis and compare them. After describing some ways of graphically representating decision problems, we take a look at some of the alternatives for the future, namely decision modelling, as described by Soo Hoo (2000), and the due care approach, as described by Parker (1998).

Key Words: information security, qualitative and quantitative analysis, influence diagram, decision modelling, due care

Table of contents

Introduction

The past two decades we've seen a large growth in information systems and its importance. In almost every line of business information systems form an essential part of their existence. The amount of information stored electronically has increased a great deal. Critical business information, personnel and customer data and more are all stored electronically.

Although information security as a whole can be considered an ancient concept, with the increased use of information systems and its storage of confidential data, the need for 'electronic' information security has grown. This paper uses the term information security, as the security responsible for the securing of information and its systems. More explicit, the protection of information (see next paragraph) and the protection for continuation of electronic information systems (computer, network etc.).

Information security is often seen as the protection of the availability, integrity and confidentiality of information.

- Confidentiality: Disclosure of information (systems) only to authorized individuals
- Integrity: Completeness, validity and readability of information (systems)
- Availability: Accessibility of information (systems)

These three concepts (known as CIA[2]) need to be sufficiently protected by security controls. Security controls range from enforcement of complex passwords to physical entrance security checks.

All information systems are subject to numerous threats. Against those threats there are various countermeasures. Threats and vulnerabilities can lead to either small or catastrofic incidents. Incidents have different impacts on businesses. Information security must be able to handle all these problems. The question is how to analyze the threats and select the proper countermeasures.

Risk analysis consists of evaluating the threats, vulnerabilities, impacts and countermeasures. Risk management can add the creation of a cost-effective security program. Decision analysis, or decision modelling is referred to as the formal procedure for analyzing decision problems (Howard, 1966). All these terms (including risk assessment) are used intensively throughout this paper.

2 These three concepts have been around for decades. In 1998 Donn B. Parker argued these three concepts are not enough. He added utility, authencity and possession for more precise areas for protection. The known CIA will do for this paper.

This paper will handle the following research questions:

- What are the important elements in information systems security?
- What are the differences between qualitative and quantitative analysis concerning information security?
- Which tools are currently available for information security risk analysis and management?
- What will the future hold for information security risk analysis and assessment?

The paper ends with a critical note about risk assessment in the form of a description and summary of "Fighting Computer Crime" by Donn B. Parker (1998). Although risk analysis and assessment gets the most attention in this paper, Parker's views can not be underestimated, because of his many years of experience.

Paper overview

Chapter one handles the basic elements of information security. It identifies and shows examples of these elements.

Chapter two gives an overview of the history and future of information security analysis. It also debates qualitative versus quantitative analysis.

Chapter three provides a view into two usable analysis tools, namely CRAMM and @Risk.

Chapter four summarizes a decision modelling approach described in a working paper by K.J. Soo Hoo. It shows a mathematically generic way of describing the problem using quantitative data.

Chapter five looks to the problem from a different perspective. Donn B. Parker's book "Fighting Computer Crime" (1998) provided a valuable insight into the way he thinks information security should be conducted. Not through analysis, but through a due care approach.

Chapter six gives a short summary and conclusion of the relevant literature.

1. Security elements

This chapter will identify and explore the most important elements concerning information security. Each paragraph identifies and explores a different element.
Some have argued that the element identification below is dated and systems have to be viewed on a broader scale, an understanding of the system "as a whole". Although there is obviously a truth in this view, because of the growing complexity of systems and therefore the explosive growth in work needed to assess the identified elements, these elements remain important to distinguish.

1.1 Assets

Every type of security is inititiated by the need for protection of an asset. Assets in information systems include hardware, software, data, people, documentation and supplies. Security controls try to protect these assets the best acceptable way. An assets' value is based on its cost, sensitivity, mission criticality, or a combination of these. When an assets' value is not directly based on costs, it is usually converted to the equivalent amount of money.

1.2 Threats[3]

The smooth functioning of information systems is threatened by technical development, technical problems, physical threats, human frailty, and inadequacies of social, political and economic institutions. Threats may arise from intentional or unintentional acts and may come from internal or external sources.

Technical problems can be computer hardware or software problems. They are sometimes hard to understand and can come completely unexpected. They may be caused by intentional attacks on the system, either from the inside or the outside. Physical threats can be extreme environmental events or adverse physical plant conditions. Human beings can make numerous types of errors contributing to problems. The diversity of the users – employees, consultants, customers, competitors or the public - of a system and their security awareness, training and interest all contribute to the overall security of an information system. Lack of training and knowledge causes unawareness of potential harm.

3 Paragraph based on: Guidelines for the Security of Information Systems (1992)

For instance, the choice of a password. Many users, without guidance, choose obvious passwords, which are easily ascertained. Others frequently put passwords on the side of a terminal or on the back of a keyboard. Both are apparent security blunders.

External attacks enjoy the most media attention, but may not be that important at all. Internal attacks are still often considered as the main threats to information systems, though there has been a shift from internal to external perceived threats. The conventional wisdom that 80% of intentional security attacks are caused by insiders, might not be true anymore. This is partly due to increased monitoring and increased awareness with insiders, as to the growth of external attacks[4].

An extensive but not exhaustive list of threats identified by the qualitative analysis tool CRAMM (the CCTA Risk Analysis and Management Model provides a qualitative method for identifying important controls; you can find more about CRAMM in chapter three) can be found in appendix A.[5]

1.3 Vulnerabilities

All types of threats named above can be considered as endangering information systems. Although most have always been threats, some have grown relatively more important over the years. With the proliferation of computers, increased interconnectivity, the increasing number of users and the growth of networks (the internet and intranets), the vulnerabilities of information systems have become harder to cope with. Grown vulnerabilities include the multiplying of possible failure points, the inability to adapt to technological leaps forward and the slow evolution of legal fundaments in this domain.

A good example of the latter is the escape from justice by Onel de Guzman, the suspected author of the famous 'I love you'-virus. The Philippines did not have any legislation about computer crime, and were unable to punish de Guzman. A month after the release they had rushed through a legislature which enabled Philippines law enforcement authorities to fine those who use computers for criminal purposes in an amount equal to the actual damage caused, but no less than $2350. Perpetrators will also face jail terms of up to three years[6]. Luckily for de Guzman he cannot be fined by this new

4 In the CSI/FBI Computer Security Survey 2002, already 74% of the respondents identified the internet as a frequent point of attack in 2002. In 2000 this number was 59%, in 1996 only 38%. Although partly caused by the growth of the internet, it shows an absolute growth of external attacks.

5 An interesting reading may be the Sandia Report by John Howard and Thomas Longstaff (October 1998) who tried to present a common language for computer security incidents. They developed a minimum set of 'high-level' terms, along with a structure indicating their relationships.

6 Adlaw website: 'Philippines Passes New Web Crime Law And Will Prosecute "Love Bug" Suspect', June 19, 2000

legislation, with the amount of damage estimated by the 'I love you'-virus being as high as $8.75 billion worldwide[7].

One should expect higher vulnerabilities for businesses which include:

- high geographic distribution
- large scale computer network environments
- amount of access by third parties

1.4 Impact

The impact of security breaches on companies can be enormous. This can be concluded by just looking at the estimated annual losses from the CSI/FBI Security Survey 2002. According to this survey, in the last six years they have grown from $100 billion in 1997 to $455 billion in 2002. These numbers came from around 250 large US corporations.

Consequences on businesses are dividable in two categories: direct losses and consequential losses. Direct losses include: hardware, software, documentation, personnel and physical environment. Consequential losses include: goods, funds, intellectual assets, valuable information, competitive advantage, orders, production efficiency, goodwill, penalties, business credibility, new ventures held up, lower share price, reduction in staff morale etc.[8].

Direct losses are usually not as costly as consequential losses. Therefore the control and prevention of consequential losses must be prioritized above direct losses.

1.5 Controls / (Counter)measures

Controls for the security of information systems can be roughly divided into three possible strategies[9]:

1. Prevention of incidents
2. Prevention of consequences after an incident has taken place
3. Mitigation of consequences after they have occurred

Of course, the preferred strategy is prevention of incidents, though in certain cases this is not possible, for instance a tornado. There is no point in trying to prevent this incident (as yet), only mitigation of the consequences is

7 Computer Economics: 2001 Economic Impact of Malicious Code Attacks

8 Taken from: Guidelines for the Security of Information Systems (1992) and others

9 Risk & Chance: Chapter 9 - Handling Hazards; Fischhoff, Hohenemser, Kasperson and Kates, blz. 161

possible. Most measures concerning the security of information systems try to prevent incidents from happening.

The identification of appropriate security controls for an information system is a complex issue. There are numerous decision criteria that may be applied for determining what controls to implement[10]:

- *Deterministic benefit-cost*: Estimate the benefits and costs of the alternatives in economic terms and choose the one with the highest net benefit
- *Probabilistic benefit-cost*: Same as deterministic benefit-cost but incorporate uncertainties and use expected value of resulting uncertain net benefit
- *Cost effectiveness*: Select a desired performance level, perhaps on noneconomic grounds. Then choose the option that achieves the desired level at the lowest cost.
- *Bounded cost*: Do the best you can within the constraints of a budget that is the maximum budget company is prepared to devote to the activity
- *Maximize multi-attribute utility (MAU)*: This is the most general form of utility based criterion. Rather than use monetary value as the evaluation measure, MAU involves specifying a utility function that evaluates outcomes in terms of all their important attributes. The alternative with maximum utility is selected.
- *Minimize chance of worst possible outcome / maximize chance of best possible outcome*

Last but not least is there is an approach described by Donn B. Parker, which he calls the baseline or due care approach. Chapter five handles this approach. He, by the way, proposes the use of the word safeguards instead of measures, countermeasures or controls. Although he might be right by saying it sounds more positive, the word means the same in practice.

10 All these criteria are cited from "Uncertainty: A guide to dealing with uncertainty in policy analysis", page 26, by M. Morgan and M. Henrion (1998). Only utility-based criteria are cited.

2. Analysis and modelling

There has always been extensive debating between the differences and advantages of qualitative analysis versus quantitative analysis. The complete debate is beyond the scope of this paper, but this chapter will give a short impression of the differences between the two types, associated with information security, starting with an historical overview of information security risk analysis and modelling. Ending this chapter is a paragraph about the future of security risk analysis and modelling.

2.1 Historical overview[11]

In 1979, the National Bureau of Standards published the Guideline for Automatic Data Processing Risk Analysis[12] (which is now withdrawn). It proposed a new metric for measuring computer–related risks: Annual Loss Expectancy.

$$ALE = \sum_{i=1}^{n} I(O_i)F_i \quad \text{with} \quad \begin{array}{ll} \{O_1,...,O_n\} & = \text{Set of harmful outcomes} \\ \mathrm{I(O_i)} & = \text{Impact of outcome i in dollars} \\ \mathrm{F_i} & = \text{Frequency of outcome i} \end{array}$$

Although this metric was never enshrined as a standard, is was heavily used in the early days of information security risk analysis. The main flaw of the ALE is that it cannot distinguish between high-frequency, low-impact events and low-frequency, high-impact events.

In the mid-80's, several workshops were held about computer security risk management. The methodologies (and software tools) that sprang from these workshops, are usually seen as the first generation in computer security risk management. They provided a consensus framework for security risk management. Identified elements include the ones handled in chapter 1. Although the last few years different views have emerged, which were mostly initiated by the fact that with the growing complexity of systems a thorough examination takes a lot of time, there is still commercialized software on the market which implement the common framework (or similar schemes). Examples are BDSS, @risk and CRAMM. The latter two are described extensively in chapter three. BDSS will not be discussed further because of lack of documentation.

11 This historical overview is partially based upon the historical overview found in the paper 'How much is enough?' by Kevin J. Soo Hoo (June 2000)

12 National Bureau of Standards, FIPS PUB 65

Protected by corporate secrecy there have been some new approaches to computer security risk management in the 1990s. They mostly focus on the deployment and organizational acceptance issues, leaving the complexity and uncertainty issues unaddressed. Four general approaches from leading organisations can be identified: Integrated Business Risk-Management Framework, Valuation-Driven Methodologies[13], Scenario Analysis Approaches and Best Practices[14].

As mentioned earlier these four approaches do not address the complexity and uncertainty present in information systems risk analysis. Soo Hoo (2000) argues that they cannot be viewed as sufficient due to several shortcomings, including lack of cost justification, inability to forecast and disregard of measure's efficacy. He believes these shortcomings will urge organizations to seek more satisfactory approaches, like his own model which is described in chapter four.

The last few years there have been pleads to stop identifying all type of threats, vulnerabilities and impacts and as focus more on the system "as a whole". Instead of viewing the system as a collection of assets, the so called 'third' generation modelling should identify the systems purpose and behavior, structure, relationship to its environment and history all in a common framework[15]. After this broad *understanding* of the system, safeguards must still be identified, evaluated and ranked. According to Fletcher and others (1995), the *understanding* of the system "as a whole" should provide a more balanced and comparable solution. Not much has been done with these pleads, and there are no tools in use which employ this type of approach.

2.2 Qualitative analysis

The easiest way to explain the difference between qualitative and quantitative analysis is the use of words vs. the use of numbers. Qualitative analysis uses ordinal scales to distinguish levels of threat, vulnerability and risk. Software tools (for instance CRAMM) ask the user to give the estimated probability of a threat happening, and the expected loss on an asset. It splits the possibilities in 'Low, Normal, High' (or sometimes 'Very Low, Low, Normal, High, Very High'). Through matrices these threats and impacts are matched and a ordinal value is given to the importance of securing a certain asset. (More on CRAMM can be found in the next chapter.)

13 For complete descriptions and case studies, see 'Managing Business Risks in the Information Age', New York, The Economist Intelligence, 1998

14 See 'Best Practices in Network Security', Frederick M. Avolio, Network Computing, 2000 <http://www.networkcomputing.com/1105/1105f2.html>

15 Paper for the NISSC, 'An Open Framework of Risk Management', R. Craft, G. Wyss, R Vandewart, D Funkhouser from Sandia National Labs

The main disadvantage of qualitative analysis is that their findings cannot be tested to whether they are statistically significant. No 'statistical' answers can be given, only relative priorities. This leads to another disadvantage, the inability to give any indications about the uncertainties of the found figures. There is also no possibility for creating confidence intervals for the results. It therefore cannot, for instance, give any worst-case / best-scenario estimates.

2.3 Quantitative analysis

Quantitative analysis classifies the same elements as qualitative analysis, but uses numerical data to fill in the probabilities and tries to construct complex statistical models to predict what will happen. It uses historical data or expert estimations to provide the numbers. It needs accurate data to establish probability distributions and measure uncertainties.

The main disadvantage of quantitative analysis concerning information systems security is the absence of that accurate data. Numbers have been accumulated, but they cannot be seen as significant, because a lot of security breaches are not noticed, a lot are not reported and the losses are hard to estimate. Organizations are not happy to report a major hack because of possible media attention. Expert estimations can be used, but are always subjective judgments. There are a lot of downsides on the use of these estimates. M. Morgan and M. Henrion in 1998 concluded "*human judgments about uncertainty, or judgments made in the presence of uncertainty, frequently rely on a number of simple cognitive heuristics. Although in many circumstances these heuristics serve us well, they can also be the source of significant bias or even outright error. How significant these problems are is a strong but largely unknown function*".

An important advantage is already mentioned in the preceding paragraph. The ability to give sound figures containing uncertainties and confidence intervals for the results, provides quantitative analysis with an obvious advantage over qualitative analysis.

2.4 Future analysis and modelling

The future of analysis and modelling information security lies in the ability to get good data to support any model or tool. Most used software tools available on the commercial market use qualitative analysis to make predictions and recommendations about security measures. Organisations can use these tools to evaluate their information systems security. Some quantitatives tools are in use, but they almost always need expert data, which cannot always be considered as satisfying numbers (see the previous paragraph). Historical quality data is not available, because the numbers are not known or are not available due to corporate secrecy. Motivation for gathering quality data might be found in insurance needs, liability exposure, the need to avoid negligence and market competition. Although profound

motivations they can not guarantee it will lead to sophisticated gathering of data and the possibility for quantitative analysis.

If good data does get available quantitative analysis methods can provide a much broader view of information security risks. These methods can be extented to larger populations, or rather, different organisations without needing a complete new assessment. They can also provide significant statistical analysis, giving confidence intervals about the probability of threats and impacts. The formal approach of decision analysis and modelling can be incorporated. This makes justifiable cost-benefit analysis on which security measurement choices can be made, possible.

Chapter four will focus on quantitative analysis and decision modelling. The way the quantitative data might be gathered, whether through expert judgment or historical data is not the issue.

3. Risk analysis tools

This chapter explores some of the currently available tools for information security risk analysis and management. Mentioned earlier, CRAMM (CCTA Risk Analysis and Management Model) provides a qualitative method for identifying important countermeasures. @Risk is a more general approach, usable for any decision. It adds the use of distributions to your spreadsheets.

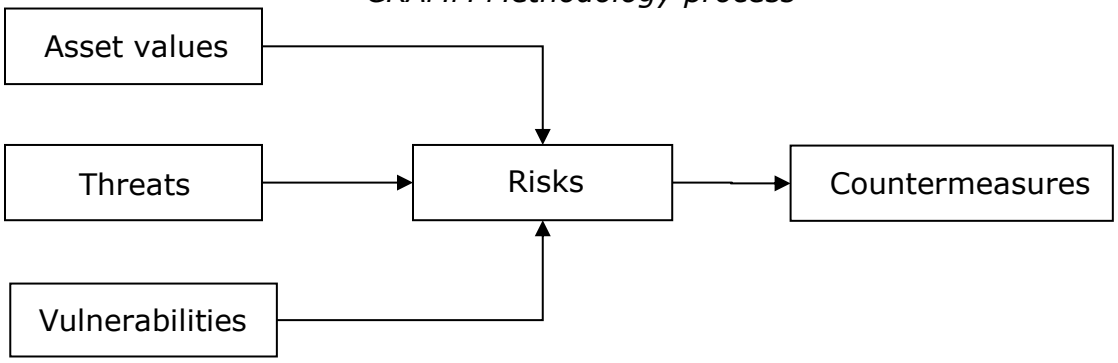
3.1 CRAMM

The CRAMM method is owned, administered and maintained by the UK Security Service on behalve of the UK Government. The corresponding CRAMM software tool has been developed by industry in consultation with the UK Security Service. Because of its origin, CRAMM is mostly used by national defense departments and very large corporations.

The CRAMM method recognizes asset values, threats and vulnerabilities. The values of these parameters are assessed qualitatively through interviews with the owners of the assets, the users of the system and security officers. Asset values are either physical replacement costs or a data value assessment.
The outcome of a CRAMM review consists of a set of recommended countermeasures that are reviewed as necessary for eliminating certain risks in information systems.

The process

Figure 3.1
CRAMM Methodology process



The process starts by identifying and valuating the assets within the system. This involves the data, software, hardware and the relationships between these assets, which comprise the system. This is stage one.

In stage two, threats and vulnerabilities are assessed using questionnaires, rating threats on a scale of very low, low, medium, high or very high. Vulnerabilities are rated on a schale of low, medium or high. CRAMM then calculates the measures of risks using a risk matrix. The risk matrix and explanation can be found in appendix B. CRAMM uses a scale from 1 to 7 for measuring risks.
Stage three covers the selection of appropriate countermeasures. CRAMM first searches its extensive countermeasure library (2400 measures) for measures which meet the risks identified in the first stages. Already installed countermeasures need to be identified and removed from the selection by CRAMM. At last the countermeasures need to be prioritised, which CRAMM can do automatically.
The last step is making a management report. CRAMM contains skeletons for exporting to a word processor.

Overview

The method just described provides the practitioner with a number of benefits, the most important being able to do a justifiable cost-benefit analysis. It does however need a lot of skill to perform such an analysis. It is therefore highly recommended not to use CRAMM if you're unexperienced, instead using a trained practitioner is suggested. CRAMM requires a lot of work and takes a lot of time. Also is it most suitable for systems already operational rather then systems which are under development. For systems in development it's harder to assess threats and vulnerabilities, because some questions cannot be answered (for instance the number of failures over the last month).

Although CRAMM is meant for risk analysis and management, it also always gives a great insight in the system as a whole. It forces the users to identify all parts of the system and think about which ones support business processes.

CRAMM also provides a so-called 'What-if' tool. It enables you to explore the effect of changes to the system. It can be used to illustrate implications of different options open to the management, or determine the effect of proposed changes to configuration.

Pros and cons

In conclusion, CRAMM has its pros and its cons. Some have already been identified above. CRAMM:

- offers a structured approach to risk analysis
- forces users to think about the system and provides great insight to the system as a whole
- contains an extensive countermeasure library
- is highly automated

But it has some cons too. CRAMM:

- can only be used by experienced practitioners
- takes a lot of time (months)
- generates a lot of hard-copy output (questionnaires)
- is slow in operational performance

3.2 @risk

@risk is a Microsoft Excel or Lotus 1-2-3 add-in from Palisade (further focus will be on the use in Excel). It is primarely a risk analysis tool, meant for any type of risk analysis, not specifically for information systems. @risk adds to Excel the ability to define probability distributions to variables.

@risk comprises three main components:

- the model window, which is used to designate inputs and outputs for the simulation, view input distributions, and define correlations between variables
- the Excel add-in, which provided the ability to directly type @risk functions into Excel cells
- the results window, which gives a variety of outputs, including interactive graphs and scenario reports

It has a user-friendly interface, using colored text in Excel spreadsheets to make it easy to identify cell values which run @risk functions. Palisade promotes the speed of @risk, which is also reviewed as being very fast, even on slow machines.

The process[16]

Risk Analysis in @RISK is a quantitative method that seeks to determine the outcomes of a decision as a probability distribution. In general, Risk Analysis with @RISK encompasses four steps:

1. Develop a Model - First, define your problem or situation in an Excel worksheet format.
2. Identifying Uncertainty - Next, determine which inputs in your model are uncertain, and represent those using ranges of values with @RISK probability distribution functions. Identify which result or output of your model you want to analyze.

16 Summarize taken from the Palisade website: See <http://www.palisade.com/html/risk/facts.html> for a more detailed description.

3. Analyzing the Model with Simulation - Run your simulation to determine the range and probabilities of all possible outcomes for the outputs you've identified.
4. Make a Decision - Armed with complete information from your analysis, and your personal preferences, make your decision.

Pros and cons

In conclusion, @risk has its pros and cons.

Pros:

- tight integration with Excel and/or Lotus 1-2-3
- extensive list of functions
- quality graphical output
- fast performance
- wide usability

Cons:

- hard to learn interface for unexperienced users
- not specifically designed for information systems

3.3 Conclusion

CRAMM and @risk are two completely different tools for doing risk analysis on information security. CRAMM is slow, takes a lot of time and has a lot of paperwork which needs to be filled in properly. If used correctly, it does however give an enormous amount of information about an information system and its security.
@risk requires the user to determine the functions needed for the analysis. Its use in Excel eases the process, but it does require some time to master.

Overall, CRAMM is best used in large corporations, which have the time and funding for an extensive analysis. A smaller firm can do better with the speed of @risk.

4. Decision modelling

The risk analysis tools described in the previous chapter shows qualitative and quantitative ways for dealing with risk. Chapter two described the adventages and disadvantages of qualitative versus quantitative analysis methods. This chapter starts with an overview of graphical representations for decision problems as an introduction to a decision modelling technique described by K.J. Soo Hoo (2000).

4.1 Graphical representations[17]

There have been different attempts at creating the perfect graphical technique for representing decision problems. All of them have there own pros and cons. We explore four types, some old ones, some newer ones.

For this exploration we use a small decision problem commonly known as the oil wildcatter's problem[18].
An oil wildcatter must decide either to drill (*d*) or not to drill (*~d*). He is uncertain whether the hole is dry (*dr*), wet (*we*) or soaking (*so*). The cost of drilling is $70.000. Table 4.1.1 shows all pay-offs.

Table 4.1.1
Pay-off matrix oil wildcatter's problem

State	Act		Probability of state
	Drill (*d*)	Not drill (*~d*)	
Dry (*dr*)	-$70.000	$0	0.500
Wet (*we*)	$50.000	$0	0.300
Soaking (*so*)	$200.000	$0	0.200

The wildcatter could take seismic soundings that can determine the geological structure at the site, at a cost of $10.000. The soundings will disclose whether the terrain below has no structure (*ns*), an open structure (*os*), or a closed structure (*cs*). Table 4.1.2 shows the probabilities of seismic test results conditional on the amount of oil.

17 This paragraph uses the paper "A comparison of graphical techniques for asymmetric decision problems" by C. Bielza and P.Shenoy (1999), and the working paper 'Game trees for decision analysis', by P. Shenoy (1996).

18 This paper uses a slightly modified version from Raiffa (1961), as it is used in the working paper 'Game trees for decision analysis', by P. Shenoy (1996)

Table 4.1.2
Probabilities of seismic test results conditional on the amount of oil

P(R | O)		Seismic test results (R)		
		No structure (*ns*)	Open structure (*os*)	Closed structure (*cs*)
Amount of oil (O)	Dry (*dr*)	0.600	0.300	0.100
	Wet (*we*)	0.300	0.400	0.300
	Soaking (*so*)	0.100	0.400	0.500

4.1.1 Decision trees

Decision tree representations give a chronological and fully detailed view of the structure of the decision problem. Before any decision tree can be completely specified, the required conditional probabilities need to be 'preprocessed'.

A count of algebraic operations shows that 24 operations are required for the preprocessing and 30 operations are required to prune the decision tree, adding up to 54 operations.

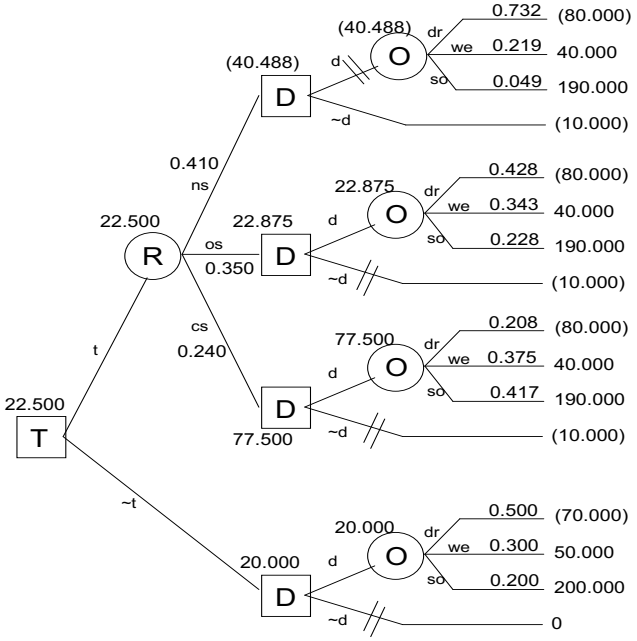


Figure 4.1.1
Decision tree representation and solution of the oil wildcatter's problem

Figure 4.1.1 shows the decision tree and solution for the example using the roll-back method. In this method, a chance node is pruned by averaging the utilities using the probabilities on the edges. A decision node is pruned by maximizing the utilities associated with its edges.
The optimal strategy is to test, not drill if it reveals no structure, and drill otherwise. The expected profit with this strategy is $22.500.

Decision trees are easy to understand and solve. They illustrate every relevant scenario. The use of scenarios contributes to the exponential growth of decision trees and limits its use to small problems. Repeating subtrees (coalescence) need to be identified manually.

Some methods have been proposed for solving the problem of preprocessing. For additional information see von Neumann-Morgenstern (1944) on the use of information sets and Olmsted's (1983) and Shachter's (1986) arc-reversal method.

4.1.2 Game trees

Game trees are actually a form of decision trees. The main difference between the two is the fact that game trees can use a sequence of variables which represent time or causation instead of information. In decision trees, the sequence must represent information and nothing else. This flexibility in game trees allows it to represent any decision problem without preprocessing. Smaller problems can be solved easy by enumerating the expected value of all possible strategies, and then choose the highest value. This way of computation is exponential with the number of information sets. A more efficient method is using local computation or dynamic programming. An explanation of this method can be found in Shenoy (1996). The roll-back method explained in 4.1.1 can also be used to solve game trees. Figure 4.1.2 shows a small problem graphically using a game tree and a decision tree.

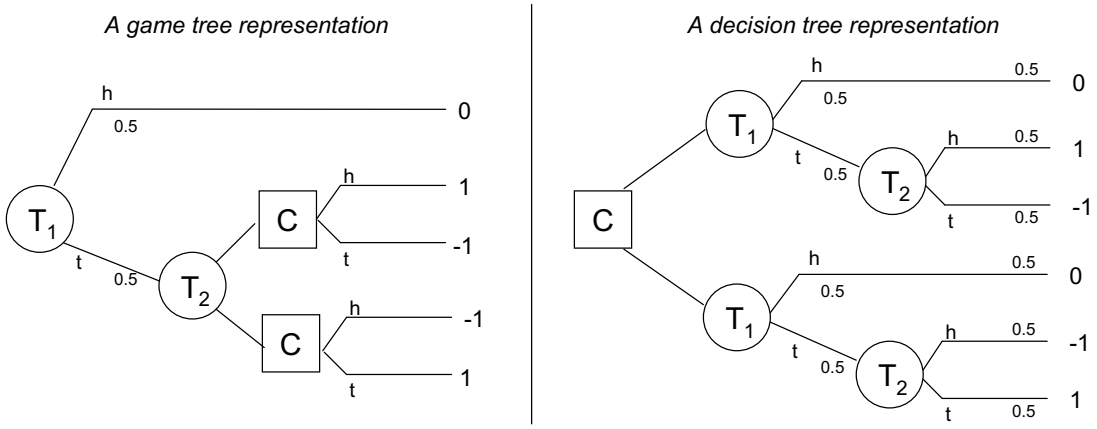


Figure 4.1.2
The difference between game trees and decision trees representations

There are no general results whether the computation of the roll-back method for game trees is more efficient than that for decision trees.

4.1.3 Influence diagrams

An influence diagram is a directed acyclic graph that displays decision variables, chance variables, factorization of the joint probability distribution into conditionals, factorization of the joint utility function, and information constraints. They avoid the combinatorial explosion of decision trees by surpressing the details of the number of branches available at each decision or chance node.

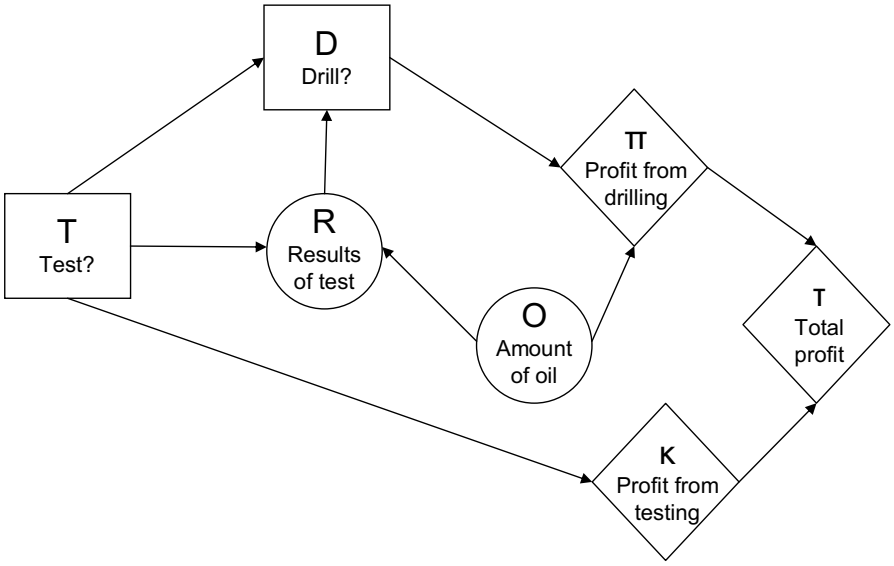


Figure 4.1.3
Influence diagram representation of the oil wildcatter's problem

Influence diagrams main strength is its compactness. They are easy to understand and it can detect the presence of unnecessary information in a problem by identifying irrelevant or barren nodes.

Influence diagrams are best suited for problems which have conditional probabilities. This is typical for the modelling of probabilities assessed by a human expert. For probabilities induced from data this is not always the case.

4.1.4 Valuation Networks

A valuation network consists of two types of nodes, variable and valuation. Variables are either decision or chance nodes, and valuations are indicator,

probability or utility nodes. Figure 4.1.4 gives a valuation network of the oil wildcatter's problem.

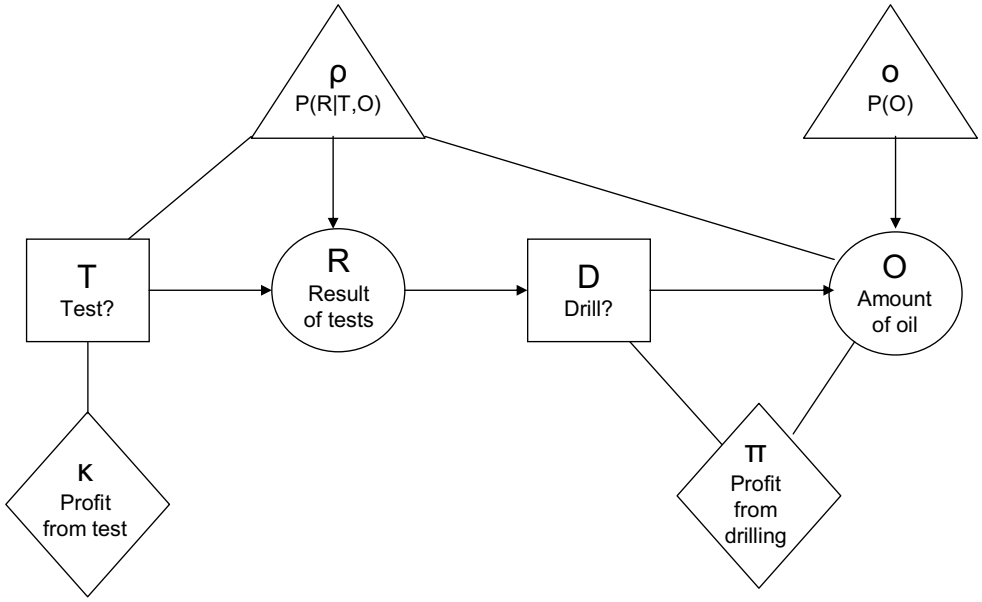


Figure 4.1.4
Valuation network representation of the oil wildcatter's problem

Decision variables are depicted by rectangles, chance variables by circles. Utility valuations, which represent additive factors of the joint utility function, are depicted by diamond-shaped nodes. Probability valuations represent multiplicative factors of the family of joint probability distributions for the chance variables, and are depicted by triangular nodes. Directed arcs are used to represent information constraints. The arc (R,D) means that de results of the test R are known to the decision maker at the time he or she has to choose a decision to drill or not to drill. Alternatively, the results of the test R are not know when the decision maker decides whether to test or not (T). For the solution of valuation networks, see Shenoy and Bielza (1999).

Valuation networks are compact and encode conditional independence relations in the probability model. They do not need any preprocessing. They are mostly compared to influence diagrams, because of their compactness. For a more extended overview of strenghts and weaknesses, again see Shenoy and Bielza (1999).

4.2 Modelling

The previous paragraph gave an overview of different graphical techniques for representing decision problems. This is now continued into proposing a possible modelling technique. This paper does not intend to have the answer on how to model information security decision problems, but it does try to give an example on how such a model could be implemented. For this example, the working paper from K.J. Soo Hoo (2000) is used as a primary source. He proposed such a model. This paper summarizes his model and ideas.

When using decision modelling for analysing information security, according to Soo Hoo, influence diagrams are preferred. This is because of the compactness and intuitiveness. Everybody should be able to understand them within seconds. Trees also offer this advantage but are usually much larger. Trees always have discrete probabilities, while for a simulation's convenience continuous distributions are easier. So for this example, influence diagrams are used.

Soo Hoo gives an example influence diagram regarding information security (see figure 4.2.1).

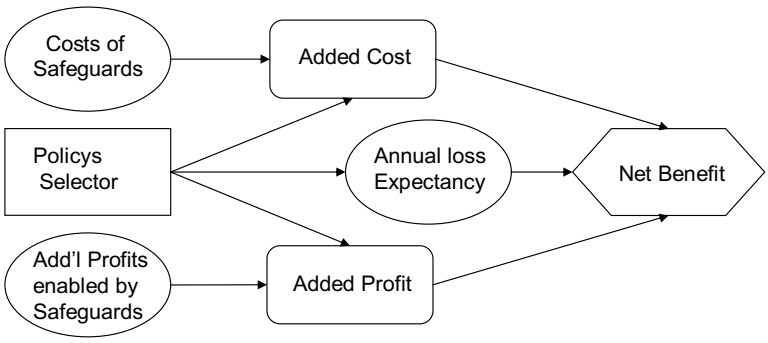


Figure 4.2.1
Example influence diagram for an information security decision problem

The most important decision that needs to be made is the selection of safeguards. The model as shown in figure 4.2.1 gives the user the ability to group several safeguards in one policy, and compare different policies.

The model for selecting the safeguards uses the following variables:

Table 4.2.1
Variables used in example model

B_i	Bad event *i* where $i = \{1,2,3,\ldots,n\}$ For example, data theft, service outage, employee theft
S_j	Safeguard *j* where $j = \{1,2,3,\ldots,m\}$ For example, awareness program, firewalls, encryption software
P_k	Policy *k* where $k = \{0,1,2,3,\ldots,l\}$ For example, status quo, incremental change, major improvement. By convention, $k=0$ represents the status quo
$R(S_j)$	New profits enabled by adoption of safeguard S_j
$I_k(S_j)$	Binary function indicating if safeguard S_j is included in policy P_k
$F_0(B_i)$	Initial estimate of the relative frequency of bad event B_i
$D_0(B_i)$	Initial estimate of the consequences of, or damage from, the occurrence of bad event B_i
$E_f(B_i,S_j)$	Fractional reduction in relative frequency of occurrence of bad event B_i as a result of implementing safeguard S_j
$E_d(B_i,S_j)$	Fractional reduction in consequences resulting from the bad event B_i as a result of implementing safeguard S_j
$C(S_j)$	Cost of implementing safeguard S_j
ALE_k	Annual Loss Expectancy under policy K

Using these variables, the utility function for the objective 'Net benefit' of policy K becomes (with *l* being the total number of policies):

$$Net\,benefit_k = Benefit_k - Added\,cost_k + Added\ profit_k \qquad \forall k = \{1,2,3,\ldots,l\} \quad (1)$$

A calculation needs to be done for each policy *k* because the decision is about which policy to adopt. Other coefficients like risk tolerance, time-value of money or others can be introduced in the function. Soo Hoo keeps it simple though. Another way to keep it simple, is not considering intangible concepts like peace of mind, goodwill, business credibility, reputation and public trust. Weights that need to be placed on these concepts are always dependent on special circumstances and hard to give weight to.

The differences in annual loss expectancies of the different policies compared to the status quo leads to the expected benefit function (with ALE_0 being the status quo):

$$Benefit_k = ALE_0 - ALE_k \qquad \forall k = \{1,2,3,\ldots l\} \quad (2)$$

The equation for the ALE_k is:

$$ALE_k = \sum_{i=1}^{n} \left\{ F_0(B_i) D_0(B_i) \prod_{j=1}^{m} \left[(1 - E_f(B_i, S_j) I_k(S_j))(1 - E_d(B_i, S_j) I_k(S_j)) \right] \right\} \quad (3)$$

An important concept in information security is the enabling of new business opportunities. The model uses a simple equation:

$$Added\ profit_k = \sum_{j=1}^{m} R(S_j) I_k(S_j) \qquad \forall k = \{1,2,3,...,l\} \quad (4)$$

Costs are seen as more easy to quantify, because they exist of quantifiable variables like investments in hardware, software, workers salaries and maintenance. Some costs are not so easily interpreted, like workers morale and other drops in productivity because of newly adopted security measures. The equation for added costs is:

$$Added\ cost_k = \sum_{j=1}^{m} C(S_j) I_k(S_j) \quad (5)$$

These equations lead to the overall equation for the *Net benefit*:

$$Net\,benefit_k = \sum_{i=1}^{n} \left\{ F_0(B_i) D_0(B_i) \left[1 - \prod_{j=1}^{m} \left[(1 - E_f(B_i, S_j) I_k(S_j))(1 - E_d(B_i, S_j) I_k(S_j)) \right] \right] \right\}$$
$$+ \sum_{j=1}^{m} R(S_j) I_k(S_j) - \sum_{j=1}^{m} C(S_j) I_k(S_j) \quad (6)$$

Soo Hoo continues by describing a sensitivity analysis for identifying the key variables with the greatest influences on the decision. Especially interesting are the "cross-over" points, where the best decision changes from one policy to an alternative.

New information about a variable (for instance greater certainty) has its own value. The value of information about a certain variable can be computed by:

$$Value\ of\ information\ for\ \overline{C}(S_j) =$$
$$\max_{k=1}^{l} \left[Net\ benefit(ALE_k, R(S_j), C(S_{j \neq j'}) \mid \overline{C}(S_j)) \right] - \max_{k=1}^{l} \left[Net\ benefit(ALE_k, R(S_j) \mid C(S_j) \right]$$
(7)

This value is not computable before the information is known. The expected value however, is. The expected value of perfect information (EVPI) can be found by computing:

$$EVPI\ for\ \bar{C}(S_j) = \sum_{\bar{C}(S_{j'})} P\left[C(S_{j'}) = \bar{C}(S_{j'})\right] \underset{k=1}{\overset{l}{Max}}\left[Net\ benefit(ALE_k, R(S_j), C(S_{j\neq j'}), \bar{C}(S_j))\right]$$
$$- \underset{k=1}{\overset{l}{Max}}\left[Net\ benefit(ALE_k, R(S_j), C(S_j)\right] \quad (8)$$

The EVPI is always positive for variables that matter to the decision. If they do not matter, they have an EVPI of zero.

4.3 Conclusion

Summarizing his findings, Soo Hoo mentions several key advantages that decision modelling offers over earlier risk models. Firstly, its top-down, iterative approach prevents the model from becoming impracticle. Secondly, influence diagramming provides a great help in the development stage. Although lack of good data is obviously a drawback, the model can compensate by using probability distributions. Soo Hoo continues with *"The adaptability and extensibility of the modelling approach make it generically applicable to virtually any computer security risk-management decision."*

One factor, overlooked by Soo Hoo, is the correlation between different safeguards and their effects. One safeguard might make another safeguard useless or, in contrast, make it more effective. One straightforward example is the enforcements of strong and difficult to guess password. This can be very important for securing your information. But if your personell isn't taught to still keep their password safe, they might resort to sticking postscripts on their laptops to not forget them, rendering the strong password almost worthless.

The most important element for a model as proposed by Soo Hoo is good data. In chapter two, the future of data-gathering is already mentioned. For the model to provide any relevant answers this is definitely needed.

5. Due care approach

The approach of decision modelling shown in the previous chapter has yet to proof it provides a good model for information security. Decision modelling, risk analysis and risk assessment all fall in a large category of 'risk-estimating' methods. They all feature the estimation of risks, losses and possible improvements.
Donn B. Parker is the author of the book "Fighting Computer Crime: A new framework for protecting information" (1998). Through 30 years of experience and over 200 interviews with perpretrators and their victims, he explains why these methods can and do not work. He proposes a method of due care.

5.1 The problems with risk assessment

Parker recognizes a few fatal flaws to quantitative risk assessment. He considers it impractical and sometimes impossible to do a risk analysis and assessment. He summarizes the failures identifying four steps:

Step 1. Risk assessment requires determining the likelihood of future harm involving specific information to be protected. This determination can not be made because there is insufficient loss experience in the specific circumstances being assessed.

Step 2. Risk assessment also requires estimations of future loss from each type of incident. The value of the information involved is often not material and hard to determine.

Step 3. Frequency and size of loss data collected in step 1 and 2 must be combined in a mathematical or logical way. The value of results is always limited by the quality of the inputs. Even using the best mathematics does not make the values valid.

Step 4. The last phase requires selecting controls. Risk assessment, however, only recognizes how must could be lost. Controls still need to be selected experientially or through another method and perform another risk assessement to see if they work.

Parker does not only criticize risk assessment, but also gives alternatives to be used instead. This paper will not discuss all these alternatives, but they are:

- qualitative risk assessment
- focus groups
- brainstorming
- polling information

- delphi technique
- exposure analysis
- scenario techniques
- baseline approach

5.2 Baseline approach

"The baseline controls that we should use to measure our conformance are the ones that any well-managed, information-intensive organization under similar conditions of vulnerability should be using, or should have good business reasons for not using." (Parker, 1998).
This is the definition used by Parker for a due care security. Security, unlike competitive business, is difficult to justify as a bottom-line expense. The baseline approach (due care) is the middle ground, providing protection to avoid negligence, harmful litigation and high insurance costs. There is no standard collection of controls for achieving due care. It all depends on the organization and its competitors. For example; if nine out of ten peer group competitors have installed an IDS (Intrusion Detection System), the company under review should install one too.

Opponents argue that a lot of organizations can end up with the same wrong controls. However, Parker argues, it's better to avoid negligence with unnecessary controls, then to have no controls at all.

5.3 Conclusion

Parker concludes that adopting baseline controls is a easier, less expensive, and more effective way to select safeguards then quantitative risk assessment. It avoids negligence, harmful litigation and high insurance cost. It does not require an excessive amount of resources like risk assessment. When due care is achieved, an organization can apply its remaining resources to identifying new threats and vulnerabilities and tackling control problems.

6. Summary and conclusion

Throughout this paper we've seen multiple ways of looking at information security and multiple ways of trying to analyze the best way of dealing with security threats.

We've seen that qualitative analysis is used more often, because of lack of good data for quantitative analysis. There are no guarantees good data will become available soon, so quantitative analysis on actual historical data may stay an utopia for a while. But if good data gets available, the quantitative approach offers the advantage of precise probabilities and their confidence intervals.

Tools are available for both quantitative and qualitative approaches. Two tools are described, CRAMM and @risk. CRAMM offers the most extensive, but also time-consuming method. It is therefore not recommended for smaller organizations. They should instead choose @risk or other easy-to-use tools.

Looking at the future of information security analysis, we've handled two views; decision modelling from Soo Hoo and due care (baseline) from Parker. Decision modelling offers a mathematic and structured view on information security control policies. The use of influence diagrams provides great help during the development of a model. One thing lacking for Soo Hoo's model (and decision modelling as a whole) is good data. No historical data is available, and will be in the near future.

Parker recognizes this flaw of quantitative analysis and proposes a completely different view. Without trying a complete risk assessment, which in Parker's view will always be impractic to do, he proposes a baseline control effort. Simply summarized as: Do the same for security as your peer group.

The question which remains to be answered is which approach is actually the best at this moment. For now, the lack of good data forces any organization to let go of trying a complete quantitative risk assessment. This does not mean the only alternative is Parker's due care approach, qualitative tools can be used with succes.

Although Parker has 30 years of experience in the field, I think his view is to conservative. Within the near future good data will not become available, but instead of sticking to his due care approach and not care about good data, efforts must be taken to ensure good data will become available as soon as possible. With the risks of information security increasing, the wealth of extra information (i.e. possibilities and confidence intervals) which comes available through good data, is needed.

Appendix A

This appendix gives an overview of the threats for information systems identified by the qualitative analysis tool CRAMM.

Masquerading of user identity by insiders
Masquerading of user identity by contracted service providers
Masquerading of user identity by outsiders
Unauthorised use of an application
Introduction of damaging or disruptive software
Misuse of system resources
Communications infiltration by insiders
Communications infiltration by contracted service providers
Communications infiltration by outsiders
Accidental misrouting
Technical failure of non-network host
Technical failure of network host
Technical failure of storage facility
Technical failure of print facility
Technical failure of network distribution component
Technical failure of network gateway
Technical failure of network management or operation host
Technical failure of network interface
Technical failure of network services
Power failure
Air conditioning failure
System or network software failure
Application software failure
Operations error
Hardware maintenance error
Software maintenance error
User error
Fire
Water damage
Natural disaster
Staff shortage
Theft by insiders
Theft by outsiders
Wilful damage by insiders
Wilful damage by outsiders
Terrorism

Appendix B

This appendix gives both the asset scales and the risk matrix used by the qualitative analysis tool CRAMM.
For instance: An assets commercial value is rated at costing 'between *f*300.001 and *f*3.000.000', its threat level at 'Medium' and its vulnerability at 'HIGH'. For CRAMM the value equals a scale of 4 (see table B.1).
Its overall risk factor is then scaled at 4 also (see table B.2).

Table B.1
CRAMMs asset value scale table

AssetValue	Commercial and economic value (Advantage for competitors worth…)	Financial loss / disturbance of activities (Resulting into losses…)
1	no commercial gain	of ƒ3.000 or less
2	a sum of ƒ30.000 or less (turnover)	between ƒ3.001 and ƒ30.000
3	a sum between ƒ30.001 and ƒ300.000	between ƒ30.001 and ƒ100.000
4	a sum between ƒ300.001 and ƒ3.000.000	between ƒ100.001 and ƒ300.000
5	a sum between ƒ3.000.001 and ƒ30.000.000	between ƒ300.001 and ƒ1.000.000
6	a sum above ƒ30.000.000	between ƒ1.000.001 and ƒ3.000.000
7	Undermines national interests	over ƒ3.000.000
8	No note	over ƒ3.000.000
9	Material damage to national interests	No note
10	Severe damage to national economy	No note

The fact that CRAMM was developed by the UK Security Service for the UK government, explains the high asset values like 'Material damage to national interests'.

Table B.2
CRAMMs risk matrix

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium
Vuln.	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH
AssetValue									
1	1	1	1	1	1	1	1	1	2
2	1	1	2	1	2	2	2	2	3
3	1	2	2	2	2	3	2	3	3
4	2	2	3	2	3	3	3	3	4
5	2	3	3	3	3	4	3	4	4
6	3	3	4	3	4	4	4	4	5
7	3	4	4	4	4	5	4	5	5
8	4	4	5	4	5	5	5	5	6
9	4	5	5	5	5	6	5	6	6
10	5	5	6	5	6	6	6	6	6

Table B.2 - continued

CRAMMs risk matrix

Threat	High	High	High	Very High	Very High	Very High
Vuln.	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH
AssetValue						
1	1	2	2	2	2	3
2	2	3	3	3	3	4
3	3	3	4	3	4	4
4	3	4	4	4	4	5
5	4	4	5	4	5	5
6	4	5	5	5	5	6
7	5	5	6	5	6	6
8	5	6	6	6	6	7
9	6	6	7	7	7	7
10	6	7	7	7	7	7

Bibliography

2001 Economic Impact of Malicious Code Attacks*, Computer Economics*, (Jan 2002)

Avolio, F.M. "Best Practices in Network Security", *Network Computing* (2000) <http://www.networkcomputing.com/1105/1105f2.html>

Bielza, C., Shenoy, P. "A comparison of graphical techniques for asymmetric decision problems" (1999)

Computer Security – Issues & Trends – Vol VII No.1

Craft, R., Wyss, G., Vandewart, R., Funkhouser, D. from Sandia National Labs, "An Open Framework of Risk Management", *NISCC paper*

CSI/FBI Computer Security Survey 2000, 2001 and 2002

Fischhoff, Hohenemser, Kasperson and Kates, *Risk & Chance: Chapter 9 Handling Hazards*, blz 161

Fletcher, S., Jansma, R., Lim, J., Halbgewachs, R. Murphy, M., Wyss, G., "Software System Risk Management and Assurance," Proceedings of the 1995 New Security Paradigms Workshop, 1995, San Diego, CA.

Guidelines for the Security of Information Systems (1992)

Henrion M., Morgan M. "Uncertainty: A guide to dealing with uncertainty in policy analysis" (1998)

Howard, J. and Longstaff, T. "A common language for Computer Security Incidents", *Sandia National Laboratories*, (Oct 1998)

"Managing Business Risks in the Information Age", New York, The Economist Intelligence, 1998

National Bureau of Standards, FIPS PUB 65

Olmsted, S. M., "On representing and solving decision problems," Ph.D. thesis, Department of Engineering-Economic Systems, Stanford University, Stanford, CA. (1983)

Parker, Donn B. "Fighting Computer Crime: A new framework for protecting information" (1998)

"Philippines Passes New Web Crime Law And Will Prosecute 'Love Bug' Suspect", *Adlaw Website*, June 19, 2000 <http://www.adlawbyrequest.com/regulators/PhillCrime.shtml>

Raiffa, H., Schlaifer, R. "Applied statistical decision theory" (1961)

Shachter, R. D., "Evaluating influence diagrams," *Operations Research*, 34(6), 871-882. (1986)

Shenoy, P. "Game trees for decision analysis" (1996).

Soo Hoo, K.J. "How much is enough? A risk-management approach to computer security" Paper (June 2000)

von Neumann, J. and O. Morgenstern, *Theory of Games and Economic Behavior*, John Wiley & Sons, New York, NY. (1944)

Interviewed persons:

- Prof. dr. J.M.A. Berkvens, Information Security Officer, Rabobank International
- Drs. C. Coumou, Seniormanager, KPMG Information Risk Management
- Eric Schansman, retired Information Security Officer, Rabobank International
- Kevin J. Soo Hoo, author of working paper "How much is enough?" (through email)