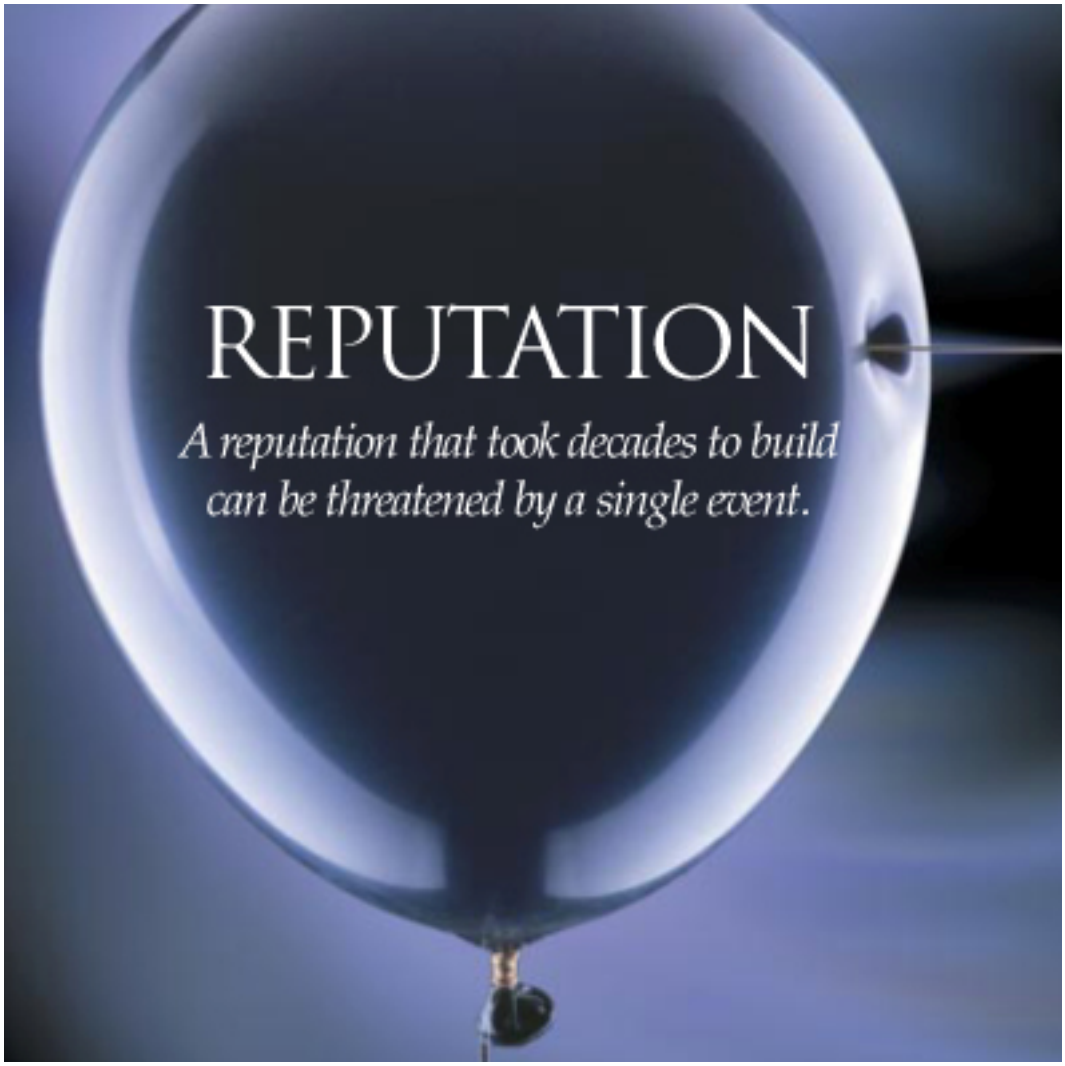
Exploring ways to Model Reputation Loss

A case study on information security at Dutch private banks



A Master thesis for the study Informatics & Economics
Faculty of economics, Erasmus University Rotterdam

Author: Cas de Bie BSc.
Supervisor at Erasmus University Rotterdam: Dr. Ir. Jan van den Berg
Supervisor at PricewaterhouseCoopers: Drs. Frans van Buul
Co-Reader: Prof. Dr. Gert van der Pijl RE

Managementsamenvatting

Dit onderzoek heeft als doel om de relatie tussen beveiligingsincidenten en reputatieschade te verkennen en te modelleren. Hierbij is er gekeken naar de mogelijke beveiligingsincidenten welke zich voordoen bij online banking systemen bij private banks en hoe reputatieschade daaruit kan voortvloeien. De private banking sector kenmerkt zich door het leveren van financiële producten en diensten aan welvarende individuen. Juist vanwege dit feit zijn de marges in deze sector initieel hoog en is de competitie daardoor de laatste jaren flink toegenomen. De private banks hebben vooral last van de toegenomen concurrentie van de vier grote banken in Nederland. Vanwege deze toename en de karakteristieken van de private banking sector, geschiedt de concurrentie vooral op basis van de kwaliteit van de geleverde producten en services. Om het hoofd boven water te houden investeren de pure private banks in het aantrekken van hoog opgeleid personeel, IT en fusies en overnames. Door de toegenomen kosten van al deze maatregelen zijn kostenbesparingen in de operationele processen aan de orde van de dag.

Omwille van het verlenen van extra service, bieden steeds meer private banks online banking systemen aan. Met deze systemen hebben klanten zelf een digitaal en actueel overzicht van de rekeningstanden en de laatst gemaakte transacties (level 2 systeem). Sommige systemen bieden zelfs de mogelijkheid om ook online transacties uit te voeren (level 3 systemen). Uit dit onderzoek kwam naar voren dat slechts weinig private banks een level 3 systeem hebben geïmplementeerd maar bijna allemaal een level 2 systeem aanbieden. Uit de interviews blijkt dat een achterstand op level 3 banken zou kunnen leiden tot een competitief nadeel.

Bij online private banking gaat het vaak om veel geld en een groot deel van de services zijn niet meer fysiek maar via het publiek toegankelijke Internet toegankelijk. Daarom is een online banking systeem gevoelig voor aanvallen via het Internet. Om deze aanvallen tegen te gaan moet een private bank voldoende maatregelen nemen om de vertrouwelijkheid (ongeautoriseerde personen mogen geen inzage hebben in geheime informatie), de integriteit (de informatie in het systeem moet volledig en juist zijn) en de beschikbaarheid (het systeem moet beschikbaar zijn en een goede reactiesnelheid hebben) van het online banking systeem veilig te stellen. Klanten stellen bepaalde eisen aan deze aspecten. Wanneer de private bank door een beveiligingsincident niet in staat is aan deze eisen te voldoen kan reputatieschade het gevolg zijn. Daarbij is het zelfs mogelijk dat de klant besluit elders te gaan bankieren.

In de literatuur over IT-beveiliging zijn weinig methoden te vinden die ingaan op de relatie tussen beveiligingsincidenten en reputatieschade. Daarnaast zijn de methoden die ingaan op het meten van schade veroorzaakt door beveiligingsincidenten niet toereikend om reputatieschade te kunnen kwantificeren. In dit onderzoek wordt getracht fuzzy logic in te zetten als modelleertechniek. Fuzzy logic tracht, om door middel van gecumuleerde expertkennis, relaties te beschrijven en te modelleren. De grote kracht van fuzzy logic is dat het in staat is om relaties te modelleren welke door experts alleen in vage termen kunnen worden beschreven. Dit doet men door de experts in linguïstische termen (woorden) de relaties tussen variabelen in het model uit te laten leggen en op de achtergrond te vertalen naar meetbare eenheden.

Om een fuzzy model op te kunnen stellen is een literatuurstudie uitgevoerd en zijn er interviews met experts gehouden. Grofweg waren hierbij twee fases te onderscheiden. Eerst werd aan de hand van een literatuurstudie een conceptueel model opgesteld over

hoe de relatie tussen beveiligingsincidenten en reputatieschade eruit ziet. Vervolgens was het de bedoeling dat met behulp van experts het fuzzy model in te vullen. Met behulp van het resulterende model zouden IT-security managers de reputatieschade kunnen bepalen die voortkomt uit potentiële of voorkomende incidenten. De volgende stap zou dan zijn om met behulp van beveiligingsmaatregelen de reputatieschade aantoonbaar terug te dringen. Wanneer het lukt om tot een dergelijk model te komen kunnen managers bepalen wat de opbrengsten van investeringen in IT-security maatregelen zijn en deze daardoor beter verantwoorden.

De eerste fase van het onderzoek waarin het conceptueel model gevormd werd is succesvol verlopen. Het resultaat was een voorgesteld fuzzy model met daarin de indicatoren voor reputatieschade en een beschrijving van de onderlinge relaties tussen de indicatoren en reputatieschade. In het kort komt het erop neer dat de incidenten welke zich kunnen voordoen in te delen zijn aan de hand van de kwaliteitsaspecten van beveiliging, te weten vertrouwelijkheid, integriteit en beschikbaarheid. Vervolgens heeft de onderzoeker bekeken wat de impact van dergelijke aanvallen op deze kwaliteitsaspecten zou kunnen zijn en gezocht naar indicatoren. Daarnaast kan reputatieschade uitgedrukt worden in het aantal klanten wat na een beveiligingsincident vertrekt. Analoog hieraan is het beheerd vermogen wat de private bank verliest doordat klanten weglopen bij de bank een goede indicator voor reputatieschade. Het conceptueel model is te zien in figuur 15. Het hieruit voorvloeiende voorgesteld fuzzy model is te zien in figuur 23.

De tweede fase van het onderzoek had als doel om aan de hand van interviews met experts bij Nederlandse private banks de voorgestelde relaties te valideren en het fuzzy model in te vullen. Deze fase verliep niet volgens plan omdat bleek dat de experts niet voldoende kennis hadden om het gedrag van hun klanten te beschrijven wanneer er zich beveiligingsincidenten voordoen. Daarom is besloten om het voorstelde fuzzy model in figuur 23 met behulp van interviews met experts te valideren en aan te passen. Er is getracht om het onderzoek een dusdanige wending te geven dat er aanbevelingen gegeven kunnen worden over hoe men alsnog een fuzzy model kan opstellen. Het uiteindelijke model is gebaseerd op het model in figuur 23 en de interviews met de experts en is te zien in figuur 24. Het succesvol invullen van dit model moet plaatsvinden aan de hand van een vervolgonderzoek waarbij gebruikers van online banking systemen bij private banks geïnterviewd worden om na te gaan wat de reactie op beveiligingsincidenten kan zijn.

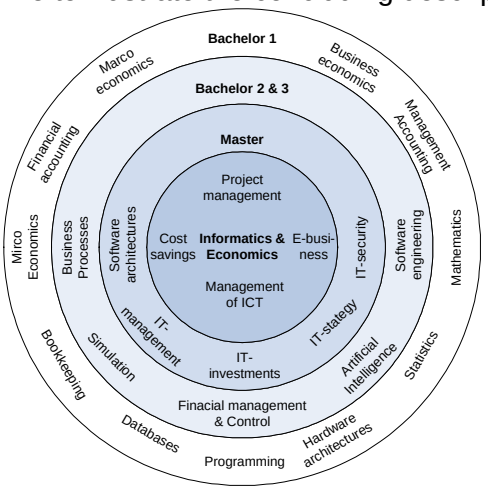
Naast het fuzzy model heeft dit onderzoek nog enkele andere resultaten. Zo bleken de experts allen tot op heden gebruik te maken van kwalitatieve argumenten om investeringen in IT-beveiligingsmaatregelen te verantwoorden en geven de experts aan dat zij geen heil zien in pure kwantitatieve methoden om investeringen te verantwoorden. De experts denken dat kwantitatieve methodes voor het bepalen van de opbrengst van investeringen in IT-beveiligingsmaatregelen de kwalitatieve argumenten niet kunnen vervangen maar wel kunnen aanvullen of versterken. De behoefte aan methoden welke de opbrengst van investeringen in IT-beveiligingsmaatregelen op basis van kwantitatieve methoden gecombineerd met kwalitatieve argumenten in kaart brengen, wordt op deze manier bevestigd.

Foreword

This master thesis is the product of the research I have conducted in the period between July 2005 and January 2006 in combination with an internship at the Security & Technology department of PricewaterhouseCoopers (PwC) in Utrecht. I have found it inspiring to work in a dynamic environment with a lot of professionals, all with different expertises. In addition, PwC is a company with a huge cumulative expertise, a lot of IT and with very good in place support services. Such an environment has stimulated my (by default) curiosity. In total, I have come to the conclusion that advising companies about IT-security issues is fun and a challenge. This is why I hope to start working at PwC Security & Technology starting next February.

Of course there were some obstacles when writing this thesis. First it was hard to become used to the rhythm of going to work every day. This was especially true when the train was overloaded with people and the public transport turned into a jungle. Social scientists who like to research the increased individualism or the origin of mankind's social behaviour are invited to travel by train on a daily basis between Rotterdam and Utrecht. Furthermore I like to thank the NS for all the delay of trains which made it possible to work a little longer on my thesis. In addition working for 6 months to find solutions to a single research problem has been a test to my patience. Also writing this thesis in English was not easy. By doing this research I have learned that the research question and the scope are the most important parts of a research.

Due to the fact that working with Visio has become a hobby while writing my thesis I would like to illustrate the concluding description of my study in the figure below.



While the study advances, the basics of Informatics and of Economics are integrated by looking how IT can have an influence on the economy and vice versa. In the end Informatics & Economics is the study of how IT can be used to enhance economics and in return which economic aspects must be taken into account regarding IT.

Finally I want to say some words of thanks. First I want to thank Jan van den Berg for the supervision of my thesis, the scientific feedback, the discussions, and the warm conversations about other important things in this world (despite of the little time he has). Next I like to thank Frans van Buul for being my guide at PwC, for the discussions and the feedback on my thesis. Furthermore I like to thank the following people at PwC: Tonne Mulder for providing me the contact information of the private banks, Otto Vermeulen for giving me the opportunity to see something of the world of business advising, Rogier van Adrichem for providing me insight in the private banking sector, Arco ten Klooster for the discussion about reputation loss and all my other colleagues at Security & Technology and students writing their thesis at PwC for the discussions and insights in other interesting topics. Other people I like to thank are: the experts which I have interviewed, Gert van der Pijl for the discussion about the CIA aspects, Ferry Wolff for eating a pizza with me while discussing the IT-security issues at online banking systems, my parents and my girlfriend Marieke for reading my (probable tedious) thesis and giving feedback and James C. Bastick for revising my bad English (I do not know anybody else who can transform stiff feedback into laughable e-mails).

Table of contents

List of figures

Chapter 1: Introduction

In this introductory chapter, first the background of the research subject is described. After this the research problem is explained, followed by the research questions that must be answered to solve the research problem. Also the research scope, the research design and the thesis outline are described in order to guide the reader through the research and the thesis.

1.1 General background

In the last 15 years Information Technology (IT) has become an indispensable production factor for a lot of companies. Because of the rapid development of IT which causes lower IT costs, IT has become a commodity (Carr 2003). Therefore many companies have invested massively in IT resources in the last 5 years (CBS 1997). Due to all this, IT investment decisions are rationalized. Furthermore a lot of companies have integrated the use of the Internet and IT in their business processes. For instance at banks almost all financial transactions are processed with the help of IT and network connections. When many clients of banks installed an Internet connection, the first online banking systems evolved. As the Internet is publicly accessible and by default has no security measures built in, there is considerable big focus on the IT-security of online banking systems. A problem then is that in practice, banks try to have a minimal level of security alleviating most of the risks, with a maximum level of convenience (Claessens et al. 2002). In this way also the security of this IT has become a business need. In addition, IT-security is more and more rationalised and handled similar to other business investments. Therefore cost-revenue analyses are made for IT-security measures. The fact that managers have a need for a method to assess the return on security investments which take the indirect costs/benefits into account is also stated by Zeki Yazar (2002):
"In the present competitive environment however, most managers tend not to rely on some general statistics or projections, when it comes to invest in information security measures which may reduce IT performance or employee productivity, while not providing any tangible benefits. While these organisations may suffer serious losses due to security breaches, others may not be sure whether they over-protect their assets by supporting security initiatives, which may also result in the loss of competitive advantage."

An interesting finding in the above citation is that managers are asking themselves not only if they have enough IT-security in place but also if they have too much. Therefore it is important that investments in IT-security measures can be allocated with the help of tools which can determine the return on security investments. Chapin and Akridge (2005)state that managers have the need for security metrics in order to answer the following IT-security management questions:

- How many resources does it take to be "safe"?
- How can the cost of new security measures be justified?
- Is the organisation getting its money's worth?
- How does the organisation compare its posture with others in the industry and with best practices standards?

The origin of this thesis lies at a seminar the researcher followed earlier this year in which the ROSI (Return on Security Investment) problem was analyzed. The underlying thought of a ROSI calculation is that if it is possible to calculate what the damage (a summation of the direct and the indirect costs of IT-security incidents) of a certain IT-security incident is before and after the implementation of IT-security measures the difference between these two moments can be calculated. In this way it can be determined how much money certain IT-security measures can save. When it is known how much money the

implemented IT-security measures save and also the costs of these measures are known the Return on Security Investment can be calculated as follows (Schechter 2004):

$$ROSI = \frac{BENEFITS\ FROM\ SAFEGUARDS}{COST\ OF\ SAFEGUARDS}$$
$$= \frac{SAVINGS\ FROM\ SAFEGUARDS}{COST\ OF\ SAFEGUARDS}$$
$$= \frac{ALE_{without\ safeguards} - ALE_{with\ safeguards}}{COST\ OF\ SAFEGUARDS}$$

In the above described formula, the savings from IT-security measures are calculated by subtracting the Annual Loss Expectancy (ALE) (the damage of IT-security incidents expected for the following year) after the IT-security measures were implemented from the ALE before these measures were implemented. By dividing these benefits of the security safeguards by the costs of it a ROSI ratio is obtained. Investments in IT-security measures are efficient if the ratio is larger than 1. The problem with the ROSI method described above is to determine a good estimation of the losses caused by occurring IT-security incidentsthe exact costs of IT-security incidents. Novell conducted a research in which Dutch managers were asked about their company's IT-security strategy. Of the 109 respondents that participated with this research, 74 percent thinks the question what revenues investments in IT-security have, can not be answered with the help of a ROI calculation. The research also states the fact that not only the direct revenue of IT-security investments is difficult to measure but also the indirect revenues are staying out of scope while they are definitely present (Erwin 2002; Novell and IT Topmanagement 2002).

When looking at the costs security incidents cause, two types of costs can be defined: direct and indirect costs. Direct costs of IT-security incidents are physical damage to the IT-systems, the costs of repairing the IT-systems and cancelling appointments and deliveries. Direct costs are costs which can be expressed in monetary terms. Indirect costs are costs which are not directly linked with the IT-security incident occurred and can not easily be expressed in monetary terms. Examples of indirect costs are the disruption of the business processes and the loss of consumer's confidence, company image or reputation (Basten and Wijnmaalen 2003; Chan 2001; OCC 1998; Overbeeke et al. 2003; Shaw 2005).

In the literature, an often mentioned indirect cost of IT-security incidents is reputation loss (ISF 2005a; ISF 2005b; Mrdovic 2004; Mukherjee and Nath 2003; www.security.nl 22-06-2005). Also, financial institutes are well aware of the risk of reputation loss. In a survey conducted by PricewaterhouseCoopers (2004) in which executive of 134 institutes out of the US, Europe and Asia 34 percent thought reputation loss was a top risk for the market value of their institute. Moreover, 22 percent thought reputation loss was a top risk to the earning of their institute. Risk of reputation loss is seen as the top risk for institutes in the financial services industry. Furthermore only 16 percent of the respondents indicate they quantify intangible risks. This is a direct support of the observation that the indirect costs are staying out of scope. The report also states the following:
"Senior executives of financial institutes may appreciate the dangers of reputational risk to market value. But many are fuzzy about how to manage this and other less visible forms of risk"

Private banks provide financial services to rich clients. Rich clients also have the need for online banking systems and because of the fact the competitive advantage of private banks exist of service; a lot of private banks have built online banking systems in the last couple of years. Because private banking involves a lot of money, a relation of trust must be present between the private bank and the client. In addition this relation often goes back several generations. A user of an online banking system trust that the private bank will ensure that its money is safe (Mukherjee and Nath 2003), in the case of a security incident this relation of trust is compromised. In effect, this can cause damage to the reputation of the stricken bank. Such an indirect cost of an IT-security incident could even be greater than the direct financial losses of such an incident (PricewaterhouseCoopers and Wilmer 2003). Because of the special relation between private banks and their clients, the chance of reputation loss due to security incidents is even more significant than at retail banks.

Summarising it is proposed there is a need from security officers and managers at private banks for methods to measure the reputation loss which could be the result of IT-security incidents in their online banking systems.

1.2 Problem description

After researching the available literature about measuring and modelling the relation between IT-security incidents and reputation loss it was concluded there is no model present about this relation. Next to this many researchers discovered the fact that the indirect costs (such as reputation loss) are not easy to measure and therefore are out of scope in almost every research about ROSI (ISF 2005b). Calculating the indirect costs of IT-security incidents is hard because of the fact subjectivity plays a large roll in this (Anderson 2001). Where someone thinks there may be a significant risk of a certain IT-security incident, another person can think that this same risk is negligible. Also the discipline of measuring costs of IT-security incidents is in an early stage (Payne 2001). Despite these facts some researchers have developed methods to calculate the indirect costs of IT-security incidents (Butler and Fischbeck 2002; Garg et al. 2003a; Moulton and Moulton 1996). The problem that arises with these methods is that they are often theoretical. The costs of IT-security incidents are composed of surveys that are filled in by companies. These costs are specified differently at each company and they often are compared, which is scientifically not correct for the reason that the way in which the figures are composed is the basis for the results at the end. Therefore these attempts have little success mostly; the indicators which are chosen are a shot in the dark. Andrew Stewart (2004) states this problem as follows:
"Attempts to model attacker's actions in an abstract, mathematical way and then to attempt to predict the future actions of attackers based on those models is a problem that is non-trivial and is currently unsolved."

Aside from the scientific problem, there is not enough reliable historical information about the costs of IT-security incidents available at Dutch companies. The reason for this is that a lot of incidents are not reported because the company is afraid to gain reputation loss (Stewart 2004). Furthermore, it is possible victims of the attack will claim compensation for the damage the incident has caused (het Financieele Dagblad 16 June 2003). The little information which is available about IT-security incidents and the costs of these incidents is not suitable to determine the indirect costs of IT-security incidents.

Another problem is the fact that the methods which are used to calculate the costs of IT-security incidents are mostly based on the probability of such an incident. The methods use the probability of a certain IT-security incident and multiply this with the financial impact a certain incident could have. In this way an expected value is calculated. In this

way if there is not a lot of data available of incidents in the past, some incidents could be pointed with a little probability of occurrence. These incidents then are overlooked while if they would occur could have a disastrous impact.

In conclusion, there is a need for a model to describe and measure the relation between IT-security incidents and reputation loss and at the same time solve the problems mentioned above. When the cause and effect relation is described and quantified the factors which determine the indirect costs can be managed to alter these costs. As described in paragraph 1.1 the online banking process at private banks is very vulnerable for IT-security incidents and the reputation loss which could be the result. This research tries to construct a method for measuring the reputation loss in a semi-quantitative way.

1.3 Research question

The research questions to be answered in this thesis are:
"Which IT-security incidents in online banking processes at private banks can lead to the loss of reputation, and which IT-security measures must be taken to manage this reputation loss?"

The research done to answer the above research question can be divided into three parts. The first part of the research concentrates on exploring the environment of the research object, i.e. online banking systems at private banks. Therefore the following questions must be answered:

1. What are relevant developments in the private banking sector with regard to the security of online banking systems?
2. What do the online banking systems look like at private banks?
3. Which IT-security incidents could occur to online banking systems at private banks?

The second part of the research concentrates on the modelling of the relation between IT-security incidents and reputation loss. With the help of literature and expert knowledge the following questions must be answered:

4. Which IT-security incidents lead to which degree of reputation loss?
5. In which way can the relation between IT-security incidents and reputation loss be modelled to enable the development of an IT-security management dashboard in order to balance the costs and benefits of IT-security measures?

1.4 Research scope

The scope of this thesis lies at the exploration of reputation loss caused by IT-security incidents in the online banking process at private banks. When looking at the indirect costs of security incidents people can think of reputation loss, loss of brand image and loss of confidence of clients, suppliers or supervisors. This research concentrates on reputation loss because this type of indirect costs is potentially the most substantial for private banks.

When looking at the stakeholders of a private bank, the following groups can be defined:

1. Current clients of the private bank.
2. Potential clients of the private bank.
3. Suppliers of the private bank. Private banks buy products and services from larger and specialised banks.
4. Shareholders.
5. Employees of the private bank.

Current clients have the most fragile relation of trust with the private bank. It is presumed that it is more likely that current clients will leave their private bank than the impact security incidents have on other stakeholders, such as potential clients not becoming a client. Therefore this thesis only looks at how reputation loss could arise in the perception of the current clients of the private bank. Other consequences of a security incident could be: suppliers who will not deliver anymore, shareholders that start legal action or employees will leave the bank.

This research will concentrate on independent medium-sized private banks. The reason for this is the fact the retail banks in the Netherlands do not offer that much private banking services and are using already-installed online banking systems for new online banking services. Moreover, the online banking systems at these big players are very complex and a lot of legacy systems are still up and running. Also, small wealth management companies are out of the scope. Their focus is mostly on personalised wealth management services and they therefore do not have banking licences and seldom offer online banking services. Furthermore, the research scope is narrowed down to private banks which are using a level 2 or 3 online banking system.

Within the online banking process the scope narrows down to the front-end of the online banking process. For a description of the front-end and back-end of the system see paragraph 3.2. In short, only the systems which are involved with the online banking process are included in the scope. All systems the private bank use internally to do their daily business are out of the scope. These processes and systems are out of scope because of the complexity these would add to this thesis.

When looking at the different sources of attacks to online banking systems only external attacks in the provided scope are interesting. The main source of risk for online banking systems is the fact the system is accessible via the public Internet. External attacks are in this way only possible via the front-end, which can in this way also provide access to the back end systems.

1.5 Research design

In the preparation phase of this research no literature was found which describes the relation between IT-security incidents and reputation loss. In some literature the relation is mentioned, but not described. The relation is proposed but never described and therefore an explorative research will be performed. This research consists of two steps. The first step is to describe the relation between IT-security incidents and reputation loss in qualitative terms. The goal then is to create a conceptual model of the relation. This is done with the help of a study of the available literature in three domains:

1. The private banking sector. Before describing the research object and subject the environment of the research object (online banking systems) is described. A literature study is carried out to describe the recent developments in the private banking sector.
2. The security of online banking systems at private banks. After the environment of the research object, first the object itself is described. A literature study is conducted to describe the aspects and properties of online banking systems. Second a literature study will be done to describe the IT-security requirements set by different stakeholders of online banking systems. Furthermore, possible IT-security incidents and how these incidents could be prevented to occur are explored.
3. Reputation loss at private banks. A literature study will be conducted to explore the factors which have influence on reputation loss.

After this the proposed relation between IT-security incidents and reputation loss which can be concluded from the literature is described in a conceptual model.

The second step consists of trying to confirm the proposed relation and quantifying the relations in this model. Due to the absence of data about IT-security incidents and the problems encountered when using other methods found in the literature, this research concentrates on modelling the relation between IT-security incidents and reputation loss with the help of expert knowledge. In the domain of the artificial intelligence a method called fuzzy logic is suitable to translate fuzzy linguistic terms given by experts into quantified indicators in the background. Fuzzy logic therefore is proposed as a method to model and manage reputation loss.
As can be concluded this thesis has the following goals:

1. To answer the research questions in order to explore and describe the relation between IT-security incidents and reputation loss.
2. To propose a fuzzy model in order to quantify the relation that will make the relation between IT-security incidents and reputation loss manageable.
3. To conduct interviews with experts to confirm the proposed model and fill in the indicators in both a qualitative and quantitative way.

After the first expert interview it came forward that it was not possible to quantify the relation between IT-security incidents and reputation loss with the help of fuzzy logic. Because fuzzy logic still is a solution to the problems found with other methods research goal 2 has changed to: “Finding the requirements needed in order to successfully construct a fuzzy logic model.” The research domains and the steps described above are graphically displayed in figure 1 below.

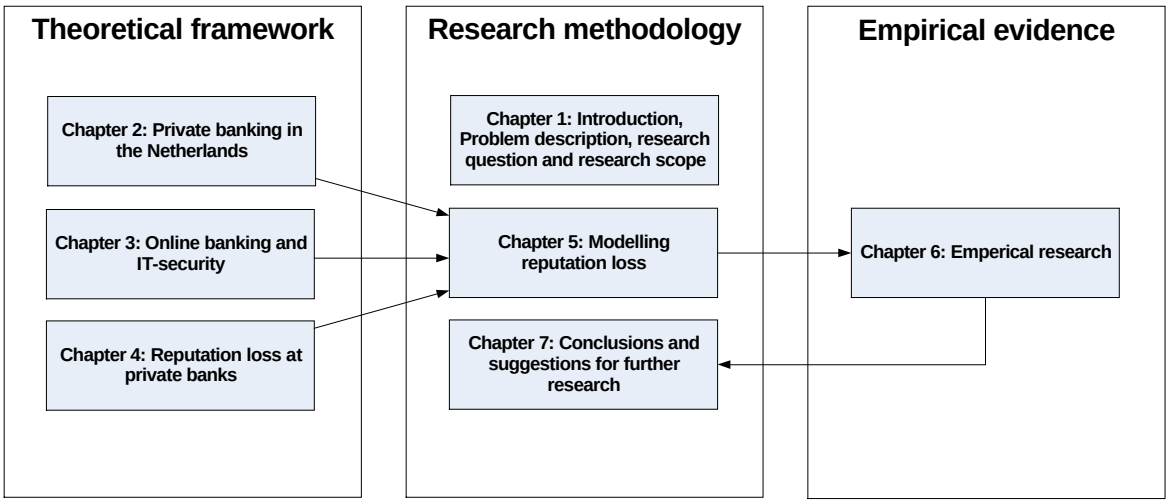


Figure 1: Graphical representation of the research design

1.6 Thesis outline

As described in figure 1 the outline of this master thesis can be divided into three domains. The first domain is the theoretical framework which consists of a literature study of the private banking sector in chapter 2, the security of online banking systems in chapter 3 and reputation loss at private banks in chapter 4. With the help of the literature and fuzzy logic a model can be built. The way in which this is done is described in chapter 5. In chapter 7 the results of the journey taken to meet the research goals are described. Together these three chapters form the research methodology domain. The third domain consists of the empirical evidence in the form of the empirical research which is described in chapter 6.

Chapter 2: Private banking in the Netherlands

2.1 Introduction

In this chapter the literature regarding the private banking market will be discussed. First the definition of private banking will be set out. After this the history of the private banking market in the Netherlands will be described followed by the market characteristics and a description of the market players present in the market. Finally the current affairs and trends in the private banking market will be explored.

In order to explore the private banking sector an explorative interview was held with Rogier van Adrichem, who is partner at PricewaterhouseCoopers and who has ample knowledge about private banking.

2.2 What is private banking?

Private banking can be considered as all financial services a certain bank offer to wealthy clients only. Fitch (2000) confirms this in the following definition of private banking:
"Private banking is providing banking services, including lending and investment management, for wealthy individuals."

Or as Lyn Bicker (1996) likes to state:
"In truth, private banking is any service the client wants it to be. Be it wealth management, money transmissions, portfolio management, the delivery of a yacht or walking the dog, private banking is the ultimate client-led business"

Private banking can thus be defined as all specialised banking (and sometimes beyond) services offered to wealthy individuals. In essence the client is king in the private banking sector. The private bank therefore has a roll of advisor and counsellor for their clients. Because of this nature of private banking there is a high level of trust in the relation between the private banks and their clients. Secrecy still is a usual service from private banks towards their clients.

2.3 History of the private banking market in the Netherlands

The origin of the Dutch private banking market can be found a couple of centuries ago. In the Dutch republic, traders required a bridge between trade and finance. Hence wealthy individuals turned to banks for wealth services such as fortune savings, raising loans or investing opportunities (Bicker 1996).

In the last 15 years the private banking market in the Netherlands was subject to a lot of changes. In the first part of the 1990s, there were good market conditions, stable price structures and high margins. The market conditions continued to improve until the year 2000, but the margins were stable and price structures were changing because of the fact that the entry barriers were smaller which, in turn attracted a lot of companies to enter the market. In the beginning of the new millennium, declining stock markets put pressure on the margins and in this way also on the profits of the private banks. Due to the fact that the competition was based on the quality of the delivered services the costs rose. From 2004 until now it has become important for private banks to investigate how they can improve profits and margins by focusing on value-creating factors (Steen 2004).

2.4 Market characteristics

The Dutch private banking sector consists of a potential market of almost a million of so-called wealthy individuals (available capital of €50.000 to €1 million) and about 72.000

very wealthy individuals (available capital of more then €1 million) (CBS 2005a; CBS 2005b).

Next to this, out of the quarterly publication of De Nederlandsche Bank (2002), it can be concluded that the capital (possessions minus debt) of the Dutch households has increased until an average of 800 percent of total usable family income. Dutch households have more capital than households in five of the seven countries in the G7[1]. Therefore it is not a surprise that international active private banks have their eye on the Dutch private banking market.

These factors show that the private banking market is becoming more and more attractive for private banks as well for the retail banks which are not overlooking the market potential and the margins which could be gained.

2.5 Market players

The private banking market in the Netherlands can be characterized as very fragmented. There are many market players. The market players which are present can be categorized into three groups (Steen 2004):

1. The big, mostly international active, private banks. These are retail banks which also offer private banking services or vice versa. These types of banks which are active in the Netherlands are ABN-AMRO, Rabobank, Fortis, ING bank, Merrill Lynch. These kinds of banks have their own infrastructure and it is important to stay in the picture internationally. A lot of these banks have taken over smaller pure private banking companies to boost up the quality of the offered private banking services. Often, the acquired private banks still operate under their own label.
2. Midsize private banks. Examples of banks in this category are Van Lanschot, Kempen & Co., MeesPierson and Insinger de Beaufort. Mostly these are independent purely private banks. These banks are also taking over small private banks or specific teams to enhance their quality of service.
3. Exclusive private banks. These are little players which focus on niches in the market. These banks stand for personal services and will therefore not offer innovative services like online banking. Mostly old money concentrates at these banks. Ten Cate is an example of such a bank. Independent wealth managers are a part of this group of private banks as well.

2.6 Current trends in the private banking sector

In the current Dutch private banking market, four driving factors can be distinguished:

1. Increasing client power
2. Increasing competition
3. Innovation
4. Increasing regulation and the need for compliance

2.6.1 Increasing client power

Wealthy clients demand high standards of services and the quality of services offered is therefore mostly more important than the costs. Private banking clients demand quality of service, good accessibility, safety and comfort (Bicker 1996). In the retail banking sector, online banking systems were initiatives of the banks because of the economies of scale this would provide. In contrast to this in the private banking market the clients want at

[1] The G7 consists of the following countries: the United Kingdom, France, Germany, Italy, the United States of America, Canada and Japan. In 1998 Russia became a member and the G8 was born.

least the same services as clients from retail banks. It is clear that where online banking at retail banks is a supply side initiative, online banking at private banks is a client driven demand (Karjaluoto et al. 2002). Clients are switching from private bank because of bad banking experiences at their bank and not because of the fact another private bank has a little more service or against a slightly better price (Bicker 1996).

There is an opportunity for private banks to counter this trend. While clients got more bargaining power due to the fact it became easier to change banks at a mouse-click, switching banks is still uncommon due to other factors such as perceived personal workload associated with changing (Karjaluoto et al. 2002). To exploit this finding private banks could build in switching costs themselves by offering clients extras which they will lose when switching banks (Steen 2004).

2.6.2 Increasing competition

In the private banking market the competition is increasing due to the following developments:

1. The bargaining power of clients is increasing as explained in paragraph 2.6.1.
2. A lot of capital is coming free in the next few years. The baby boom generation is aging and near to their pensions. In this way more potential clients will come in the picture in the next few years. Rogier van Adrichem said about this:
   > *"A lot of capital of people which have an age between 50 and 60 is now locked in their houses and companies. This capital will become free in the next few years"*
3. New entrants. Because of the fact the private banking market seems to be very lucrative because of the increasing market potential and the fact margins are high in this sector, a lot of companies are attracted to get a part of this. First there are the big international private banks which are entering the Dutch private banking market to get a part of this and to establish their name in the Netherlands. These big private banks have a lot of clients which are internationally oriented and therefore it is important for them to be present in a lot of countries. A good example is Merrill Lynch which opened a bank site in the Netherlands (het Financieele Dagblad 4 July 1997). Secondly there are the main stream banks which want to be a part of the growing market. These banks are focussing on private banking services for everyone with a year income above 80.000 euro (het Financieele Dagblad 18 June 2005) or as Jan van der Steen (2004) says:
   > *"Private banking companies in the Netherlands try to focus on the subgroups of wealthy and very wealthy individuals, but due to a more competitive market and tougher circumstances there is a trend of downgrading the amount of minimum investable money before offering special treatment to clients"*

   Lastly there are the wealth management companies which try to differentiate with special and personal products and services. These companies do not always need a banking licence but must have a wealth management licence and are under supervision.

Costs cutting

Due to increased competition (mostly based on the quality of delivered service), the profitability and the margins are decreasing (Beek and Schut 2002; Karjaluoto et al. 2002). That is why private banks must concentrate on winning new clients and retaining the existing clients (PricewaterhouseCoopers 2005a). Because of the decreasing margins, economies of scale become more and more important. In light of this the trend of mergers and acquisitions in the last few years in the financial sector can be explained (Munck et al. 2001). Also the costs of offering products and services are rising because of the expertise

which is needed. Cost cutting programs are therefore no exception in the private banking market in the Netherlands (Steen 2004).

Entry barriers

To exclude new entrants of the market entry barriers can be used. These are factors which cause potential new entrants not to enter the market. In the private banking market in the Netherlands the following entry barriers exist (Steen 2004):

- Level of service. When all current players have a high standard of offered services which is built in many years time, a new entrant cannot offer the same level of service as it enters the market.
- High capital requirements. New entrants must invest a lot in human capital and IT to offer a competitive range of products and services.
- Reputation. As described earlier reputation is an important asset for private banks. Settled market players have years of experience in building this reputation. New entrants must first build a reputation of a trustworthy private bank and this is therefore a major entry barrier.
- Regulation. Private banks must comply with a lot of regulation such as the ROB standards to obtain a banking licence. Two other important regulations to which a private bank could be obligated to comply are the Basel II standard and if the private bank is present on the US stock exchange also the Sarbanes-Oxley act. To be compliant with these regulations asks for a lot of investments and effort and therefore this is also a major entry barrier for new entrants.

Because of these entry barriers it is almost impossible for new players to enter the market. Most new entrants therefore are banks which are changing their focus such as retail banks and merchant banks.

Differentiation of products and services

For a private bank in the Netherlands it is, as noticed before, very important to acquire new clients and to preserve current clients. In combination with the fact clients are increasingly demanding state-of-the-art products and services it is for this reason why differentiation is crucial for a private bank to compete with other players on the market. This can be done by good relationship management performed by the private bank. Moreover, IT can be used as a new distribution channel. An online banking system for instance, can influence the perception of the service mix (number of contact moments, level of service and the number of distribution channels) offered by the private bank in a positive way (Steen 2004). Therefore it is important for private banks to invest in the right projects such as recruiting, training and development of skilled employees and state-of-the-art IT (Bicker 1996; PricewaterhouseCoopers 2005c).

A development with regard to the education and training offered by private banks to their employees is the fact that Relationship management has become more and more important in a highly competitive market. Rogier van Adrichem thinks that the focus in the training budget must shift more to the training of soft skills. Furthermore he says that employees at private banks often have a lack of knowledge of international tax regulations. This is unfortunate because clients of private banks are often financially active in several countries. Private banks can also buy skilled teams from other private banks to enhance the quality of their human resources.

Another trend in the products and services offered by private banks is the use of a so-called open architecture. An open architecture means that a private bank no longer only offers products such as funds which are developed by their own but they now offer just the most attractive products for their clients, even if this means these products are from a competing private bank.

Rogier van Adrichem said about this:
"Only the small private banks are using the open architecture mechanism. The big retail banks, which offer also private banking services, obtain more revenue out of their own products and therefore offer only a few products developed by external parties"
As can be concluded out of this statement the open architecture initiative is currently more myth than reality (PricewaterhouseCoopers 2005a).

2.6.3 Innovation & IT

Clients demand more real-time information and transparency of the state of their assets and the costs of the products and services the private banks offer. Aside from that the employees of a private bank need IT tools to analyse the assets of clients and the market. In this way the bank can develop better services (Steen 2004). In addition online banking is a client-driven initiative. It is not an extra service in which a private bank can differentiate itself. Therefore it is not a competitive advantage but becomes a competitive disadvantage when overlooked. The private bank that can offer a good price/quality service ratio and has a high level of transparency at the same time will gain the respect of the new generation of clients (Steen 2004).

The investment power of the smaller private banks is not very big and therefore the budget which is available for IT must be filled in as efficient as possible. Therefore a lot of smaller private banks outsource their IT systems to third parties. In this way they have bigger budgets available to develop new online services. A problem then to overcome is the new dependence with the service provider. Making good service level agreements is therefore very important.

2.6.4 Increased regulation and supervision

Because of the increasing demands on the stability of companies and the cooperate governance which is needed to accomplish that, more regulation was made in the last couple of years. In the Netherlands there are several institutes which regulate the financial sector in general. In general there are three institutes which are important to this subject:

1. De Nederlandsche Bank (DNB). The DNB has the goal of creating stability for financial institutes, financial transactions, and prices in the Netherlands. To accomplish this, the DNB has set up the "Wet toezicht kredietwezen" (supervision of credit institutes act) which describes to which requirements banks must comply in order to get a banking licence. This licence is needed in order for banks to supply credit loans to their clients.
2. The Bank for International Settlements (BIS) is an international organisation which fosters international monetary and financial cooperation and serves as a bank for central banks. Within the BIS the Basel Committee was established. This committee exists of members from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States. The committee formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them through detailed arrangements which are best suited to their own national systems. The most important regulation set up by the Basel Committee is the Basel II standard. The Basel II capital accord is designed to create a higher level of transparency and more sound risk management practices and techniques for financial organisations (Lötgerink 2004). The accord describes how to assess the operational risk which a financial institute could encounter and how much capital there must be reserved to cope with these risks when they occur. The Basel II accord will be obligatory worldwide by 2008 (Vrede 2005). Banks which implement the advised measures to

prevent operational loss can save money because in that case lower capital requirements are needed.

3. The “Autoriteit Financiële Markten” (AFM), is a supervisor on the financial market in the Netherlands. For banks this supervisor ensures that banks which have a banking licence are compliant with the Wtk. (www.afm.nl)

As can be seen in the description of the regulations and supervisors in the private banking sector in the Netherlands, the need of being compliant with these rules is becoming more important. Regarding the IT-security of online banking systems banks must be compliant with certain best practice standards. Fore more information about these requirements see paragraph 3.3.3.

2.7 Conclusion

Summarizing this chapter, it can be said that the private banking market is lucrative to new entrants because of its capacity and initially high margins. Because of entry barriers present in the sector only banks or financial institutes which are formerly not present on the private banking market are able to overcome these barriers. In the Netherlands this can be seen through the fact that the four big retail banks are becoming active in the private banking market. An increasing competition in which private banks are trying to cut costs and provide differentiated products and service at the same time, is the result. In order to do this investments in IT and human resources is needed which causes increased costs. Another factor which increases the costs of private banks to do their business is the need to be compliant with increasing regulation requirements. Furthermore because of the increasing competition lower margins are the result.

Chapter 3: Online banking and IT-security

3.1 Introduction

In this chapter the need for IT-security in online banking systems is explained. To do this first the definition and the characteristics of online banking systems is explored. After this the IT-security requirements for online banking systems are described. When online banking systems do not meet these requirements incidents could happen. Also the different types of incidents which could occur in online banking systems are portrayed. Lastly the IT-security measures which could prevent incidents to occur are explored.

3.2 What is online banking?

Karjaluoto et. al. (2002) defines online banking as:
“Electronic banking comprises all electronic channels clients use to access their accounts and transfer funds or pay their bills, including telephone, the Internet, mobile phone (WAP, SMS, GPRS), and digital television.”

Another definition brought by the Office of Comptroller of the Currency (OCC) (1998):
"PC banking" refers to computer hardware, software, and telecommunication systems that enable retail clients to access both specific account and general bank information on bank products and services through a personal computer (PC)”.

In this thesis an online banking is defined as automated banking services provided with the help of the Internet. These services can commonly be accessed with the help of different kinds of multimedia devices, such as desktop PCs, laptops or even mobile devices such as smart phones and PDAs.

3.3 The functionality of online banking systems

Online banking systems can be divided with the help of the functionality provided. Generally three levels of online services offered can be distinguished (Huyveneers 2001,; Mishra and Lucknow 2005; Pennathur 2001; Spivey 2001):

- Level 1. This level is sometimes also called the information stage. At this level the bank is only present on the Internet with an internet page. On this page general information about the products and services which are offered by the bank is present. The online banking system in this phase consists of a stand alone web server which is not connected with the bank’s internal systems.
- Level 2. This level is sometimes also called the communication stage. Banks that have a level 2 online banking system operational offer specific client tailored information. Clients can retrieve information about their account balance and the last transactions made. For this kind of online banking systems an authentication and authorisation procedure is needed to make sure only those users that are entitled can retrieve account information. At this level the web server which establishes connection with the user is coupled with the internal systems of the bank.
- Level 3.This level is sometimes also called the transaction phase. Banks with a level 3 online banking system offer full service banking products and services via the Internet. Clients can make transactions online and can retrieve real time information about their account balance and last-made transactions. In this stage also a connection between the web server and the internal systems of the bank is needed.

3.4 The architecture of online banking systems

An information system such as an online banking system can be defined as an information processing entity which consists of hardware, software, data, people and procedures (Overbeeke et al. 2003; Ridderbeekx and Berg 1998). In figure 2 below the components of an online banking system at private banks are described.

Componant in IS	Instance in online banking systems at private banks
Hardware	Personal computers, mobile devices (PDA, GSM), mainframes, servers networks, firewalls, IDS, workstations
Software	Applets, webapplications, operation systems, banking applications for internal use, other office software
Data	Account balance, transactions, userinformation, internal banking data
People	Employees and clients of private banks
Procedures	Information security policy, internal controls

Figure 2: The different components of an online banking system

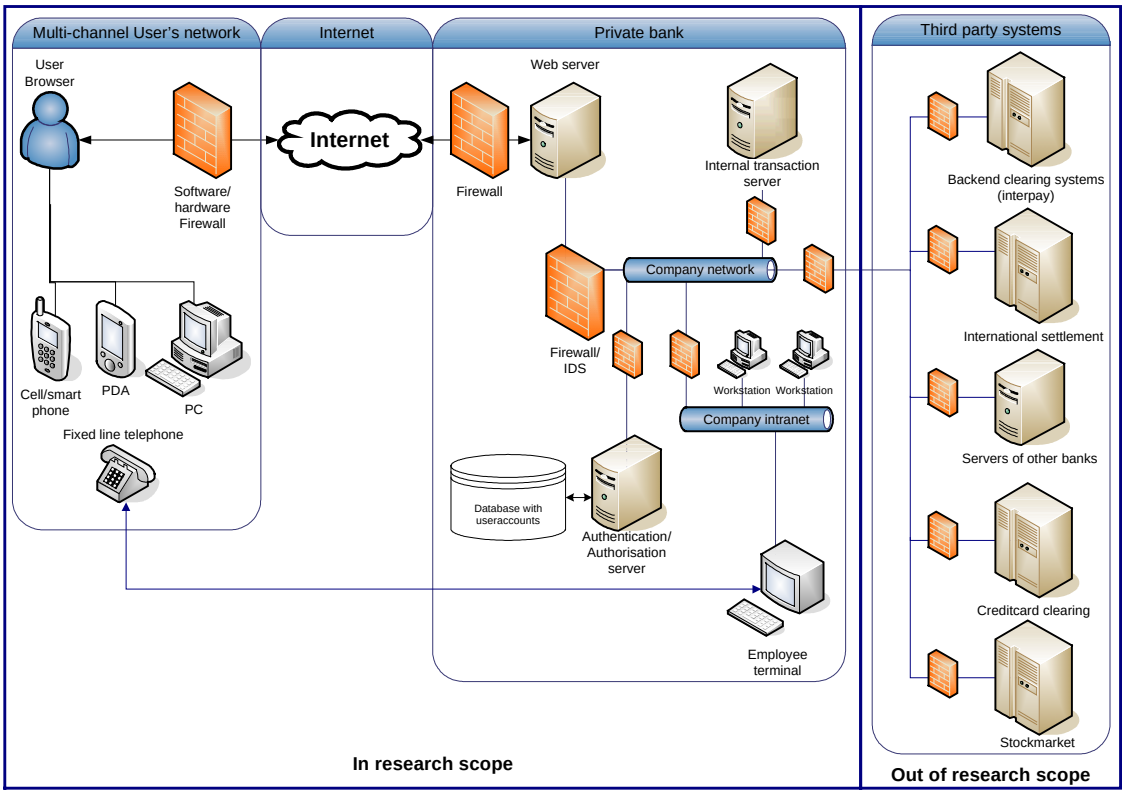


Figure 3: An example of the architecture of an online banking system.

In figure 3 an example of a typical system architecture of an online banking system is shown (Claessens et al. 2002). In such a typical implementation of an online banking system four different domains can be distinguished:

1. Client side systems and software
2. The Internet
3. Internal banking systems at the private bank
4. Coupled third party systems

3.4.1 Client side systems and software

The client side systems consist of all systems and networks the client uses to have access to the online banking system. The user connects with the online banking system with the help of a browser which can be integrated in several devices. Examples of these devices are a smart phone, PDA or just a personal computer. Furthermore because of the fact direct services will be offered it is also possible to just call an account manager to give orders for transactions. In this case the order will not go via the Internet. Users, who are aware of the dangers of a public Internet, will typically use a firewall to protect their connection devices.

3.4.2 The Internet

The Internet has a communicative function in the online banking system. Via the Internet the system of the user (PC, PDA or mobile phone) can be connected with the systems of the private bank.

The Internet is based upon standardized protocols. With the help of TCP/IP (Transmission Control Protocol/ Internet Protocol) blocks of data are send to computers which have an IP address. For instance the files of which a webpage consists can are divided into blocks of data which all have a header in which the destination of the data is recorded. The blocks can travel separately on the Internet. Web pages on web sites on the Internet are constructed with the help of the HyperText Markup Language (HTML). HTML describes the mark up of a web page with the help of tags. These tags are translated by the web browser in to marked up text. For example this text is bold will result in "**this text is bold**" in the web browser (Santos 2000). With the help of HTTP (HyperText Transfer Protocol), which is a request/response protocol between clients and servers, a request to the web server for receiving a webpage is made by the web browser. The web server responds with an acknowledgement message after which the requested data is send to the web browser with the help of TCP/IP.

Often online banking systems are implemented as applet based or HTML based client-server systems (Wiesmaier et al. 2005). When a bank makes use of an applet (often written in the programming language Java) the online banking application is wrapped into a stand alone program distributed via the Internet and the execution by the Internet browser. Such an applet is more flexible in the sense that a programmer can make proprietary connection settings and functionality. The working of such an applet based online banking interface is displayed in figure 4 below.

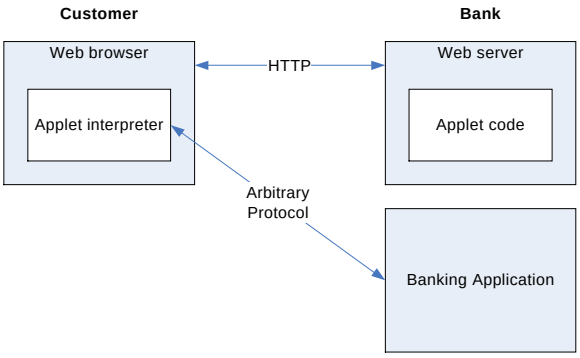


Figure 4: The working of an applet based online banking system (Wiesmaier et al. 2005)

The web browser on the users system sends a request for connection with the online banking system to the web server. The web server replies to the request and sends the applet (a separate program) to the users system. The applet is executed by an add-on engine integrated in the web browser.

An HTML based online banking system uses HTTP for the communication between the user's web browser and the private banking systems as can be seen in figure 5.

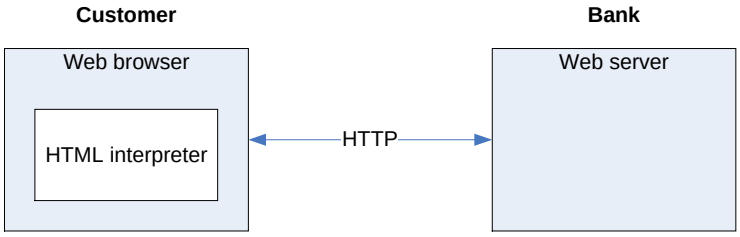


Figure 5: The working of a HTML based online banking system (Wiesmaier et al. 2005)

In such an online banking system the web browser sends request to the web server at the private bank. In response the web server sends the requested HTML pages to the web browser. The web browser has an HTML interpreter in order to translate HTML into a graphical representation of the webpage. When account information is needed the web server will send requests for this information to the private bank's internal information systems.

3.4.3 Internal banking systems at the private bank

The internal systems of the online banking system at the private bank consist of the following components:

- The authentication/authorisation server. This server provides authentication and authentication information with the help of a database with user information. Login names, passwords, user rights and other user information such as client name, address and other contact information is stored in this database. If the web server requests the authentication (is the user really the one it is pretending to be) of a certain user the authentication server looks up the given login name and password (these will be typically filled-in forms at the login page) and looks if the username really exists and if the correct password is provided. Furthermore this server can also be used to look up the user rights (which pages the user is authorized to see, which information the user is authorized to changed etc.) of a certain user. Depending of the user rights of a certain user the web server will make a custom representation of the online banking web pages.

- The internal transaction servers can process all internal financial transactions, for example transactions between banking accounts which are all present at the own private bank. This transaction server will typically also handle the authorization of these financial transactions. This means the user who initiates the handled transaction is really authorized to perform this transaction (is the account balance of the user sufficient to perform the transaction, is the user authorized to perform the transaction which involves a certain amount of money etc.). The internal transaction server can ask the authentication/authorisation server for this information.
- An employee terminal is required to give employees of the private bank the possibility to enter orders for transactions which clients have placed with the help of other channels than the Internet (for example with the use of a telephone call to the account manager a private banking client can ask for a certain transaction) into the internal banking system for processing.
- A firewall or Intrusion Detection System (IDS) has the task to protect the internal information systems against IT-security incidents performed by persons with malicious intentions. The firewall in this context has the task to protect information systems against unauthorized access and other forms of attacks. An IDS is a system which has the task to detect suspicious behaviour in the network traffic.
- The third party systems are the systems which process the clearing and settlement between the internal systems and external systems of other banks which are needed to process the financial transactions.

The front-end is defined as the part in which the communications and transactions between the user and the private bank occurs. In the online banking system architecture displayed above this could be regarded as the user's systems, the Internet, the web server and the systems which are in place to make the connection possible, such as the authentication server. All systems in which the private bank is processing transactions and account information and in which account data is stored can be referred as the backend of the online banking system (Mol 2002).

3.5 The IT-security of online banking systems

IT-security is all about protecting IT-assets against certain threats. Each threat can be described with the help of a corresponding risk. The relation between risk, threats, incidents and damage which could be the result of incidents, is graphically described in figure 6 (Oscarson 2003a).

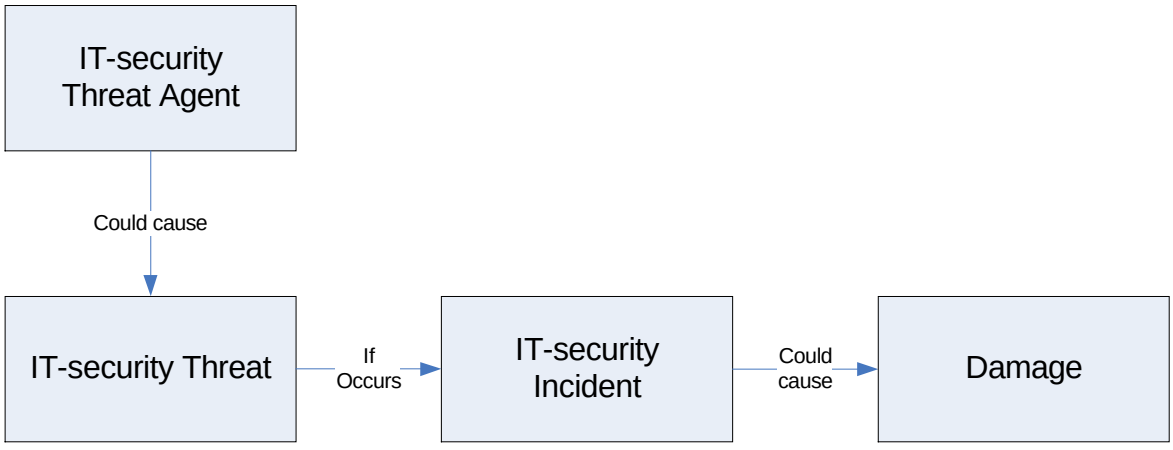


Figure 6: Graphical representation about the relation between threats, incidents and damage

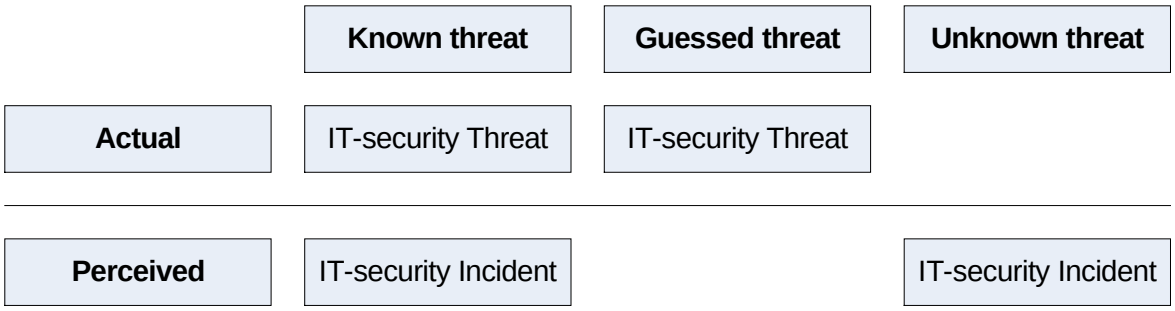


Figure 7: Different types of threat

Figure 6 represents the relation between threats, incidents and damage. Each security threat has a threat agent. This is an identity which could cause the IT-security threat such as an attacker, the user or even the employees of the online banking system. When a threat becomes reality an incident has occurred. Such an incident can cause damage to the online banking system. Oscarson (2003a) also defines different kinds of threats as can be seen in figure 7. If a certain threat has occurred before it is called a known threat. In contrast when there is no evidence of a proposed threat becoming an incident in the past it is called a guessed threat. If a certain threat has become an incident in the past but it is not acknowledged as a threat this can be called an unknown threat.

IT-security measures can have two different goals:
- Preventing a threat of becoming an incident.
- If an IT-security incident occurs despite of the in place preventive measures, other IT-security measures must minimize the damage caused by these incidents.

In this way IT-security measures guarantee the reliability of the online banking system. Overbeeke et al (2003) then defines the different aspects of the reliability of the delivery of information, which are described in figure 8.

Aspect	Characteristics	Threat	Examples of IT-security incidents
Confidentiality	Exclusivity	Disclosure	Espionage, tapping, hacking
		Abuse	Private use of resources
Integrity	Correctness	Change	Unauthorized changes in data, virus attacks
	Completeness	Deletion	Unauthorized deletion of data
		Addition	Unauthorized addition of data
	Validity	Ageing	Data is not up to date
	Authenticity	Falsification	Fraudulent transactions
	Non-repudiation	Repudiation	Denial of certain action
Availability	Timely	Relay	Overloading of infrastructure
	Continuity	Failure	Defect in infrastructure

Figure 8: Table with a description of the quality aspects of IT-security (Overbeeke et al. 2003)

Generally the three quality aspects of IT-security are called the CIA-triad and can be described as (Biene-Hershey and Bongers 1997; Harris 2003; ISF 1997; Overbeeke et al. 2003):
Confidentiality: Is the extent to which the use (retrieving, adding, changing and deleting) of data and the functionality of the system is restricted to authorized users.
Integrity: Is the extent to which the data and functionality of the system is correct. For an online banking system to be integer the data and functionality of the system must be complete (all data and functionality which must be in place is in place), correct (the data

and functionality in the system must be present as inserted), valid (data and software is correctly updated), authentic (the data and functionality entered into the system is legitimately entered) and last but not least not reputable (users can not repudiate actions which are performed in the system).
Availability: Is the extent to which functionality of an information system (such as an online banking system) is available to the users of the systems when needed. Therefore the data and functionality must be available and timely. IT-security incidents that tamper with this aspect are mostly aimed to disturb the working of the hardware and the software of the system.

If the different components of IT-security as described in figure 8 are combined with the components of an online banking systems as defined in figure 2 IT-security is the tool to ensure (Ridderbeekx and Berg 1998):
1. The correct functioning and availability of hardware.
2. The confidentiality and integrity of the software and data.
3. A correctly implemented security policy (procedure) which users (people) will comply with.

3.5.1 Security requirements for online private banking

The most important stakeholders which have security requirements for online banking systems at private banks are the private banks, the clients of the private banks and the sector regulators.

The private banks are trying to prevent IT-security incidents by implementing IT-security measures. With regard to these measures the financial sector is often seen as a best practice group because of the following reasons (PricewaterhouseCoopers 2005b):

- Financial service institutes, such as private banks, have larger IT and IT-security budgets than companies in other sectors.
- Financial institutions are regarded to be more secure than the average company. This superiority can be attributed to more efficient spending, and spending on strategic planning, not technology.
- Financial services companies already use risk models, return on investment models and other strategic tools in other parts of the business and have begun to apply these same tools to information security.
- Regulation and supervision in the financial sector has tightened in the last few years. This was among other things initiated to protect the continuity of financial institutes after examples of bad practice such as at Bearings Bank. The idea behind this was that if such events would occur more often this would also damage the reputation of the financial sector. In the long run this could cause diminishing returns and profits for the sector as a whole. Therefore the financial institutes are willing to cooperate to be compliant with the in place regulation.

In general the motives of private banks to implement IT-security measures are protecting their company against threats and to be compliant with regulations. Because of this private banks are slightly more likely to use ROI methods and contribution to business objectives as justifications for security investments. Despite of this private banks are still far more likely to rely on legal and regulatory requirements to justify their investments (PricewaterhouseCoopers 2005b).

Clients who are using an online banking system of a private bank are aware of the IT-security issues of such a system. Also these clients will not use online banking systems when they think they are unsafe. In addition even a little media attention about an unsafe online banking system can damage the reputation of the owning bank (Sathye 1999). As can be seen in figure 9 (Aladwani 2001), according to managers the most important

challenges for online banking systems are the Internet security and clients' trust. Other top 10 challenges for online banking systems which private banks must overcome in order to meet the security requirements of clients, are assuring clients' information privacy, making clients more aware of security risks and assuring the continuity and speed of online services.

Challenge	Rating of IT managers	Rating of senior management	Overall rank
Internet security	1	3	1
Clients' trust	2	1	2
The speed of service delivery	4	2	3
Clients' information privacy	3	6	4
Clients' awareness	5	9	5
Continuity of the service	6	10	6
Spread of computer use	8	4	7
Spread of Internet use	7	5	8
Difficulty of using online banking by some clients	12	7	9
Pricing of Internet service	10	8	10

Figure 9: The future challenges for online banking according to banks

Because of the increasing regulation and supervision in the financial services market, also sector regulators place IT-security requirements for online banking systems at private banks. In general there are two important institutes which have made regulation regarding the IT-security at banks. The DNB has provided the ROB (Regeling Organisatie en Beheersing, regulation on organisation and control) to provide directives and recommendations for the organisation and control of business processes at financial institutes. The basic principle of the ROB is that financial institutes are responsible for organizing and controlling their business processes in such a way that their business is conducted in a controlled and sound manner (Lötgerink 2004). The Basel Committee on Banking Supervision has set up several principles which must be addressed by private banks when they offer online banking services. A short description of the ROB and the "Basel principles for managing risk in online banking" can be found in appendix B.

The IT-security requirements of these three stakeholders are shown in figure 10. As can be seen the requirements are categorised with the help of the CIA aspects. The IT-security requirements of the three different stakeholders are for the most part in line with each other. A difference which can be seen in figure 10 is the fact that the both the private banks and the regulators demand good non-repudiation mechanisms, while clients are not concerned about this. Many this difference can be explained with a conflict of interest between the private bank and the client. A private bank must be sure a client can not repute a transaction made in order to do business in a correctly manner. A client could even have benefit of transactions which he can repute. Therefore non-repudiation is regarded as a risk for private banks only. Another important difference is the fact that clients think the availability of the system is mainly important because of usability requirements. Clients think online banking systems must be available when they wish to use them and moreover the system must have acceptable response times. For the private bank the availability of the system is the most important in order to assure business continuity. For instance the response times of the online banking systems are only important in order to please the users of the system.

Aspect / stakeholder	Private banks	Clients	Sector supervisors
Confidentiality	- Assure secrecy of account information - Protection of internal data, such as information about prices, strategy, financial states and employees	- Secrecy of account information such as account balance and transactions information - Secrecy of client information	- Exclusivity of account data must be ensured with the help of sound authorization measures
Integrity	- Correct internal financial data - Non-repudiation of financial transactions	- Accurate information processing - Correct account information - Unauthorized transactions are impossible	- Non-repudiation of transactions and information must be assured - The reliability, accuracy and completeness of online banking transactions, records and information must be assured
Availability	- Prevent service outage in order to assure business continuity	- Services must be available 24x7 - Services must have a good performance (in order of seconds)	- Banks must have measures to prevent service outage - Banks must have repressive measures in place such as back ups - Banks should have emergency response programs in place

Figure 10: IT-security requirements for online banking systems of the major stakeholders

3.5.2 IT-security measures in online banking systems

In order to meet the stakeholders' security requirements described in figure 10 IT-security measures must be implemented in the online banking system. This paragraph will briefly describe the common used IT-security measures at private banks which have implemented online banking systems.

As described in paragraph 3.2.3 an online banking system consists of five groups of components, namely: people, hardware, software, data and procedures. Furthermore in this thesis the possible attacks on online banking systems are categorized in the three main quality aspects of IT-security, Confidentiality, Integrity and Availability. It is important for private banks to have measurements in place in all component groups against attacks in all quality aspect groups. Furthermore IT-security measures can be divided in four groups (Overbeeke et al. 2003):

- Preventive measures. These are measures which are implemented with the goal to prevent IT-security incidents. Almost all measures which are aimed against specified attacks can be defined as preventive.
- Detective measures. These measures have the purpose of detecting (potential) security incidents. These measures therefore do not counter security incidents by it but are very helpful in combination with preventive or repressive measures.
- Repressive measures. These measures have the goal to minimize the consequences of security incidents when they could not be prevented.
- Corrective measures. These are measures which have the goal to repair damage security incidents have caused.

Preventive and detective measures are mostly used to prevent security incidents. In contrast repressive and corrective measures are used to minimise and repair the damage after security incidents occur. Because of this in this thesis there are globally defined two goals of security measures, preventing security incidents to occur (preventive/detective measures) and fighting back when they could not be prevented (repressive/corrective measures). The way in which these IT-security measures can fight against threats and incidents is displayed in figure 11 below.

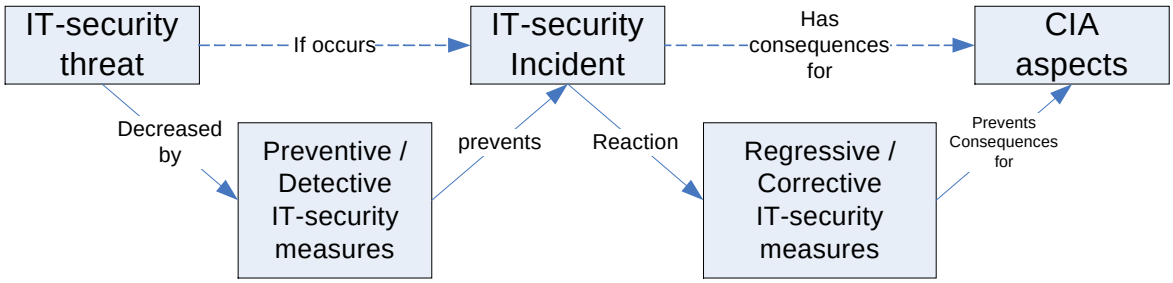


Figure 11: How IT-security measures can fight threats and incidents

With respect to IT-security measures there are now three different classification mechanisms:

- The type of object which must be protected against IT-security incidents
- The type of attack objects must be protected against
- The goal of the security measures

All security measures can therefore be placed in a certain block displayed in figure 12 below.

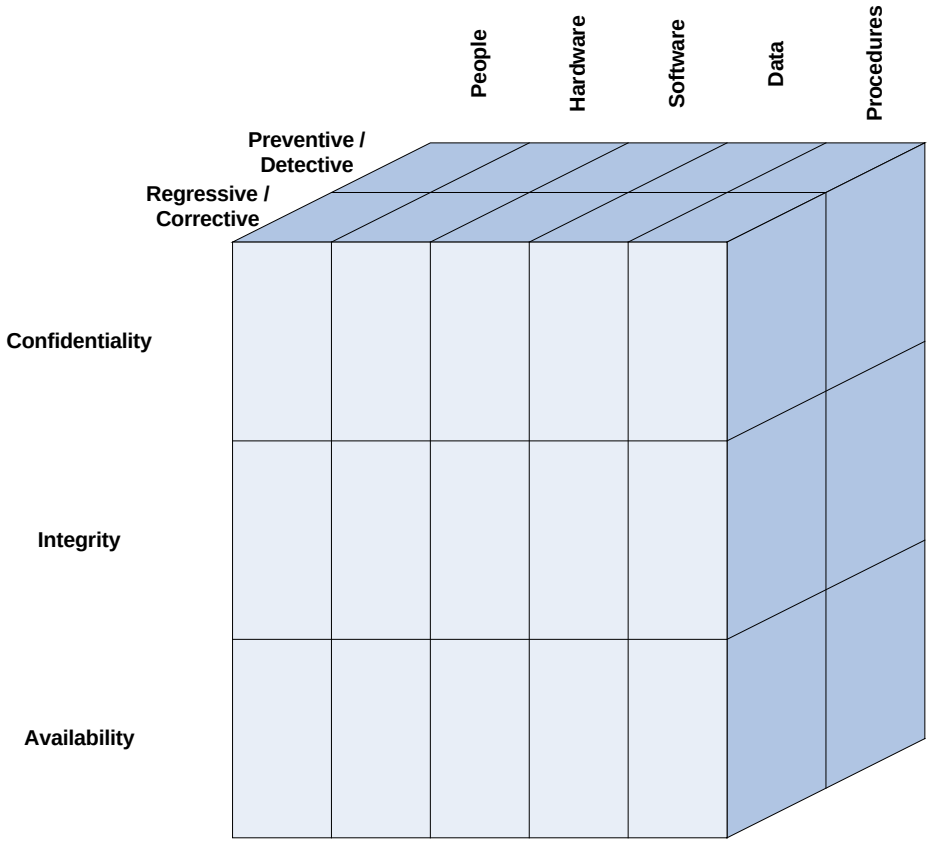


Figure 12: Overview of aspects of IT-security measures

In appendix C three figures are displayed which each set out the specific measures taken for each CIA aspect. In the remaining paragraph general concepts are described which must be implemented with the help of concrete security measures.

People measures

To ensure the confidentiality and integrity of the online banking system it is important to prevent unauthorised users to access the system. To ensure this an identification, authentication and authorisation mechanism must be in place.

In the first place it is important to know who the user is. This is called the identification of the user and is mostly done by asking for an user ID, such as an username or with the help of the IP-address of the user (Overbeeke et al. 2003). The next step then is to authenticate the user. Authentication is proving that the user is who it claims to be. There are several authentication mechanisms based on one of the following principles (Claessens et al. 2002; FFIIEC 2001; OCC 1998; Overbeeke et al. 2003):

- Authentication by something a user is. This can be done with the help of bio-optics such as iris scans and fingerprint scanning.
- Authentication by something a user knows, such as a password or a PIN (Personal Identification Number). There are some problems with password security. Passwords are sometimes too easy, are not frequently changed, are written down if they are to complex to remember, are not stored safely, and can be eavesdropped. Changing passwords frequently or even using one-time-passwords can help to overcome these problems.
- Authentication by something a user has, such as a smartcard, a list of TAN (Transaction Authentication Number) codes, a bankcard in combination with a card reader or a token. With the help of a smartcard a card reader or a token a so called challenge-response authentication can be performed. A user gets a challenge to perform an algorithm on the by the bank send data. The user responds with the data which results out of the algorithm. The bank can verify if the data is converted accurately and therefore knows the user has the correct algorithm.

After the user has authenticated itself, user rights can be given to the user. This is called authorisation. In practice this is done by assigning roles to the users. On basis of these roles they can read or write information in the system. Also the data in the system is classified in order to determine which access rights a certain role has to certain information in the system.

Next to protecting access to the online banking system also users must be informed about the IT-security measures which are in place. For example it is very important users are informed about recent security threats and trends on the Internet, such as a list of phising websites and forums with information about occurring fake e-mails. Furthermore it is important that banks stress the need of IT-security measures at the home PC, such as software firewalls and virus scanners, and security updates and patches.

Hardware measures

In order to prevent access of unauthorised users to the online banking systems on the network level firewalls, IDS and network compartments can be used. Firewalls combine hardware and software to block unwanted communications into and out of a private bank's network, while allowing acceptable communications to pass (OCC 1998). In short, firewall have the purpose of keeping unwanted network traffic out of the private bank's systems and letting wanted or trusted network traffic into the systems. By making network compartments and protecting these compartments with firewalls it is more difficult for an attacker to gain access to internal banking systems. In order to make these compartments it is important that private banks define which systems should be connected with other system. In this way only necessary connections between systems exist in the network. When despite of the above mentioned IT-security measures an attacker mentions to break in to the private bank's internal systems it is important that this could be detected and recorded. Intrusion Detection Systems are special kinds of firewalls which analyse the network traffic to detect awkward network traffic which can point at an attack. The success of firewalls preventing unauthorised access to online banking systems depends on the policy the bank has regarding blocking traffic. The bank must identify which traffic to the

internal systems from the Internet is forbidden and corresponding to this which ports are blocked or open. Furthermore firewalls are only effective when all connections between the internal banking systems and the Internet are routed via the firewalls (Committee on Information Systems Trustworthiness National Research Council 1999).

To ensure the availability of the online banking system it is important to have a business continuity plan. This plan includes arranging redundant connections and systems, making and restoring backups, and having UPS systems installed.

Software measures
It is very important that the software which is used in the online banking system is secure. Therefore it is also very important to test the security of the software extensively in the development phase. Some literature mentions this is the real big problem in the IT-security these days (Comsec information security 2005; Jaquith 2002). Network security can be implemented in a very well manner in which the risks of confidentiality incidents can be decreased. Developing secure software is more difficult than that. In the first place it is very important to implementing security measures when developing the software. In this way security is weaved in the software. Next to this when the software is in the live stage, security incidents which compromise the confidentiality of the online banking system should be investigated and the software must be protected against similar attacks. Furthermore software must also be regularly patched when exploits and their solutions are published. For private banks it is important to stay informed about security risks and incidents on the Internet.

Data measures
Encryption algorithms are working with keys with which the data can be encrypted and decrypted. The secure of such algorithms depends on the encryption algorithm which is used and the key length of the algorithm. There are two kinds of keys which could be used when encrypting data, symmetric and asymmetric keys. When using a symmetric key, the same key is used to encrypt and decrypt the data. A problem then is that both parties (the sender and the receiver of the encrypted data) must be in possession of the same key. Therefore the key must be given to the receiving party and sending the key via the Internet is not safe. To overcome this problem asymmetric keys are used in practice. When using asymmetric keys to encrypt data, the data is encrypted with a public key by the sender and decrypted with a private (which is secret) key by the receiver. Each private key has an own public key. This pair of keys is produced at the same time by the sender after which the sender can send the public key via the Internet. In this way only the receiver can decrypt the message (Overbeeke et al. 2003).

To ensure that transactions which are executed in the online banking system can not be denied it is important to secure the non-repudiation of these transactions. This can be done by recording which indentity has made certain transactions. Mostly this is done by logging transactions in combination with authentication mechanisms.

IT-security policy measures
Private banks should have set up a security policy regarding the confidentiality of the system. In this policy it could be recorded how the private bank will handle sensitive client information (often this is recorded in a privacy statement). This could be done by setting up a code of conduct which specifies among other things how employees should handle sensitive company and user information. To create security awareness special programs could be a solution. When executing such a program it is important that management commitment to the code of conduct can be seen by the employees to make this awareness sustainable (Basten and Wijnmaalen 2003). Also having an incident response

plan is very important. When confidential data is disclosed an incident response plan can help to arrange the response to the media. Also the next steps which must be taken, such as informing the involved users and arranging the financial compensation, are defined in such a plan. Another important measure which must be included in the IT-security policy is the segregation of duties at the private bank. A programmer for instance may have access to data in the test phase of the software development but when the system goes live this access rights should be removed. Generally there can be defined three distinct functions which must be performed by separate individuals, knowing the maintenance of the system, the supervision on the system and the development or changing the system.

To assess the in place IT-controls and IT-security measures an audit of the online banking system must be performed. An IT-audit consist of an objective review of the system design, an assessment of the in place internal controls, assurance about the existence of proper policies, procedures and standards (OCC 1998). Next to this, a penetration test could be performed in order to find weaknesses in the online banking system. When conducting a penetration test security experts of a third partly have clearance to attack the online banking system like if they are attackers themselves. Moreover private banks should gather as much information about IT-security incidents as possible in order to be able to analyse what the weaknesses of the online banking system are. Incident information could also give more insight in the performance of the in place security measures. Lastly, information about the attack and attacker could be useful for prosecution of the attacker in a later stage.

Finally, not only inadequate IT-security controls of the private bank itself can cause reputation loss but also the insourcing party can have inadequate IT-security controls if IT is outsourced. Therefore it is important for a private bank which is outsourcing IT to third parties, to have a Service Level Agreement with the insourcing party in which IT-security requirements are recorded.

3.5.3 IT-security incidents in online banking systems

If security measures are not sufficiently implemented in order to meet the stakeholders' requirements IT-security incidents could occur. In this paragraph the different kinds of incidents are pointed out.

As described in paragraph 1.4 the scope of this research is limited to external attacks. This involves IT-incidents which are caused by attacks to the online banking system via the Internet. Globally all IT-security incidents which could occur can be divided into three categories:

1. Attacks which are pointed to retrieve classified information (attacking the confidentiality of the system).
2. Attacks which try to modify the data and functionality which is present in the system (attacking the integrity of the system).
3. Attacks which aim to disturb the availability of the system (attacking the availability of the system).

Attacking the confidentiality of an online banking system

Attacks aimed at the confidentiality of the online banking system are trying to get classified information. Sometimes only accessing this information is enough, but mostly this information is used to perform an attack against the integrity or the availability of the online banking system.

Examples of such attacks are (OCC 1999; Spivey 2001):

- Phising, is a general term for all attacks which have the goal to obtain classified information of online banking clients and accounts. This can be done with the help of a fake website.
- Spoofing, is a general term of an attack in which an attacker is pretending to be another entity by pointing the URL of this entity to itself. There are three kinds of spoofing attacks. First an attacker can pretend he is the bank and intercepts the traffic between the user and the bank this is called a man-in-the-middle-attack. Second, an attacker can make a false website which has the same look and feel as the original online banking website. After this the attacker tries to point the URL of the legitimate online banking website to its false reproduction of the website. Third there are some websites on the Internet which can only be accessed with the help of a redirection from another website. An attacker can try to pretend he is the website from which the user is redirected. In this way the attacker can have access to restricted websites.
- Pharming, is a term for an attack in which a URL of a website is hijacked in order to direct traffic to this URL to a fake website.
- Sniffing. Such attacks are aimed at eavesdropping for classified information. On the internet there are a lot of tools available freely with which such attacks can be performed. A lot of banks use the Secure Socket Layer (SSL) mechanism to counter a sniffing attack. An SSL connection with the bank is established if the website offers a trusted certificate. The connection then is encrypted and an attacker can only retrieve encrypted data which is very difficult to decrypt without the key.
- Man-in-the-middle-attack. This is an example of a spoofing attack in which the attacker is pretending he is the bank by spoofing the URL or redirecting the traffic between the bank and traffic via his PC. The use of an SSL connection can prevent man-in-the-middle attacks by authentication of the bank by showing the user a digital certificate. The user can verify if the bank is really the bank it pretends to be. However an SSL connection is sometimes not as secure as a lot of private banks think. For instance, it is easy for attackers to make a false certificate. If the web browser which the client of an online banking system uses, does not (sufficiently) check for validity of the certificate, the attacker can pretend he is the bank and retrieve classified information (Comsec information security 2005). In contrast to this banks in the US are reevaluating the use of an SSL connection for online banking purposes. This because of the proposed fact the users of online banking systems do not understand the https URL usage. Furthermore the banks say the users of online banking systems do not have the patience to wait several seconds for establishing a secure encrypted connection (Miller 2005).
- Identity theft is a general term for stealing a digital identity. Attackers try to retrieve information with the goal to pretend they are another person. Identity theft has evolved in the last year because of the following developments:
    - Increasing number of consumers surfing or shopping on-line
    - More online sources of personal information where users use the same login name and password
    - Increased use of credit and user information exchanged with banks and retailers.

  Furthermore the use of mobile devices has increased dramatically in the last years. Because of this development it is easy to obtain digital IDs by stealing the physical hardware where these are stored on (Shaw 2005).
  Identity theft is mostly performed by using phising, spoofing and pharming techniques or by installing spyware on the user's PC. This spyware logs the user's

actions such as typing their username and password for entering the online banking system. Since users are routinely asked to install "add-ons" such as applets and active controls, most users will not understand how easy it is for a fraudulent site to install an applet that appears to offer one service but in reality captures and transmits confidential data back to the site in question (Bohm et al. 2000). Identity theft is the number one crime in the United States. Reported incidents of identity theft are projected to more than double, from 700,000 in 2001 to 1.7 million in 2005, and the costs to U.S. financial institutes alone will increase 30 percent each year, to more than 8 billion dollar in 2005 (Glaessner et al. 2002).
- Attackers can just break into online banking systems to obtain classified user and account information.

A recent phising attack used to get classified information from clients of the Postbank in the Netherlands (Stellinga 2005). Users of the online banking system of the Postbank got an email in which they were asked to go to a website of the Postbank (which has the same look and feel as the legitimate online banking website) to enter classified user information such as login names, passwords and transaction authorisation codes. The Postbank estimates that because of their warnings for the phising e-mail, only a couple of hundred clients have entered their classified bank account information at the fake website.

A good example of an attack against the confidentiality of an online banking system is the case of the identity thief called Abraham Abdallah. When the police arrested him in March 2001, he had Social Security numbers, credit card numbers, bank account information and other personal information of some of the richest people in the United States of America, including Steven Spielburg, Oprah Winfrey and Martha Stewart. He did this with the use of phising websites, cracking mailboxes and social engineering (Glaessner et al. 2002).

Attacking the integrity of an online banking system
Attacks aimed at the integrity of the system can have the following goals:
- Deleting data or functionality
- Changing data or functionality
- Adding data or functionality

Examples of such attacks are (ISF 2005a; OCC 1999; Spivey 2001):
- Viruses, trojans, worms or other malicious code which can modify, destruct or add computer programming codes, computer network databases, stored information, or computer capabilities.
- Breaking into the online banking system to process unauthorized financial transactions or to add, delete or change information in account information.
- Destroying data or programs with logic bombs. Mostly this is done via the front-end of the online banking system which operates with use of the Internet. Attackers can therefore access the back end systems of the private bank through the front end systems if these are not sufficiently secured.
- Defacing websites. If attackers break into the web server so they can upload other source codes they can alter the look and feel of the website.

A good example of how an attack against the integrity of an online banking system can also be an attack against the confidentiality of the system is described by Wiesmaier (2005). First an attacker infects the user's system with a computer virus or a Trojan containing a spy (such as a key logger). This spyware eavesdrops on the keyboard and mouse to obtain the ID, the PIN and the TAN in the background. If all information is obtained the spy closes the web browser. This is done before the TAN is sent to the bank

server. Thus the TAN stays valid. After this the attacker can login at the online banking system as if he is the user with the help of the obtained ID and PIN. Now the attacker can use the obtained TAN to perform an unauthorised transaction. If the victim reuses the TAN he will be told that it is invalid because it was already used. But as he has entered this TAN just before the web browser crashed, he will probably not be too surprised. The user will either think the transaction has succeeded, or he will use the next TAN to execute the transaction.

Attacking the availability of the system

Attacks which are aimed at the availability of the system have the goal to disturb the availability of the data and functionality of the system. Examples of attacks to the availability are (CERT 2002; ISF 2005a; OCC 1998; Spivey 2001):

- Distributed Denial of Service attacks (DDOS). Often this is done by attackers with the use of so-called worms. These are programs which are distributed among a lot of PCs which are connected to the Internet (forming a so called botnet). The user often does not know his personal computer is infected with the worm. After the infection of a certain amount of PCs, the attacker can command the PCs to send a request to a certain website. Because all the infected PCs can generated thousands or even millions of requests per minute the web server can only give an acknowledgement message back but never comes to the phase of sending the data of the website back to the PCs. In this way normal users who are trying to connect with the website get an error back from the web server.
- Buffer overflow attacks. When software is not correctly patched it can contain so-called exploits (known weak points in the software used in the system). An attacker can exploit these weak points to cause a buffer overflow in the system a denial of service as a result.
- Breaking into systems to shut down services. Often exploits (which are known vulnerabilities of a certain system) are used to break into systems. When an attacker can log in the web server for instance he can change settings such as that the web server will not provide the service which it is intended to provide.

An example of an availability attack is the Code Red worm which was launched in 2001. The worm attacked buffer overload vulnerability in the Microsoft IIS software. Next to this the worm also caused DOS attacks and heavy Internet traffic. According to computer economists the worm was responsible for 1,2 billion dollars of damage because of the use of 250.000 computers in a 9-hour period (Glaessner et al. 2002).

3.6 Conclusion

In this chapter the characteristics and the IT-security issues of online banking systems at private banks are explored. In addition the IT-security requirements of such systems set by the private bank, the clients and the sector supervisors were compared. The requirements of the different stakeholders only differ at two points. First clients do not have a concern regarding the non-repudiation of transactions and account information. Second clients have usability requirements regarding the uptime and the response times of online services. In contrast the private bank only sees uptime as an important security issue because of the assurance of business continuity which must be in place. Another conclusion is that despite the fact the financial sector is a best practice group regarding the state of IT-security, there are still significant threats present. In order to fight these threats more effort and investments in IT-security measures are needed.

Chapter 4: Reputation loss at private banks

4.1 Introduction

The goal of this chapter is to describe the relation between IT-security incidents and reputation loss. This is done by explaining the arrow in figure 13 by first defining reputation loss. In chapter 3 the IT-security incidents were already described. Therefore this chapter begins with defining right-handed expression in figure 13, reputation loss. Finally the factors which only have influence on reputation loss are described.

Figure 13: Relation between IT-security incidents and reputation loss

4.2 What is reputation loss?

Lin et. al. (2003) defines the reputation of a certain entity as something which is judged by an external entity such as a client in the case of a private bank. Furthermore the reputation of an entity could be in a certain steady state and is based on the historical behaviour of the entity. Reputation can thus be seen as a rating in which a stakeholder states if the entity meets the expectations of the stakeholder. If the bank does not meet these expectations reputation loss could be the result.

The risk of encountering reputation loss can also be called reputation risk and is defined by the DNB (2004) as:
"Reputation risk is the current or prospective risk to earnings and capital arising from adverse perception of the image of the financial institute by clients, counterparties, shareholders, or regulators."
Because this definition can also be found in other literature (Basel Committee on Banking Supervision 2003) the above definition of reputation loss is used in this thesis.

Lastly a certain incident at an entity which is a member of a certain sector could cause reputation damage to the whole sector. An IT-security incident in the online banking system of a certain private bank for instance, could cause reputation damage to other private banks which use online banking systems (Huyveneers 2001,).

4.3 Factors that influence reputation loss

4.3.1 Business risks

When private banks do their daily business and the business conditions are not in line with the implemented operations, private banks could be subject to risks. Chan (2001) has identified five general risks which private banks and other financial institutes could encounter:

1. Market risk. The risk of changing market prices and exchange rates.
2. Credit risk. The risk of bad loans. An example of this risk is a client who could not pay his loan.
3. Liquidity risk. The risk of a bank not able to meet its obligations towards its clients or business partners. An example of such a risk could be a bank that could not provide clients with the money on its accounts.
4. Legal risk. The risk of a bank that is not compliant with regulations and legislation because it has not implemented enough guidelines.
5. Interest risk. The risk of financial states that could be damaged because of interest changes.
6. Operational risk. This can be defined as "a threat to the capital and results of an institute because of inadequate execution of transactions with clients or other

stakeholders, qualitative or quantitative shortcomings or human shortcomings and inadequate decision making (De Nederlandsche Bank 2004).

The above mentioned risks are defined as risks a private bank has to cope with in its daily business. Where the first five risks are risks that are partly determined externally and related to the strategy of the bank, operational risk is only related to the bank's own operations. When one of these risks become reality reputation loss can be the result due to the fact that current clients lose their trust in the bank. In figure 14 below this relation is shown (Chan 2001).

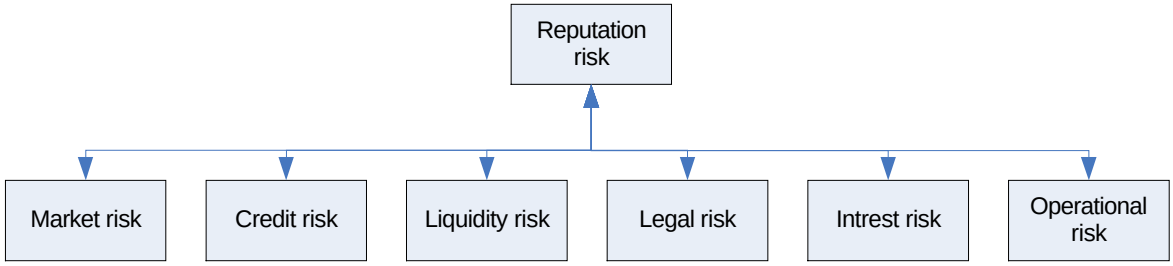


Figure 14: The relation between the different business risks at a private bank

For this research the operational risk is the most important because the online banking process is a part of the daily operations at the private bank. Within operational risk the DNB (2004) defines IT-risk in the ROB as:

"a threat to the capital and results of a financial institute caused by an inadequate strategy and policy or shortcomings in the used technical resources for information processing and communication".

IT-risk includes the risk of compromising the three quality aspects of IT-security. IT-security therefore can be seen as a subset of IT-risk. Figure 15 displays the relation between operational risk and reputation loss.

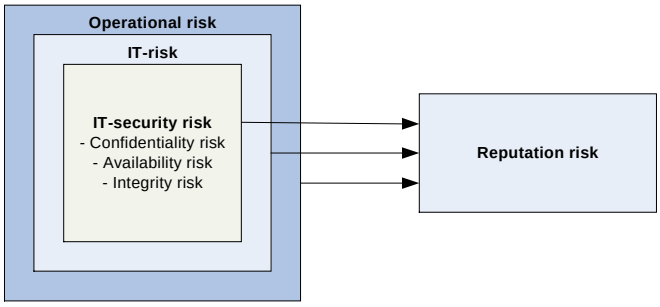


Figure 15: The relation between operational, IT and IT-security risk and reputation loss

4.3.2 Trust in online banking systems

In the USA, EDS (2005) has conducted a research among 610 users of online banking systems about the recent IT-security issues of such systems. The most answered security drawbacks of online banking systems were:

- Risk of security breach (60%)
- Risk of misuse of personal information (48%)
- Risk of intrusion on privacy (47%)

Also the users of online banking systems seem to be aware of the threats to online banking systems:

- Identity theft (81%)
- Risk of network, transaction and account intrusion attacks (57%)
- Insufficient encryption and sensitive data (48%)
- Phishing (44%)

With these figures it is clear that users of online banking systems in the USA have major concerns about the security of these systems. Despite this the same research points out that 93% of the respondents are “very” or “somewhat” confident that their bank protects their information. Another significant finding of this research was that 55% of the respondents would “discontinue banking activity until they were assured the crisis was resolved” as a reaction to security incidents. In addition 30% of the respondents would “close all accounts and eventually move to another bank” and 10% would “close some accounts and try another bank” when they became aware of a security incident in the online banking system. This research gives a perfect insight in how users of online banking systems would react to security incidents. Users are aware of the security risks of online banking systems but trust their bank will protect them from these incidents. If the private bank fails to accomplish this, the trust in the bank is damaged and clients are likely to leave.

In the Netherlands a survey was held to determine the best Dutch online bank (Geert-Jan Smits 2004). From this research it can be concluded that out of a total of about 7 million households 2.8 million use online banking. Also there are about 2.5 million households that have a computer with Internet connection but do not use an online banking system yet. This group is the potential new group of online banking system users. Of this group 1 out of 5 has the intention to use online banking in the future. Of the households that have a computer with Internet connection and do not have the intention to use Internet in the future 14% says the reason for this is that they think online banking is unsafe. This means a total of 280.000 households could be persuaded to use an online banking system as soon as the banks can assure them the system is sufficiently secured. Because there is no proof that IT-security incidents occur frequently the perception of these users is based on the reputation of online banking systems, which is likely not in line with the risk users are really encountering.

Like the Dutch, the Australian users of online banking systems are mainly not adopting online banking systems because of their doubts about the current IT-security measures (Sathye 1999).

Clients of private banks who use an online banking system must trust the system in order to use it. Trust in online banking systems is important because of the fact that financial transactions are done while there is a physical distance between the private bank and the client. For the client this means it is more difficult to have control on the execution of these transactions. In other words the client must rely on the online banking system and the private bank that the transactions are performed correctly. Factors that can have an influence on the level of trust clients have in an online banking system are (Avinandan Mukherjee 2003):

- Performance measures of the system, such as network and download speed, navigability, reliability, connectivity and availability
- The risk of disclosure of sensitive information about the client. This could be general client information such as the name and address of the client but also financial information. It is therefore for the client important to know in which way private banks handle these kinds of information.
- Clients base their trust in an online banking system of a private bank on the reputation of the bank.

Moreover, also financial institutes are aware of the fact an IT-security incident could cause a decrease in user’s trust. A research conducted by the ISF (2005a) in which companies were asked what the consequences of IT-security incidents could be, the loss of orders or contract ranks fifth and reputation loss is rated sixth.

Concluding potential users of online banking systems are likely not to adopt the online banking system because of security concerns. If a client is already using the online banking system they have placed their confidence in the system and in the bank that they will be protected against IT-security incidents. If this trust in the system is damaged by the occurrence of IT-security incidents, reputation loss can be the result. Hence it is important for private banks to prevent incidents from occurring because the trust in an online banking system and the reputation of the private bank are easier to lose than to gain (Lin et al. 2003). Private banks can gain user trust by assuring a certain level of quality for the CIA aspects of the online banking system. In addition, when a private bank has a good reputation the clients are more likely to trust the online banking system of this bank.

4.3.3 Media and current reputation

Reputation loss will only occur in a great manner when an IT-security incident is picked up by the media. How severe the reputation loss caused by IT-security incidents can be depends on several factors. Some of these factors are summed up below:

- The kind of media which picks up the news. If the daily newsflash on TV gives attention to the incidents this has more impact than local newspapers writing about it.
- The time in which the incident becomes news. For instance the summer time is often a period without a lot of news. In this period an IT-security incident could get a lot of media attention.
- The state of the private bank's reputation before the incident occurred. If the bank has encountered more incidents in the past which came into the news the reputation loss caused by a new IT-security incident could be greater. In addition former negative news items of the private bank, which were not related to with the security of the online banking system, can enhance the reputation loss caused by a security incident.
- The nature of the IT-security incident will determine if it is newsworthy. If one client has observed the fact the online banking system is not available this is not as newsworthy as an incident which really causes all the online banking clients to be unable to reach the online banking system.

In order to cope with the media attention a security breach will get, private banks should have incident response programs. They also should establish and periodically test a communications plan in order to respond in a correct manner when an IT-security incident really occurs. Banks should provide client support to supplement their online banking services and to reduce exposure to reputation risk. Client service affords a bank the opportunity to minimize the negative impact that occasional system failures or performance problems may have on a private bank's reputation by restoring client trust and satisfaction (OCC 1998).

4.3.4 IT-security incidents causing reputation loss

As described in chapter 3 an online banking system is always exposed to security risks. Security risks can be defined as threats which could occur. Security measures try to oppose the threat. When a certain attack manages to bypass these IT-security measures it becomes an incident. An IT-security incident can have consequences for respectively the confidentiality, integrity, and the availability of the online banking system. Reputation risk may arise if online banking systems are unreliable, if performance or data integrity is flawed, or if private client information is compromised. Such events may lead to adverse client and media reaction. Reputation risk also may arise if the bank fails to provide adequate disclosure of information or fails to resolve client problems associated with the use of online banking systems (OCC 1998). Because a user of an online banking system

demands certain requirements on the CIA aspects of the system as described in paragraph 3.3.2, if an incident occurs which compromised the user's CIA requirements of the system, users will lose their trust in the security of the system. Private banks are reacting on this by investing more and more money in IT-security measures (Spivey 2001).

Between the user's trust in the online banking system and the reputation of the private bank there exists a positive relation. When reputation of the bank is damaged, a new IT-security incident will be likely increase the breach of trust. On the other hand if the private bank has a good reputation the user's trust in the system can be increased. The breach of trust can lead to a client leaving the private bank. In this way the reputation of the private bank can be decreased in the eyes of that client because of an IT-security incident.

An good example of how a potential confidentiality problem caused by spyware programs can cause reputation loss is given by Lucas (2005):
"Reputation loss could become even more overwhelming than anything mentioned so far in examining the affects of spyware on level of production. Just imagine any one of the major SEC regulated brokerage firms losing millions of pieces of confidential information of their clients. The loss of confidence instilled within a companies business would be devastating. The brokerage industry is built upon a foundation of trust. The results of a newspaper headline reading "XYZ Brokerage Firm has recently found a security hole in which millions of clients confidential records have been divulged", would certainly cause a loss of production."

Glaessner et al. (2002) say about the relation between IT-security in online banking systems and reputation loss:
"Although not often acknowledged, a substantial denial of service or long-term intrusion that results in fraud, impersonation, or corruption of data can effectively cripple a bank's operations for a period of time. If that time is sufficient, it can irreparably damage the bank's reputation and possibly compromise its credit standing. Because market participants' confidence is critical, such an event could have a pernicious impact in a relatively short time."

In short these quotes are pointing out the fact that security issues such as fraud (integrity issue) and the disclosure of confidential information (confidentiality issue) can lead to reputation loss. Also they mention the fact that this reputation loss is due to a decrease of trust users have in the online banking system. Important then is to determine how the relation between IT-security is (Oscarson 2003b).

4.4 Conclusion

The conclusion of this chapter is graphically displayed in figure 16.

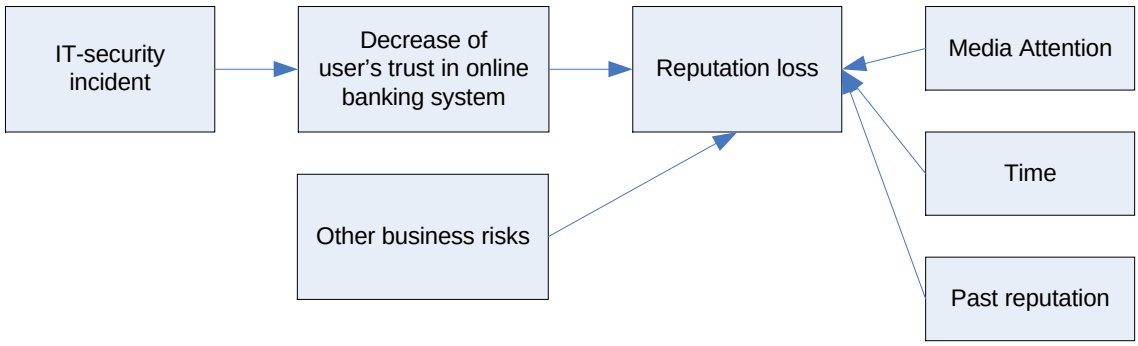


Figure 16: Resulting relation between IT-security incidents and reputation loss

Reputation loss in the context of this thesis is regarded as the decrease of the current client's perception of the degree to which the private bank meets its requirements. If IT-security incidents occur, the user will lose some trust in the online banking system. Since the private bank does not meet the user requirements this has a direct effect on the reputation of the bank in the eyes of the user and reputation loss is the result. The best indicator for the amount of reputation a private bank loses is the number of clients that leave as a result of the incident. With the help of this indicator a loss of capital under management can be determined with which also the loss of earnings can be calculated. Other factors that can enhance the amount of reputation loss in the case of an IT-security incident are other business risks which have become reality, the amount of media attention, the time in which the incident occurs and the former reputation of the private bank.

Chapter 5: Modelling reputation loss

5.1 Introduction

In this chapter it will be described how the relation between IT-security incidents can be modelled with the help of fuzzy logic. In order to accomplish this, first a conceptual model of the relation is explained. After that other ways to model and quantify reputation loss are explored and feedback is given. Next it will be set out why fuzzy logic is a solution which can circumvent some problems found in the other methods. Furthermore the working of fuzzy logic is briefly described together with the fuzzy representation of the conceptual model.

5.2 Conceptual model

Out of the chapters 2, 3 and 4 an extended version of the model in figure 17 can be made:

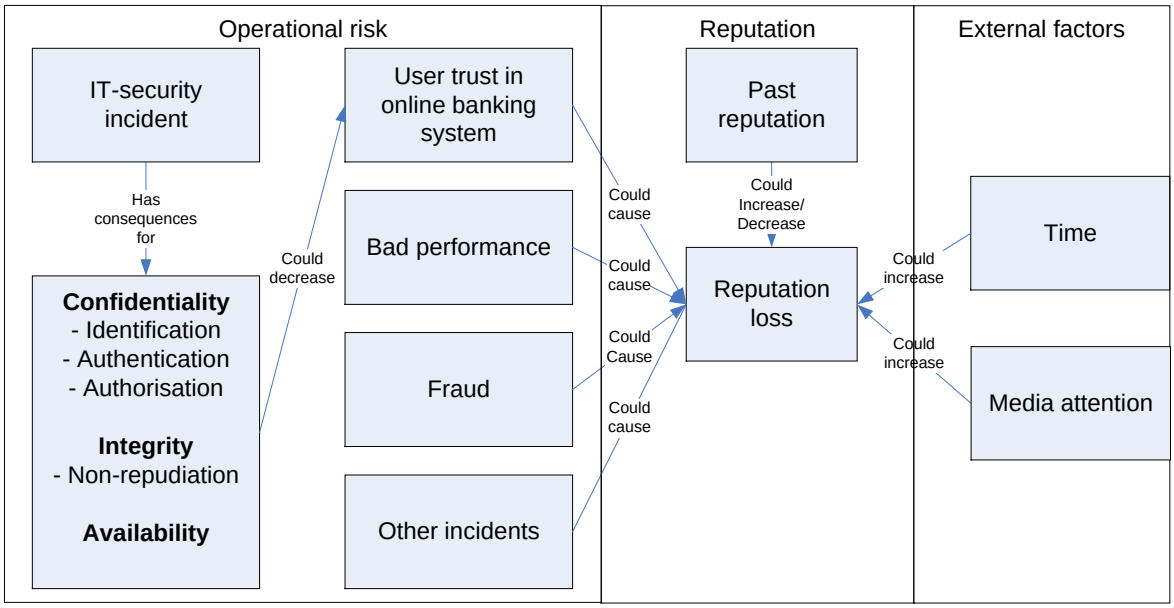


Figure 17: Conceptual model of the relation between IT-security incidents and reputation loss

Compared to figure 16, some additions and changes have been made with the conceptual model in figure 17 as a result. First the CIA aspects are added because a user will lose his trust in the online banking system for it does not comply with the security requirements of the user. As described the user trusts the system that it will protect the user against IT-security incidents. When a user observes a deviation in one or more CIA aspects it will lose this trust in the system. If this decrease of trust goes beyond a certain threshold the bank will not comply with the expectations of the client anymore and a user could leave the bank to go to another private bank. Furthermore the conceptual model in figure 17 zooms in on the operational risk a private bank could encounter. In addition, a bank's reputation can also be damaged by other business risks as described in chapter 4. To illustrate the fact that IT-security incidents are just one kind of accidents that could happen within the operation risk domain, other incidents are added in figure 17. Lastly, the factors in the total relation are grouped into three categories. As explained, the first category consists of factors that are an example of operational risk. Second the reputation domain consists of the reputation lost and the past reputation of the bank. Third, the external factors *time* and *media attention* are grouped. The groups of factors in the operational risk domain and the reputation domain are of importance for the relation between the private bank and the user of the online banking system.

After qualifying the relation between IT-security incidents and reputation loss with the help of a literature study and the formation of a conceptual model it is now important to take the next step to the quantification of the model. To measure the causality between the different indicators, it must be determined in which way the different indicators influence each other. In paragraph 5.3 some methods described in the literature are put forth which could be used to measure reputation loss with the help of indicators.

5.3 Measuring reputation loss

When measuring an indirect cost like the loss of reputation some problems arise. Often there is no sufficient historical data available to make conclusions based on quantitative research methods. Therefore some researchers have made methods to measure the indirect costs of IT-security incidents with the help of certain indicators that can be translated in terms which can be quantified. In this paragraph a summary of used methods to express indirect costs like the loss of reputation is set out. Furthermore each research method will be critically reviewed.

A good example of a method to calculate the loss of reputation caused by IT-security incidents is described by Garg (2003a; 2003b). This research focuses on the decline of the share price for the company that was attacked. In this approach some problems remain unaddressed. First, this approach will only work when a security incident is coming into publicity, this is however a rarely fact. Second, the decline of the shares could be caused by other influencing factors, which can not be separated. Third, the share prices of the companies which have experienced an IT-security breach are only monitored for three days. Therefore it is possible that the prices will go up again after this period and the resulting value of the loss of reputation can even be reduced to nearly nothing.

Anandarajan and Wen (1999) have defined three problems of the traditional methods to calculate the return on investment of IT-security investments:
1. The hidden costs of IT-security measures are neglected in these methods.
2. The indirect costs of IT-security incidents are neglected in these methods.
3. Risk is not properly integrated in these methods.

This is why Anandarajan and Wen proposed a method in which the first step is to define the indirect costs of IT-security incidents in certain processes. The next step is to find indicators for these indirect costs which can be expressed in monetary terms. Then the researchers asked respondents to fill in a survey with questions about the likelihood of certain IT-security incidents and their impacts. In the end they calculate the Internal Rate of Return (IRR) and the Net Present Value (NPV) of the intangible benefits (indirect costs saved) IT-security can provide. To have an idea how much these results can vary when the indicators or the chance will vary, they conducted a sensitivity analysis by also calculating the IRR and the NPV when the intangible benefits are ten percent higher or lower. A major disadvantage of this method is the fact that indirect costs can only be expressed in monetary terms. Another disadvantage is the fact that the proposed relations between the measures taken is given by the researchers.

Butler and Fischbeck (2002) have set up a method to determine a threat index for certain attacks. With the help of a so-called “multi-attribute analysis” they can set priorities regarding investments in IT-security measures. With this method the loss of trust and reputation can be assessed. Two following steps must be made in order to assess the Threat Index, which indicates how big the threat of indirect costs caused by IT-security incidents is:

1. Define the different kinds of indirect costs of IT-security incidents.
2. Define the maximum damage for each of the different kinds of indirect costs.

3. Calculate the Priority Weight (Wj) for each kind of indirect costs (j). In order to do so, three steps must be made: whatever type of indirect costs has the highest priority; this type of indirect cost gets the value 100.
   a. The most important indirect cost on basis of the impact the cost gets a Priority Value (Pj) of 100. The other indirect costs get a Pj relative to the most important indirect cost. Thus if a certain indirect cost is likely to have the half of the priority compared to the indirect cost with the highest priority, it gets a Pj of 50.
   b. Now it is possible to calculate the Wj for each indirect cost. This is done with the following formula:

$$W_j = \frac{P_j}{(\sum nP_j)}$$

   As can be seen for each indirect cost j the Priority Weight Wj is calculated by dividing the Priority Value (Pj) of that cost by the summation of the Priority Weights of all the kinds of indirect costs. In Figure 18 this is done for four different kinds of indirect costs.

Indirect costs	Priority value (Pj)	Priority weight (Wj)	Maximum costs (Xj)
Lost revenu	20	0,08	$10.000
Reputation loss	80	0,33	4
Lost productivity	100	0,42	240Hrs
Regulatory penalties	40	0,17	3
Summation of priority	240	1	

Figure 18: Table with the Priority Value, Priority Weight and Maximum costs of four types of indirect costs

   As can be seen in figure 18 the maximum costs of the indirect costs are expressed in different units. The Lost Revenue and Regulatory Penalties are expressed in scales of severity ranging from 1 to 4 and 1 to 3.
4. Define the different types of IT-security incidents that could occur.
5. Define the frequency for each type of IT-security incidents.
6. Determine for each type of incident (i) what the costs (Xij) for each kind of indirect costs (j) are.
7. The Damage Weight of a certain incident i for a certain indirect cost j is calculated by dividing the costs of the incident Xij of the indirect costs by the maximum cost Xj:

$$V_j = \frac{X_{ij}}{X_j}$$

8. Finally the Threat Index for a certain incident (TIa) by can be calculated by first summing up the Priority Weight W for an indirect cost j multiplied with the Damage Weight V of an incident i. Next, this summation will be multiplied with the frequency of occurrence of the incident for which the TI is calculated.

$$TI_a = Freq_a \ * \ (\sum\nolimits_{j=attributes} (W_j * V_j)$$

   In 19 below the threat index for the four indirect costs and three possible incidents is calculated.

		Indirect costs								
Threats	**freq/yr**	**Lost revenu (1)**		**Reputation loss (2)**		**Lost productivity (3)**		**Regulatory penalties (4)**		**TI**
		Xij	**Vj**	**Xij**	**Vj**	**Xij**	**Vj**	**Xij**	**Vj**	
Procedural violation (a)	4380	$2	0,0002	1	0,25	2hrs	0,0083	0	0	376.69
Theft (b)	24	$182	0,0152	2	0,5	1hrs	0,0042	2	0,67	6.75
Virus (c)	912	$0	0	0	0	3hrs	0,0125	0	0	80.03

Figure 19: Threat Index scores for several threats

The method of Butler and Fischbeck has two major advantages. First they measure the indirect costs with the help of indicators which can also be expressed in other terms than monetary values. Second with the help of this method a single Threat Index of a certain incident can be made while including multiple impacts of such an incident. The major disadvantage of this method is the fact that incidents which do not happen frequently will have a very low TI while they could be a severe threat. Furthermore the problem of quantifying more vague kinds of indirect costs, such as reputation loss, without subjectivity stays unsolved.

An automated method which could measure indirect costs is CRAMM. The three key components of the CRAMM method are asset values, levels of threat (the likelihood of an incident occurring) and vulnerability (Yazar 2002). After conducting structured questionnaires to determine the state of these three key components the results of these questionnaires are entered in the CRAMM software, which calculates the outputs for the level of threat with the help of linguistic values “very low”, “low”, “medium”, “high” and “very high” and the level of vulnerability with the values “low”, “medium” and “high”. The advantage of this method is the fact that linguistic terms are used to express the outcome. Despite this the main disadvantage of this method is the fact that the processing mechanism of the software and the type of input and output stays static and cannot be changed easily. Also this method is based on qualitative data given by a single expert. In this way conclusions from this method depends strongly on the subjectivity of that expert.

5.4 Why fuzzy logic?

In figure 20 below an overview of the characteristics of the above described methods and fuzzy logic is given. In this table the property “output” describes if the output of the model is given with the help of numbers (numeric) or with the help or expressed in words (linguistic). The validity of a model describes to what degree the model is measuring what it is indented to measure, in this case reputation loss. The reliability of the model describes to what degree the input and therefore also the output of the model is independent from coincidence. In other words are the outcomes of the model reliable. If a model is reliable it is not automatically also valid. If a model measures variables in a reliable manner the model still can measure the wrong things. In contrast if a model is not reliable it is also not measuring what it is indented to measure and therefore automatically not valid (Baarda and Goede 2001; Babbie 2004). In figure 20 also the level of researcher subjectivity is shown. If the model prescribes how expert knowledge must be processed in order the outcomes of the model are not easily influenced by the researcher. In contrast when the researcher chooses an ambitious method for processing the data in the model the researcher could more easily influence the model outcomes. Also when expert knowledge is obtained by interviews and the researcher uses this information to construct arbitrary numbers; these numbers are more subjective than with methods which allow the outcomes to be fully based on the respondents’ reactions.

Method	Monetary indicators only	Input	Output	Validity	Reliability	Level of researcher subjectivity
Garg, stock indices	Yes	External Statistics	Numeric	Low	Low	Medium
Anandarajan and Wen, IRR & NPV	Yes	Case study	Numeric	Low	Low	High
Butler and Fischbeck, multi-attribute analysis	No	Interviews	Numeric	Medium	Medium	Medium
Zeki Yazar, CRAMM	No	Questionaire	Linguistic	High	Medium	Medium
Fuzzy logic	No	Cumulative expert knowledge, Interviews	Linguistic	High	High	Low

Figure 20: An overview of the characteristics of the methods for measuring the indirect costs

As can be concluded from figure 20 the major problems of the methods described in paragraph 5.3 are:

- Some methods can only express indirect costs with the help of monetary indicators
- The level of subjectivity of the research method is mostly too high. One reason for this is that for instance in the case of Garg's method no expert knowledge is used. Therefore the validity of this method solely depends on the way in which the researcher chooses his indicators and processes the data. Furthermore if expert knowledge is used this is done with the help of a single interview, questionnaire or case study. In this way no cumulative findings can be obtained. Therefore the danger exists that the researcher jumps to conclusions to fast. In this way sometimes it is difficult that the intended outcomes are obtained. Also the methods are mostly subject to coincidence. Therefore the methods do not have a sufficient validity and reliability.

To solve these problems fuzzy logic can be used. People often use words (also called linguistic terms) for the identification and specification of a problem. Fuzzy logic tries to model these fuzzy expressions in a similar way as human beings solve problems in practice (Kasabov 1996). Fuzzy logic comes in handy when the relation between a certain cause and effect is not clear and when this relationship can not be expressed in a single state only. Or like Lotfi Zadeh, the founding father of fuzzy logic, likes to say (Krempl 2005):
"Fuzzy logic involves the making of accurate models of what is fuzzy".

With the help of a fuzzy system it is possible to cumulate expert knowledge into a model. Therefore fuzzy logic has more evidential value and therefore is more reliable than the other methods displayed in 20. The increased reliability and because fuzzy logic describes a method to model expert knowledge the subjectivity of the researcher is decreased. Also the validity of a fuzzy system is high because reputation loss can be measured in terms which directly deliver the outcome which is intended, i.e. a conclusion of the amount of reputation loss and what this means for the private bank. Fuzzy logic can model the relation between IT-security and reputation with the help of linguistic variables which need not necessarily be expressed in monetary terms. In this way fuzzy logic is a method which can model the relation between IT-security incidents and reputation loss in the same terms and universe in which the expert thinks. In this way also the output is more meaningful for the experts than with the other proposed methods.

5.5 How does fuzzy logic work?

The first step of building a fuzzy model is representing the proposed problem with the help of fuzzy variables. This process is called fuzzy conceptualisation. Fuzzy variables can be

quantitative (for example temperature or time) or qualitative (for example truth or belief) (Kasabov 1996). The problem described in this research (which security incidents could lead to reputation loss) is by essence a problem which can be expressed with the help of fuzzy variables. With the help of expert knowledge the fuzzy variables can be expressed in fuzzy labels. The process of representing a linguistic variable into a set of linguistic labels is called fuzzy quantization. These fuzzy labels in their turn are mapped upon a numeric variable with the help of membership functions. Each direct translation of linguistic terms into numeric values will lose some of the information given with the linguistic terms. Therefore fuzzy logic tries to define a certain amount of categories for a variable. Therefore membership functions are used for this translation. In the world of mathematicians a certain value is or is not a member of a certain category. With fuzzy logic it is possible for a certain value to be a member of more than one category (Brule 1985,). The transition from one to another category is gradual. In this way a numeric value can be part of more than one fuzzy label.

In order to explain how fuzzy logic works, an example of a fuzzy system will now be worked out. If we look at the reputation loss an IT-security incident could cause, an indicator for the reputation loss could be the number of clients which leave their bank when a certain security incident has occurred. An expert at the private bank could express the amount of reputation loss with words like “low”, “moderate” or “high”. When a certain incident occurs and the amount of clients leaving the bank as a result would be 20 some experts will say the reputation loss is “low”. Other experts would say is “moderate”. Also it is possible that an expert thinks this amount of clients leaving the bank causes a reputation loss which is between “low” and “moderate”. The membership functions model these expressions by letting a certain value of reputation loss to be part of more than one category at the same time. The membership function for the indicator “number of clients leaving” is constructed by asking experts at which number they think the reputation loss can be started to be called “low”. After this the expert is asked until which value for the variable “number of clients leaving” it can be called “low”. This is also done for the other two categories “moderate” and “high”. The ranges may overlap each other because a certain number of clients leaving their bank could be a member of more than one category. If the answers of the expert are been set out, a membership function as displayed in figure 21 is the result. The categories are displayed with the help of the coloured lines. On the horizontal axis the unit in which the temperature is expressed (number of clients leaving) can be seen. The vertical axis indicates to which part a certain value for the “number of clients leaving” is part to a category.

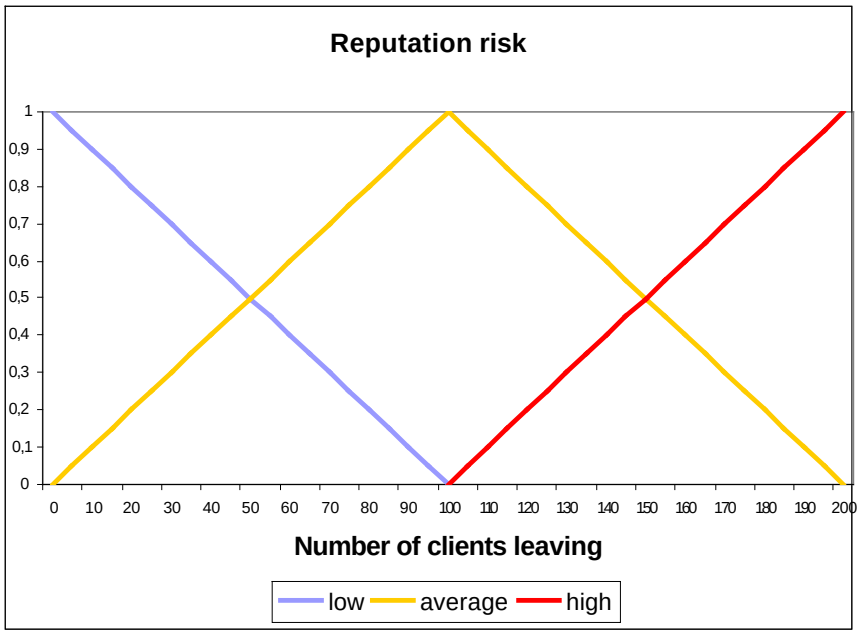


Figure 21: A membership function for the indicator temperature

To make a model of a certain relationship it is necessary to describe the cause and effect relation between a number of variables. In this example three influencing indicators are defined for reputation loss: “service outage”, “financial loss due to security incidents” and “the number of account compromised”. When all the indicators are defined and the membership functions for these indicators are defined, a processing mechanism transforms the input for the indicators into an output.

Schematically a fuzzy system which describes the state of the reputation loss is shown in figure 22.

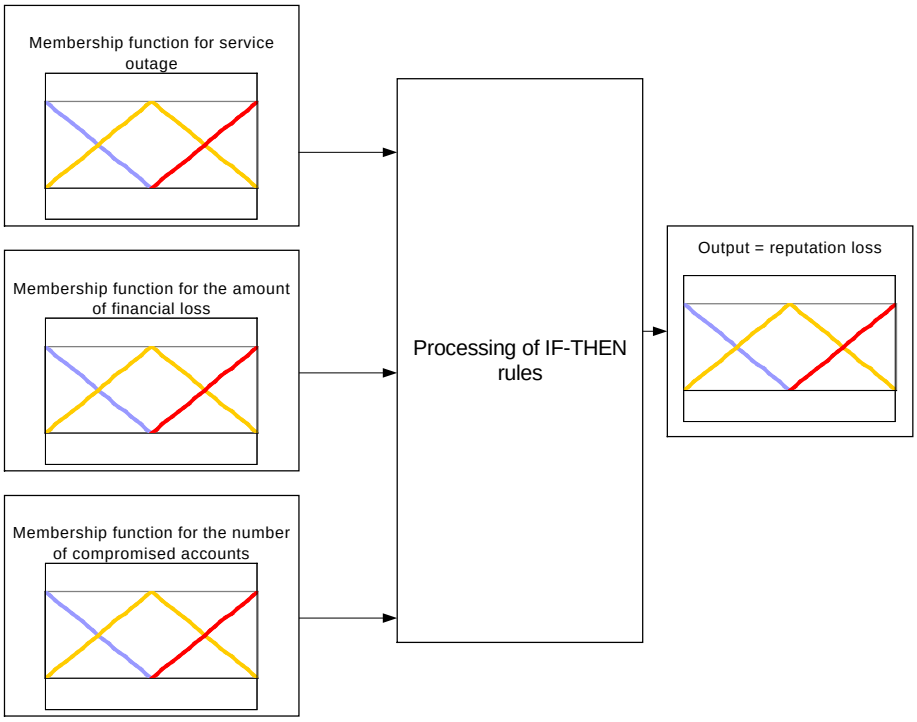


Figure 22: An overview of a fuzzy system

A fuzzy system is used to process fuzzy input to a form of output. Depending on the method used for processing the type of output can be crisp or fuzzy. In this case a fuzzy rule could be:
IF the service outage is "short" AND the amount of financial loss is "high" THEN the reputation loss is "high".
The output for the variable "reputation loss" could be numeric or linguistic depending on the method used to process the IF-THEN rules.

When both the membership functions and the IF-THEN rules are defined it is possible to determine the output of the reputation loss with the help of numeric inputs for the indicators. One method to do this is called the mamdani reasoning method. In figure 23 an example of a mamdani reasoning method is shown (Cornelissen et al. 2001; Dubois and Prade 1998). For instance if the numeric value of service outage is 10 hours, the degree to which it belongs to category A1 is a1 and the degree to which the value belongs to category A2 is a2, as can be seen at the left hand of figure 23. Furthermore the following two fuzzy rules are defined:
IF service outage is A1 THEN the reputation loss is B1.
IF service outage is A2 THEN the reputation loss is B2.
The corresponding values for the state of the weather can be found by drawing horizontal lines for the a1 and a2 values in the membership functions of respectively B1 and B2. By shading the area below the two lines the fuzzy conclusion can be found by finding the centre of the area.

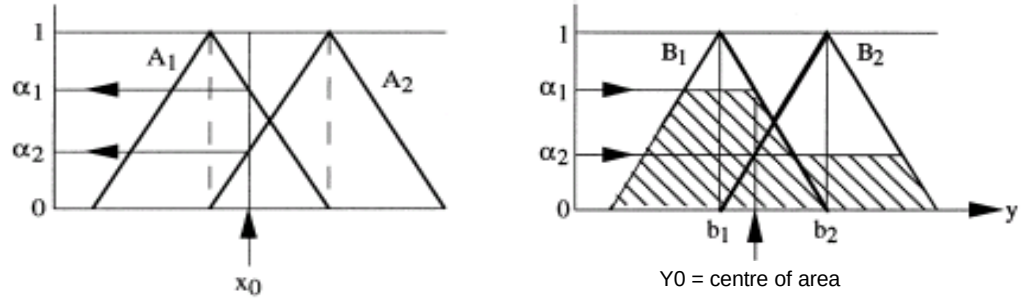


Figure 23: An example of the mamdani reasoning method.

5.6 Modelling the relation between IT-security incidents and reputation loss

As described in paragraph 5.4, fuzzy logic was proposed to use to model the relationship between IT-security incidents and reputation loss because it would solve the problems encountered with other methods. In figure 24 a step-by-step plan is shown for building a fuzzy model for the relation between IT-security incidents and reputation loss (Cornelissen et al. 2001).

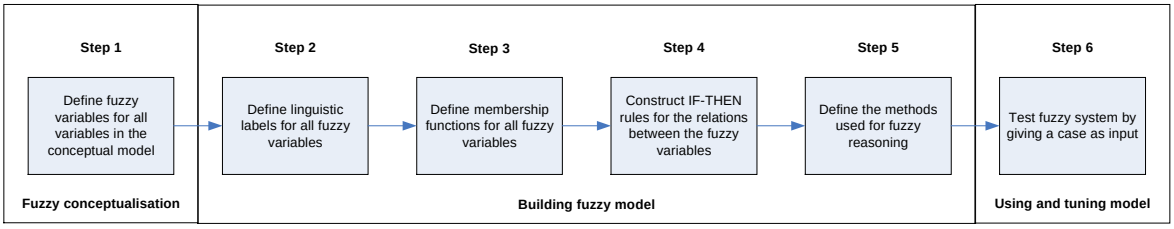


Figure 24: A step-by-step plan in order to make a fuzzy model of the relation between

The deliverables of steps 2 to 4 were meant to be the result of interviews with experts at private banks. After the first interview with an expert at a private bank it was clear the chosen expert group lacked the knowledge about their clients which was needed to successfully construct the membership functions and the IF-THEN rules. Due to the fact

the experts did not had enough information in order to accomplish steps 2 to 4 and therefore also steps 5 and 6 could not be reached. Because this problem has its origin at the research design and this could not be altered at that stadium, the research was continued in order to accomplish step 1 and get directions of how steps 2 to 4 could be made. Therefore the goal of the interviews held with the experts at the private banks was changed to validate the indicators and the proposed relations. Furthermore the way in which the membership functions and IF-THEN rules can be obtained was explored with the help of the interviews.

The first step consists of the fuzzy conceptualisation of the conceptual model. To accomplish this, fuzzy variables must be found for the shown variables in figure 17. In order to construct the fuzzy variables the following questions must be solved:

- What is the impact of a certain incident on the confidentiality, integrity and availability aspects of the online banking system? In order to measure the impact of incidents on the CIA aspects indicators for each aspect are needed.
- What is the impact of reputation loss caused by IT-security incidents on the private bank's business? To determine what the impact of reputation loss at a private bank could be, reputation loss must be expressed with the help of an indicator.

In figure 25 the proposed fuzzy model is described. This model is obtained by translating the conceptual model shown in figure 17 into a fuzzy logic model.

Because there are no experts which can express the decrease of trust into fuzzy labels or are able to translate the decrease of trust into a numeric variable this variable is bypassed in the proposed fuzzy model. In order to reduce the complexity of the model, incidents in the past which have influenced the reputation of the private bank are not included in the fuzzy logic model. The result could be that hidden reputation loss (which is the result of a former incident but becomes visual when an IT-security incident occurs) will not be taken into account. Furthermore the model in figure 25 is constructed with the assumption that an IT-security incident becomes public because only then the reputation loss would be significant. Also the type of media which brings the news and the time in which the news is brought are factors which have an influence on the likelihood of an incident coming into the news. Despite the fact these factors will have an influence on the reputation loss because of IT-security incidents, they are not taken into account in the model because of their external character. Because of this character it was impossible to measure these factors with the help of the experts at the private banks. Lastly the proposed model will only look at the reputation loss caused by current clients leaving the private bank when an IT-security incident has occurred. Next to the current clients also the dissatisfaction of potential clients, current suppliers and employees, because of incidents could cause reputation loss.

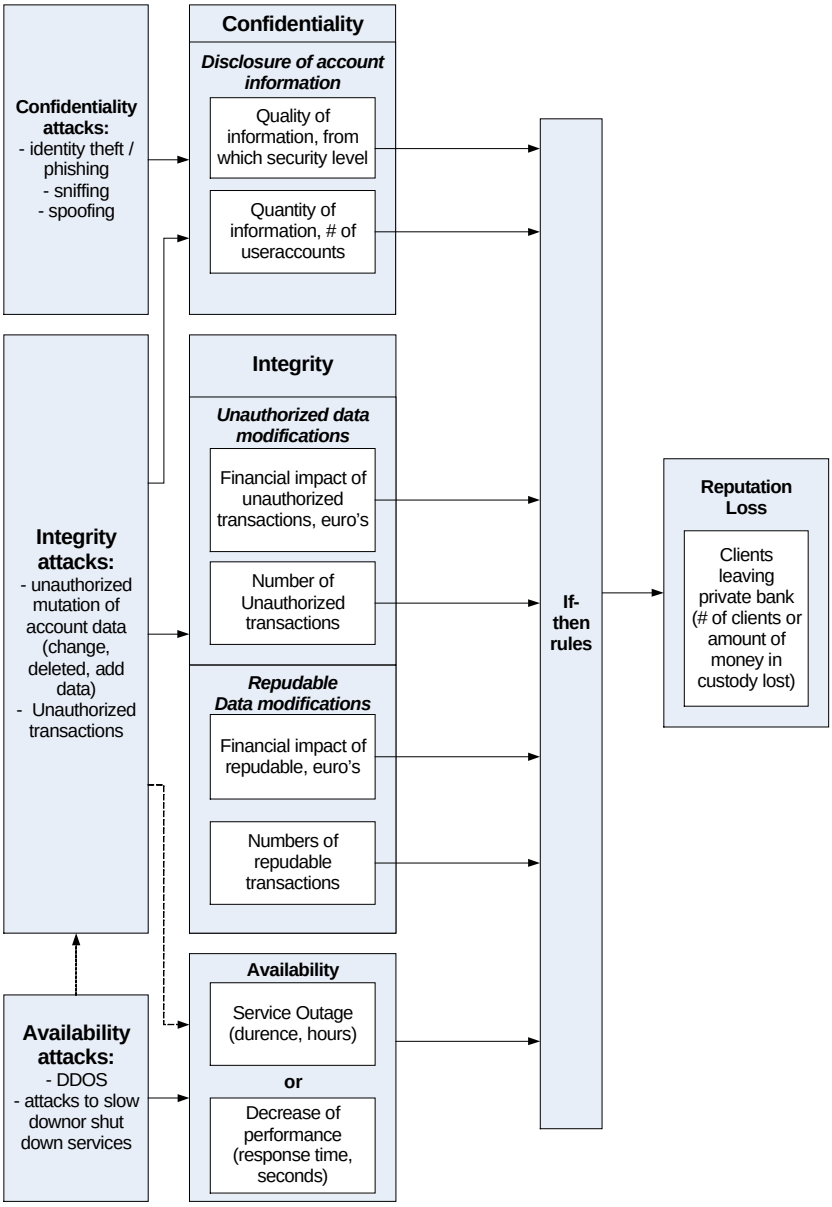


Figure 25: The proposed fuzzy model for reputation loss caused by IT-security incidents

5.6.1 Modelling the attack categories

In figure 25 the categories of IT-incidents at online banking systems at private banks, as defined in chapter 3, can be seen. The attacks are categorized in one of the CIA aspects but could also damage other CIA aspects. If a certain attack is sure to also impact another aspect this is shown by a solid line in figure 25. If an attack could impact another aspect a dotted line is used.

An integrity attack could also negatively influence the availability of online banking systems, such as a decrease of performance or even service outage. For example, if an attacker has broken into the online banking system and has made changes in the system, the delivery of normal services could be disturbed. Also the confidentiality of the online banking system will be compromised when integrity attacks are performed. Often an attacker needs some classified information about the user in order to break into its account. Furthermore when an attacker is able to perform unauthorized transactions he also has access to classified account information about the user and his account. An

availability attack which causes a server to crash can also damage the integrity of the system because data is lost.

5.6.2 Indicators for the impact of IT-security incidents

For the impact on the confidentiality of the online system caused by attacks the amount of user accounts which are disclosed is defined as an indicator. Also the security clearance of the account information disclosed is defined as an indicator.

An attack which will negatively influence the integrity of the online banking system can have two mayor results. First unauthorized (data) modifications can be performed in the system. Secondly these or legitimate modifications can be made reputable. In this way it is extremely difficult for a private bank to prove the modifications or to trace them back to the attacker. Modifications in an online banking system can cause financial damage. Therefore the indicator “financial impact” is chosen which is expressed in a currency (euros). Also data modifications could have more impact for the system as a hole, when more data is modified. Therefore the indicator “amount of data modifications” is included in the model. When more unauthorized modifications in the system are made it is more difficult to keep such an IT-security incident secret for the users of the system and the press. These two aspects are also applicable for repudiation of data modifications.

For the availability of the system two different indicators can be found. First the online banking system can be unavailable due to an attack. An indicator for this is called “service outage”. Service outage can best be measured with the variable time in hours. Another consequence of an attack against the availability of the system could be the delay of the online banking services offered. A good indicator for this is the response time. This will be measured in time expressed in seconds. For these two indicators of the availability of the system it is assumed that an incident will not at the same time cause a service outage and an increase in response time. Therefore these two indicators for the availability of the online banking system exclude each other.

As described in chapter 4 reputation loss can be seen as a decrease of user’s trust in the private bank. If an IT-security incident occurs at an online bank several stakeholders can have a negative perception of the security of the online banking system. When users lose a certain amount of trust in the system they can leave their private bank by opening an account at a competing private bank. Because trust itself is hard to quantify only an indicator for reputation loss is taken into account. Reputation loss caused by clients leaving the private bank can be described with the help of the lost capital under management. Private banks know exactly how much interest they can make on their capital under management. The financial loss because of missed interest on the lost capital under management is therefore defined as the indicator for reputation loss.

5.6.4 If-Then rules

As can be seen in figure 25 the IF-THEN block for the reputation loss indicator has an input of 7 indicators. That many input values would generate more IF-THEN rules than can be determined with the help of expert knowledge. This problem must be solved by constructing a multilayered fuzzy model. A way to model this could be to add an IF-THEN block at each CIA aspect. The indicators for the unauthorized data modifications, reputable data modifications and the disclosure of account information interact with each other. Therefore this must be taken into account when building the second IF-THEN layer into the model.

Chapter 6: Empirical research

6.1 Introduction

In this chapter the empirical research conducted is explained. First, the empirical research setup is discussed. After that, the questions asked to the respondents are summed up followed by their replies. Finally the outcomes of the interviews are discussed.

6.2 Empirical research setup

As explained earlier, the researcher was not able to construct the membership functions and the IF-THEN rules for the model shown in figure 25 by interviewing experts. Therefore the expert interviews got four new goals. First it is important to confirm the business need for a fuzzy model. Second the experts where asked to confirm the proposed relations and indicators as shown in the fuzzy model in figure 25. Third the interviews were used to determine which information and data is needed in order to successfully construct the membership functions and IF-THEN rules of the fuzzy model. Lastly the interviews were used to obtain an expert judgement of how specific IT-security measures could decrease the impact of incidents on the CIA indicators and the reputation loss. In combination with the literature findings the interviews can be used to answer the research questions stated in paragraph 1.3.

The expert interviews are based on open questions. These are questions for which the respondent is asked to provide his or her own answers (Babbie 2004). Semi-structured interviews were held with the help of a list of topics and example questions. In this way it is easier for the researcher to improvise in order to get more detailed information which is tailored to the respondent and the private bank he works for. A problem which can be encountered with this method is the fact that it is more difficult to make generalised conclusions. In paragraph 6.3 this problem is solved by categorised the answers to the questions with the help of questions which are a generalisation of the actual asked questions. Moreover, some subjectivity of the researcher when making conclusions out of these interviews can be present. The researcher tried to solve this problem by sending the worked out interviews for feedback to the respondents.

The interviews were held at the private banks at which the respondents work. Also no other persons were allowed to participate in order to prevent social desirable answers of the respondents. The interviews were not taped due to the fact that information about the IT-security of online banking systems is regarded as confidential information and the correspondents would not cooperate otherwise. In some cases the respondents asked the researcher to sign a non-disclosure agreement. As a result the answers were noted by the researcher which is less objective. To ensure the answers were recorded onto paper correctly the researcher has worked out each interview directly after the interviews were held. Another measure taken to make the respondents comfortable to answer sensitive questions was that the answers would be processed anonymously in the thesis. Note that for the research it is more important to know if all respondents think alike and give the same answers than knowing the individual answers of the respondents. Despite the measures taken to ensure the respondent no confidential information about the security measures at their bank would be disclosed some respondents maybe not gave all information they had in order to answer the questions asked.

When selecting the respondents the researcher concentrated on stand-alone medium size private banks or private banks that are a stand-alone entity owned by a larger bank. Large international private banks are therefore out of the picture. Also the four retail banks in the Netherlands (ING, ABN AMRO, Rabobank and Fortis) are out of the research scope. First

it was intended to only do interviews of experts at private banks that have a level three banking system. The reason for this is the fact that IT-security risks are significantly higher at full service online banking systems. Unlike the retail banks, which all are level 3 systems, these kinds of systems are very rare in the private banking sector. Therefore also level 2 systems were brought into the scope of the research. For this research, only level 1 online banking systems were not suitable because only availability issues can be the result of IT-security incidents for such systems.

In order to select interview respondents the researcher first obtained a list with all the official banks present in the Netherlands. This list was obtained from the DNB's website. By deleting all the known retail banks and internationally active banks, a shorter list was created. By visiting the website of the banks on the remaining list all banks which are not private banks were deleted. In this way a list with only Dutch private banks was constructed. The second step was to determine which level of online banking system these private banks have. By visiting the websites of the private banks and calling private banks with the question if they provide online banking services, private banks without (level 2 or higher) online banking systems were deleted from the list. The next step was to contact the banks with the question if they would cooperate with this research.

The next step was to set a respondent profile for the respondents needed at the selected private banks to conduct the interviews. Because of the interview goals described earlier the respondent must have knowledge of the technical aspects of the online banking systems, the in-place security measures and conducting risk analyses. Furthermore it was important that the respondent had a link to the business of the private bank in order to give his opinion about the impact of IT-security incidents on reputation loss. Within private banks often an internal audit department exists which among other things assess the IT-controls present at the bank. The internal audit department also consists of EDP-auditors, which are, because of their profession, familiar with both the technical and business aspects of IT. An internal EDP-auditor therefore could be a suitable expert for this research. Next to this the Security Officer has made his entrance at private banks in last years. A security officer has the task to ensure that the security in general is well arranged in private banks. Security officers are mostly people who have both technical expertise and business insight in order to balance and are therefore a second suitable expert for this research. In one case an online banking system architect was interviewed. Because he was extensively in touch with clients of the bank in order to meet client requirements of online banking system, this expert also has expertise regarding the IT-security of online banking systems and business aspects.

The banks at which the expert were interviewed are described in appendix C. Information about the operational performance of the bank is found in financial year reports of the banks and out of the interviews taken. In appendix C the interviewed respondents are described as well.

6.3 Interview findings

The interview findings below are categorised with the help of the goals these questions have.

6.3.1 Exploring the online banking environment

Who are the most important stakeholders of your private bank?

All private banks mention the current clients, the shareholders and the employees of the bank as important stakeholders. Also potential clients were mentioned as stakeholders. If a bank does not meet requirements set by potential clients these individuals will not turn into clients in the future. As can be seen in the operational performance of the interviewed

banks described in paragraph 6.3, for private banks it is important to increase the capital under management in order to increase their income and earnings. This is especially important when operational costs increasing as well.

One respondent stated that employees would not even want to work for the bank anymore if the quality of the delivered services and products would reduce. In this way such a bank has to perform in line with the requirements of the employees in order to assure that employees will stay at the bank.

Another bank stated that regulators and supervisors in the sector such as the DNB and the AFM are important stakeholders for that bank. These regulators and supervisors have set more requirements which private banks should implement. For a bank it is important to have a good relationship with the regulators and supervisors in order to stay compliant with regulation and legislation in the sector.

Is your bank an independent bank or a part of a larger organisation?
As can be seen in the descriptions of the private banks in paragraph 6.3, Insinger de Beaufort, Kempen & Co and van Lanschot Bankiers are independent private banks. Theodoor Gilissen Bankiers and Delta Lloyd Bankengroep are part of a larger company. The respondents of the independent banks say that it is very important to settle their brand name as a trustworthy bank. Moreover they emphasize that being independent leads to more customised and personal service delivery. Mister Bout of Theodoor Gilissen Bankiers states that being part of a larger private banking association opens doors which were closed before. First, products and services can be set up more efficiently. Due to this there is more budget for centralised investments. What is more, the quality of the in place IT at Theodoor Gilissen has increased by the decision to centralised the IT at a central place in Europe.

Who are your bank's main competitors?
For the pure private banking service all the interviewed banks state the same group of banks. Next to mentioning banks which are interviewed in this research the banks mentioned the following names: MeesPiersson and Staal Bankiers. Furthermore the banks mention the increased competition of the big four retail banks ING, ABN-AMRO, Rabobank and Fortis. For stock exchange services performed by the private banks, Alex and Binq, the two big Internet stock exchange banks are mentioned. These answers are in line with the literature which mentions increased competition in the private banking sector. Large banks such as the big four banks in the Netherlands can offer banking services against a lower prices because of economies of scale. Because the private banking market is very attractive these banks try to take over a part of this market from the specialised private banks. The only way private banks can survive this is by offering more quality in their services and products with a personal touch. In addition, the stock exchange services at private banks are threatened because of the efficient way Alex and Binq are doing their business. Private banks are trying to cope with this by offering wealth management services. In this way not the client is choosing to invest his money in a certain stock but the private bank does. The idea behind this is that the private bank has more expertise on this subject. There are some exceptions such as Kempen & Co. which is trying to compete with the internet banks with their own Internet stock exchange services. Theodoor Gilissen has bought Stroeve to get more hold on these services.

What are the main new developments in the private banking sector?
Three out of five banks say the competition from the four large retail banks in the Netherlands has increased. Next to this two out of five banks say the transparency of the costs and the quality of services and products has increased because stakeholders want

to have insight in the bank's operations. In line with this the banks say their clients have become more demanding and therefore the service level has gone up in recent years. Furthermore, clients have become more and more risk averse since the downfall of the stock exchange in the beginning of the 21st century. Clients therefore are not only looking for private banks which have the highest performance ratings on their money but can also give assurance about their capital. Another development which four out of the five private banks acknowledge is the increasing regulation and legislation combined with more rigorous supervision. Banks are investing more to be compliant with recent regulation and legislation such as IFRS, the ROB and Basel II. As one bank emphasizes, the AFM now independently publishes shortcomings found within financial institutes like private banks.

6.3.2 Exploring the functionality of online banking systems

What is functionality of the online banking system of your bank? What level has the online banking system of your bank?

Four out of five private banks have implemented a level 2 online banking system. Only one bank makes use of a full service level 3 online banking system.

The functionality of the level 2 online banking systems is mostly the same according to the four respondents. The system gives insight in the account balance of a banking account. The refreshing frequency of this account summary is different at each bank and defers from daily to even quarterly. The private banking client has insight in mutations in his account balance and investments. Furthermore information about performed financial transactions is shown in this summary. With the help of this information the client could see how his portfolio of stocks is performing, which transactions the private bank performs (when the bank manages the capital for the client) and what the state of the credit loans at the bank is. If a client is a so called execution only client (the client manages its capital on its own) the orders for making transactions are done by telephone or with the help of the account manager.

The level 3 system which was present at a single bank, gives daily account information. Furthermore the client can perform financial transactions on its own. He can for instance digitally execute payments and buy or sell stocks on the stock exchange markets.

The banks which had a level 2 online banking system were asked why they do not have implemented a level 3 system and if they are planning to do so in the future. These banks mostly say they have a lot clients for which the bank provide wealth management services and therefore do not need the function of making online transactions. Furthermore in the Dutch private banking sector a lot of old money is present. These are clients which have inherited their money, are a little older and do not have the need to use online banking systems. The only reason to implement online transaction services in the future is to offer more convenience to the execution only clients, which is not the main target group. It can be concluded that just a small part of the private banks in the Netherlands uses level 3 online banking systems. This is in contrast to the main stream banks which all use this level of systems. Two of the four banks having a level 2 systems say they have discussed adding functionality to the system in order to upgrade to level 3 systems. They mention the reason for not doing this is the increase of costs and risks while no additional benefits are obtained. The only bank interviewed with a level 3 system doesn't agrees with this and even thinks that his bank is that successful because of the offering of advances online services.

Which reasons did your bank have to implement an online banking system?

The most heard argument to implement a level 2 online banking system is the fact that a lot of the clients are people which are internationally active. With the help of a level 2

system, clients can have insight in the state of their bank account anywhere and anytime. Four of the five banks therefore stated that the main reason to implement the online banking system was in order to offer a higher service level to their clients. In addition, three out of the five respondents said that they implement an online banking system because their clients are expecting this. Another reason for implementing online banking systems is the decrease of operational costs as a result. Three respondents said though this was not the main reason, cost savings played a big role when deciding for the implementation of an online banking system. Just one bank said they implemented an online banking system in order to improve the communication between the bank and their clients by enhancing the Internet communication channel.

On top of the mentioned reasons above, the bank that implemented a level 3 online banking system stated that they were offering these services in order to have a competitive advantage. This bank had the philosophy that if they offer all banking services by their own the client is not forced to hold a second banking account at another bank. In this way these clients will be less sensitive to offerings of their other bank and will less likely go to another bank for banking services. Also the private banks with a level 2 system have mentioned the prevention of a competitive disadvantage was a reason to implement the system. Because all their competitors are also offering an online banking system they could not stay behind.

6.3.3 Exploring implemented security measures in online banking systems

Which IT-security measures are taken at the online banking system of your bank?

Hardware

All respondents are using firewalls to prevent unauthorised data transmissions on the hardware level. Four out of five respondents do also have IDS systems in place. An IDS can be a firewall with extended functions. Three out of five respondents say their bank has divided the internal network into compartments with the help of firewalls. These measures are taken to prevent an attacker to have access to all internal systems when he has entered just one of them. All banks have stated to have duplicate systems in order to prevent the online banking system going down because of attacks or incidents.

Software/Data

To prevent sniffing by an attacker on the Internet, all respondents state their bank makes use of a SSL connection. For user identification/authentication to the online banking system, three out of five banks still rely on username/password combinations. Two banks are using card readers or tokens to implement two-factor authentication. The user must go to the website of the private bank to login. The login page is secured with the help of a SSL connection. After the user has filled in his account number and the number of his bank card he receives a challenge to fill in the correct number at the login form. This number can be generated by inserting the bank card in a card reader and entering the PIN. When the user pushes a button he obtains the unique code which must filled in the login page. Another way in which such a unique code can be generated is with the use of so-called token. A token is a device which generates unique codes with time based intervals. In this way the user has to authenticate his self with the use of something he knows (the PIN) and something he has (bank card, card reader). One bank uses smart cards to prevent man-in-the-middle-attacks (MIM attacks). An attacker can perform a MIM attack by falsification of the private bank's certificate. In this way the user establish a SSL connection with the attacker. The attacker can decrypt the encrypted data send by the user and can therefore view this data in plain text. Afterwards the attacker can establish a connection with the bank as if he is the user. Smart cards can prevent MIM attacks by requiring users to send a certificate to the bank when establishing an SSL connection with

the bank's systems. In this way the attacker has no private key of the user and therefore cannot pretend he is the user. Such a security measure can also ensure non-repudiation of transactions. The user cannot deny transactions because he is the only one which could make these transactions given the signing of the message. Two banks were stressing that two factor authentication could be more expensive but is much more secure.

One bank indicated that they are using user detection for intrusions. This is done by sending information about last performed transactions and logins to the user. In this way the chance of a user detecting deviations in the systems is increased.

Four of the five banks say that the IT-security challenges are in the application security. The network security has evolved to a level at which it is good enough to prevent almost every attack on the network level. The remaining risk of network attacks can be solved with very expensive additional measures. Therefore the benefits of such measures compared with its costs are not enough in order to implement these measures. Because a big part of the front-end software of an online banking system is in essence publicly accessible via the Internet it is very important to secure this software. The respondents claim that a lot of security incidents are caused by mistakes in the software. Therefore it is very important that software developers are aware of security issues. Furthermore online banking applications must be extensively tested before they are launched.

Procedures
All banks state that each year an audit is performed on their online banking system. Moreover four out of five respondents indicated that they have recently ordered a third party to perform a penetration test on their online banking system. The increased regulation and legislation has increased the attention to such audits and tests. The ROB for instance demands that an audit is performed on the IT systems of the bank.

Three out of five banks mentioned that also the authorisation of the employees of the bank regarding the online banking system is very important. Mostly only the account manager of a certain bank account is authorised to access account information. One respondent told about his first days at the private bank in which he had obtained account information on local hard drives of PCs via the company network. Therefore he said it is very important to have procedures in place which tell how information must be handled.

At another bank the respondent told about the in place segregation of duties and the four eye principle which when making important changes in the system.

Two of the five respondents think private banks will cooperate more in the future in order to cope with IT-security issues and incidents. These respondents think private banks should not think of security as a competitive advantage but something which is inevitable. Furthermore they claim that the security at their competitors is also important for them. If one bank does not have implemented sufficient IT-security and an incident occurs, a decrease of client confidence in the whole online banking sector could be the result.

Other remarks regarding the security of online banking systems
Out of the interviews it can be concluded that the state of IT-security at private banks is becoming more professional. Banks are increasingly willing to cooperate with each other in order to overcome the risks and the threats of the Internet. Forced by new regulation and legislation the private banks are also going towards quantifying the risks present at the private banks' online banking systems. The need for IT-security measures is continually increasing because of the new regulation and legislation and the enhancing

technology. IT-systems are becoming more and more complex to manage and to secure while the tools used to attack online banking systems are evolving.

Also conflicting requirements of stakeholders can make the security online banking systems difficult. For instance a user of an online banking system wants a system which is easy to use and is performing fast. Private banks want to secure systems with security measures such as data encryption or smart cards for authentication which can compromise these demands.

Private banks are conducting risk analysis regarding the IT-security of their online banking systems but investments in IT-security are still made on basis of qualitative arguments. The respondents don't believe making decisions about IT-security investments could not be based on quantitative figures only. Some respondents acknowledge that measuring the impact and the risks of incidents to the reputation of the private bank could help explaining the need for IT-security measures. One respondent explained this as follows:
"When persons in the higher regions of the company must sign for the residual risk after taking IT-security measures, it becomes more likely the return on investments in IT-security must be explained"

Did your bank outsourced (a part of) the online banking system to a third party? How does your bank try to ensure the quality of the IT-security measures taken by this third party?
Two banks have recently outsourced their IT to a third party service provider. In this way also the IT-security is outsourced to the third party. The quality of the IT-security measures taken by these parties is ensured with the help of Service Level Agreements (SLA's) in which the security requirements set by the bank are defined. Furthermore the internal audit department of the banks that have outsourced their IT resources, have checked the in place security at the third party systems. The main reason for the other banks not to outsource their IT resources was the need for financial expertise in order to guarantee the quality of the offered online services.

6.3.4 Validating the occurring attack categories

Which confidentiality attacks do occur at the online banking system of your bank?
Three of the five banks stated that they do not recently have encountered phising attempts. The respondents think the reason for this is the fact the private banks are relatively unknown with the public. Two of the five respondents did acknowledge phising as the main problem for online banking systems due to the recent wave of phising attacks. One bank mentioned the occurrence of sniffing attacks and three of the five banks stated that port scans are daily business (despite the fact that not all port scans are malicious this is something banks monitor in order to get information of potential attacks).

Which integrity attacks do occur at the online banking system of your bank?
Three of the five banks state that they have not recently encountered attempts of attackers trying to break into their online banking systems. One bank said they have encountered a so called SQL-poisoning attack. Such an attack is performed by entering SQL statements for database executions into the forms present on the bank's website in order to break into the system. Furthermore all the four banks which have answered this question stated that they have not recently seen unauthorised transactions caused by external attackers. The banks say that it could occur that the account balance of a certain bank account deviates from the suspected value. These deviations in account balance are always caused by internal errors and mistakes in the online banking systems. The clients that detect and report such a deviation are compensated by the bank. Some banks are using a fixed bank account to which transactions from the private banking account could

be done. In this case it is more difficult for an attacker to perform unauthorised transactions because he should first change the account in order to transfer money to itself.

Which availability attacks do occur at the online banking system of your bank?
All four banks who have answered this question stated they have not encountered availability attacks recently. According to three respondents it is difficult to protect a private bank's website from availability attacks, such as DDoS attacks. One of the respondents said the damage of potential DDoS attacks could be minimised with the help of firewalls which allow a limited number of connections with back end systems.

Two respondents stated that malicious code attacks on the online banking systems are occurring frequently because viruses and Trojan horses on the Internet are also targeted against web servers. Also the private bank's systems could be infected with malicious code by incoming e-mail. By implementing high quality virus scanners and having a strict patching policy for the online banking systems the risk of availability issues caused by malicious code can be decreased.

Other availability issues which do occur but are not caused by external attacks are problems like hard disk failure, back up problems and power outage.

6.3.5 Validating the chosen fuzzy variables for the CIA aspects

What would be the reaction of the users of the online banking system to the consequences a confidentiality attack has for the system? What could be good indicators for the impact such an attack has for these users?
According to four of the five banks, clients are really mad when confidential information about their person or their bank account is compromised because of a confidentiality attack. Furthermore the banks think that there is a big chance that clients who come aware of such an incident will leave the private bank for one of its competitors.

The respondents mention several factors which could influence the reaction of clients on confidentiality incidents. First if such incidents are occurring more than once it is more likely such incidents will get more media attention. In this way more users of the online banking system could be aware of the incident and the impact of such an incident to the reputation will be more severe. Also the scale of the confidentiality attacks could be of importance for the reputation of the private bank. If only one client has been the victim of a confidentiality attack and the client does not communicate this to the media the worst what could happen is that this client is leaving the bank. If confidentiality attacks are occurring at more online banking accounts, the chance of media attention becomes higher and banks suspect more clients to leave their bank.

Another factor mentioned is the level of confidentiality of the information compromised. If only account information is compromised the damage to the user's trust in the system is less than when also the corresponding user information is retrieved by an attacker. By separating personal information and account information of a user, banks try to benefit from this conclusion.

Also the banks are indicating that the reputation of the user itself is an important influencing factor. If a user is a well known and very wealthy public person, the compromise of his online banking information is more severe than the information of an unknown user.

Good indicators of the decrease of the users' trust in the online banking system because of confidentiality attacks, could be the extent to which information is compromised, the frequency of occurrence, the scale of the attack and the level of media attention the incident gets.

The impact of confidentiality attacks to the users trust in the online banking system is the same independent from the level of online banking system (level 2 or level 3).

What would be the reaction of the users of the online banking system to the consequences an integrity attack has for the system? What could be good indicators for the impact such an attack has for these users?
Users confidence in the online banking systems will also decrease when users become aware of the occurrence of an integrity incident. According to two respondents the amount of money a certain unauthorized transaction involves is of importance for the news value of the incidents. Also the frequency of occurrence is important for the news value. In addition the user that is a victim of an integrity attack will be more frighten when such a transaction involves more money but the his trust in the system will not be damaged more. Two out of five respondents think the fact that such an incident could occur is the real reason of decreased user's trust in the online banking system. One respondent illustrates this by mentioning that a lot of incidents with a low monetary value could have more impact on the users trust in the system than just a single incident involving a lot of money.

The respondents of private banks which have a level 2 online banking system in place think they are not very vulnerable for integrity attacks because the system does not offer the functionality for users to perform online financial transactions. In this way the only way an attacker could perform for instance unauthorized transactions is by breaking into the internal banking systems via the front-end of the system. The respondent of the private bank with the level 3 online banking system stated that the integrity of the system could even be more important than the confidentiality of the system. Users of a level 3 online banking system expect that performing unauthorised transactions from their bank accounts is impossible. If this expectation is not met by the private bank users can lose all the trust they had in the system and stop using the system or will leave the bank.

Is the non-repudiation of transactions in the online banking system an issue for the users?
All respondents think non-repudiation is not a user issue but one of the private banks. The bank wants to be sure a certain transaction is performed and in the case of disputes with clients they must have evidence. Furthermore it is not in the concern of the bank that users can prove that they have ordered for a certain transaction. For the non-repudiation at the bank side of the system log files are present in which the occurrence of transactions are recorded with the help of user information. For instance the account number, bank card number and IP-address from the user that initiated the transaction are recorded. Because a lot of banks still work with account managers that a client can call to perform transactions, also these phone calls are recorded for the purpose of non-repudiation. One bank states that the only way the bank could be sure that a transaction is really initiated by the user is with the help of user authentication when setting up a connection. As described earlier this can be implemented with the help of smart card technology.

What would be the reaction of the users of the online banking system to the consequences an availability attack has for the system? What could be good indicators for the impact such an attack has for these users?
The respondents indicate that the private banks are thinking in terms of hours and percentage of up time when talking about the availability of online banking systems.

With the regard to the downtime of the online banking system the respondents think in general users will think an outage of a couple of hours is a mere inconvenience. In contrast when an online banking system is not available for more than 24 hours clients will be less happy. To users of a level 2 online banking system this would not immediately lead to a decrease of trust in the system if such incident is occurring rarely. However, when a level 3 system is unavailable for more than 24 hours this would have more impact on the user's trust. Also when such incidents are happening more frequently users are unhappy about the system and can think of stop to use the system or even leave the private bank. The respondents of both the level 2 and 3 systems think users will understand scheduled downtime because of for instance maintenance. The respondent of the private bank with a level 3 bank said that the most important function of IT-security measures regarding the availability is that the system is kept up and running during attacks.

A less important issue is having problems with the response time of the system. Users will not turn their backs to the system easily when the site is slow but will see this as an inconvenience. Both the respondents with level 2 and 3 systems think that response time is less important for users than the availability of the system. Also, in the case of performance problems due to an availability attack this effect would be stronger with a level 3 system than with a level 2 system because level 3 users would perform more operations.

6.3.6 Validating the chosen fuzzy variable for reputation loss

How important is the reputation of your bank? Which factors determine the reputation of a private bank?

All the banks think the reputation of the bank is the most important thing a bank can have in the private banking sector. A lot of client relations are based on the trust there is between the bank and the client. Two respondents think that when banks are targeting at more wealthy clients the reputation of the private bank becomes more important.

One respondent stated:
"It is very important to monitor the reputation of our bank when positive or negative events occur. For instance for a private bank it is important to know how many clients are leaving the bank because the bank's reputation has decreased in the perception of the client. "

Another respondent stated the evanescence of the reputation of the bank as following:
"*Trust comes by foot and goes with horse speed"*

What are the consequences of reputation loss?

The five respondents have mentioned different four consequences of reputation:

1. Clients are leaving the private bank and are stepping over to their competitors.
2. The continuity of the company could be in danger if clients don't want to do business with the bank anymore.
3. Potential clients will not be acquired as new clients.
4. There will be a lot of costs of repairing the reputation be involved with an incident which damages the bank's reputation. A good example of such costs is the extra marketing and promotion costs of again establishing the company name as trustworthy.

How can reputation loss be measured?

All respondents think the number of clients leaving their bank when a security incident has occurred is a good indicator for reputation loss. By cumulating the capital under

management of the clients which will leave their bank, the lost capital under management due to an IT-security incident can be calculated. All banks know what the average return percentage on their capital under management is and they can therefore calculate the lost revenue. Such a financial indicator for security incidents can translate something fuzzy like client trust in an online banking system to something concrete like the loss of income.

6.3.7 Validating the relation between IT-security incidents and reputation loss

What is the order of importance for the user of the online banking system of the CIA aspects?

All respondents of banks with a level 2 system think their priority list regarding the CIA aspects of their online banking system is:

1. C
2. I
3. A

The reason for this classification according to the respondents is that if the relation of trust is broken by a security incident which compromises confidential user information, the reputation of the bank is damaged the most. After this integrity issues could have the most impact to the private bank's reputation. Some respondents do think the order of importance can be different if a level 3 system is in place. Incidents which have an impact on the availability of the online banking system are regarded as the least important because clients can only access account information.

The order of importance of the CIA aspects is different when a level 3 system is in place. The respondent of the only private bank which has a level 3 online banking system in place mentioned the following order:

1. I
2. C
3. A

The reason for this classification according to the respondent is the fact that in a level 3 system also transactions can be made. Clients will lose the most trust in the system when the possibility for attackers to perform unauthorized transactions exists. Clients will also lose trust in the system when sensitive information of the client is compromised by an integrity attack but this does not involve financial loss for the client. In addition a level 3 system will more likely be the subject to an integrity attack because attackers can have more benefit from such attack. On the third place comes the availability of the system. The respondent thinks users find it very inconvenient when the system is unavailable but will less likely result in a decrease of user's trust in the system than integrity and confidentiality issues. In addition the correspondent thinks that the availability of a level 3 system is more important than for a level 2 system because there could be time constraint to certain transactions.

All respondents think the degree in which clients lose their trust in the system could dependent on certain client characteristics. For instance if a client is an important public entity even in level 3 systems the client could think a confidentiality incident could be more severe than an integrity attack.

Are there other factors which could have influence on the amount of reputation loss caused by an IT-security incident?

The respondents indicate that the following other factors could influence the amount of reputation loss encountered by a private bank when a security incident has occurred:

- The reaction of clients which are victim of the incident. The problem then is that it is very difficult to predict client reaction because this depends for a part on the personality of the client.

- Media attention. If a security incident has occurred, media attention could increase reputation loss because other users of the online banking system will become aware of the incident. In this way even if these clients were not a victim of the incident, users of the system can lose trust in the system. First the type of media which publishes the incident could have an impact on reputation loss. If the news is brought by the daily newsflash on television the news gets more exposure than if it is published as a little article in an unknown newspaper. Because of the increasing news delivery via new media such as news postings on the Internet, the news of a security incident could get a lot of attention fast. Second the time in which the incident has occurred is also important. If there is a more important news item, the incident could get less attention than in times in which all media are waiting for something to occur which they can publish.
- The extent to which the private bank can react to the news of an incident. Private banks could decrease the reputation loss caused by security incidents by informing their clients of the incident in a good manner.
- Other problems occurred in the past or at the same time at the private bank could enhance the reputation loss gained by a security incident. If the bank is in the news because of bad performance and a news report about a security incident comes on top of it the bank can encounter considerable reputation loss.
- Regulators and supervisors of the financial sector are more aware of incidents happening at private banks. For instance the AFM has recently decided to publish shortcomings and incidents in the online banking systems of among others private banks in order to inform the public.

6.4 Discussion

Out of the answers to the interview questions described in this chapter first it can be said that the proposed private banking market is becoming more competitive because also the retail banks are increasingly trying to get a share of this lucrative market. Because of this increased competition the banks are more and more competing on basis of the quality of the delivered services. Because of the increased competition the revenues will decrease while the costs are increasing because of the increasing service level offered to the client. These answers are corresponding with the findings out of the literature study in chapter 2.

Because of the increasing competition on basis of service delivery more and more banks are offering online banking systems. Four out of the five banks which were interviewed had a level 2 system. Just one bank had a full service level 3 online banking system, this in contrast to the Dutch retail banks which all have level 3 systems. Reasons for the private banks for implementing level 2 online banking systems are the fact that a lot of clients are internationally active and because clients are asking for this functionality. Banks also mentioned the cost savings such a system could provide and the competitive disadvantage they could have should they not implement such a system. The main reasons for the private banks not to implement level 3 systems are the fact that the target client group does not require that level of functionality, the higher costs, and increased risks such a system would cause. It must be said that this could be an old-fashioned approach to a highly automated market. To illustrate this, the argument given by the private bank with a level 3 online banking system was that offering a level 3 system could give a private bank competitive advantage as clients do not need to open a separate account at a mainstream bank in order to perform online payment transactions. When staying behind could give private banks with a level 2 online banking system a disadvantage, these banks are advised to reconsider their position.

In order to secure their online banking systems private banks are using firewalls, IDS systems and other network measures in order to divide the company network into compartments. Also, they have duplicate implementations of systems available. All banks

are using SSL connections to protect against sniffing attacks. Despite this, three out of five banks are still only using single factor authentication while multi-factor authentication is recommended. Two-factor authentication is mostly implemented by using a card reader or a token. This solution offers authentication by something a user knows in combination with something the user has. Such a system can be professionalized with the help of smartcards and user certificates. In this way also man-in-the-middle attacks can be ruled out. Also non-repudiation of user transactions can be ensured in this way. New implementations of three-factor authentication in which smartcards can be combined with authentication by something a user is, are coming up. An example of such an implementation is a system that can call the user in order to recognise the user's voice before it gives the authorisation to perform transactions can be made. With the help of all the above and in chapter 3 mentioned IT-security measures it is possible to construct a online banking system which is secure to most of the summed up IT-security incidents mentioned in chapter 3. Therefore it is not the lack of proper measures which causes private banks not to be secured against such attacks. The private banks themselves chose not to implement the highest security standards because of other reasons such as the high costs, the difficulty of implementation and the organisational pressure such measures would give. The banks do not implement the most advanced IT-security measures because the think the benefits of such measures will not be exceed the costs of implementing them. The benefits mentioned are mostly explained with the help of qualitative arguments. In addition, the need for IT-security measures is mostly justified with the help of telling which security threats else would stay unaddressed. In this way the investments are argued with the fear of incidents which can happen without them instead of performing a quantitative cost-benefit analysis. The proposed reason for this could be the fact it is much easier to argue the use of a security measure by telling which incidents it would prevent than it is to define the exact benefits such measure has. Another reason a private bank could have not to implement the most secure measures is the fact the stakeholders are not asking for more security.

In the light of the increased competition and the cost savings which are a result, IT-security investments will be more difficult to justify in the future. If for instance a better firewall is proposed it is likely the added value of the new firewall compared to the old one must be shown. In this way the quantification of the benefits of IT-security measures will be unavoidable in the future when the recent market trends will hold. In addition the users of online banking systems are becoming more aware of the risks of such systems and are increasingly demanding proper measures implemented by their private bank. A good example of this was the story the respondent of the bank with a level 3 system told about a group of potential clients that only would do business with the bank if they could prove their online banking system was secure. In order to assess the in place security measures at the private bank, the group of potential clients brought their own security expert with them. These two conclusions indicate that in the nearby future more business cases for IT-security investments will be available. Until that time it is unlikely private banks will use pure quantitative terms. This picture is confirmed by the answers of the respondents which indicate that methods for the quantification of the benefits of IT-security measures could enhance the qualitative arguments used to justify the investments in IT-security but could not replace these arguments.

With regard to the attacks defined in figure 25 the respondents do acknowledge the categorisation of these attacks and there occurrence in general. However no attacks seem to occur at the private banks according to the respondents. For instance phising attacks are acknowledged as the major security issue for online banking systems at this moment, but the respondents all say they have not encountered such attacks in the past. The reason mentioned for this is the relative unfamiliarity of attackers with the private

banks. Also, the private banks themselves think they are a too little fish to catch. Malicious code and exploits are sometimes present in the systems but with the help of good patching policy and the installation of virus scanners and firewalls these cannot cause a threat to the system. The seldom occurred deviations of account balances in the past all had an internal cause, such as mistakes made by the system or the employees. Three of the five banks think that they can hardly influence the occurrence of DDoS attacks. Availability issues which did occur were problems with hard disk failure, backups and power outage. This indicates that most availability problems are caused by internal problems with security and management of the online banking systems. It must be pointed out that it is not sure to what extent the respondents do not mention IT-security incidents that do occur. The design of this research was also not suitable to get detailed information of the actual occurrence of such incidents. Also, the proposed relation between IT-security incidents (via the impact these incidents have to the CIA aspects) and reputation loss is confirmed by the respondents. In addition, the proposed indicators “service outage”, “decrease of performance”, “security level of disclosed information”, “the financial impact of unauthorized transactions” and the indicators describing the scale of the attacks to the integrity and confidentiality were confirmed by the respondents. With regard to the integrity of the online banking system it can be concluded that non-repudiation is not an issue for the client for the reason that it is common in the financial sector that this is not provided to the client. For the bank’s internal processes it is very important when things go wrong, but clients do not lose their trust in the system as they have an advantage when a transaction is reputable. Last but not least the respondents state that the reputation of their bank is the most important asset and the “loss of capital under management” is a good indicator to measure reputation loss.

Chapter 7: Summary and conclusions

7.1 Introduction

In this chapter the conclusions regarding the research questions defined in paragraph 1.3 are given. These conclusions sum up the knowledge gained out of the literature and the empirical research conducted. The highlight of these conclusions is the concluding model in figure 26. Finally, some suggestions for further research are given.

7.2 Research conclusions

The private banking market is highly competitive and dynamic

For private banks current clients, potential clients, employees, and sector regulators and supervisors are important stakeholders. The most important stakeholder is de current client as business income and earnings are the direct result of doing business with these stakeholders. Furthermore, mergers and acquisitions are performed frequently in the financial sector. Despite this, three of the five banks that were interviewed are independent private banks. Private banks seem to think that being independent causes private banks to stay more focused towards a certain group of clients that can be served with specialised products and services. The competition in the private banking market consists of the interviewed specialised private banks, the four big retail banks (ING, ABN-AMRO, Fortis, Rabobank) and for stock exchange service the new Internet banks Alex and Binq. For the private banks the retail banks are the most feared competitors due to their economies of scale and their broad portfolio of financial products and services. Due to the high margins of private banking products and services a highly competitive field exists and the competition is still increasing. In order to compete with the retail players and the online brokers the private banks are investing in mergers and acquisitions in order to obtain extra expertise. In addition, the private banks try to attract potential clients by the quality of service and the attention the specialised banks can give their clients. Because of the increasing costs of the abovementioned initiatives, reorganisations and cost cutting programs are initiated as well in order to save costs. Other trends in the private banking sector include the increased transparency of products and services, the client demand for stable portfolios and the increased regulations and supervision in the sector.

Private banks with level 2 online banking systems are missing opportunities

As can be seen out of the respondents' answers there are not a lot of banks which have implemented a level 3 online banking system. A level 3 online banking system therefore could give a competitive advantage because clients will not be forced to hold a payment account at one of the retail banks. When more private banks will upgrade from level 2 to level 3 online banking systems, the banks that not upgrade their system will have a competitive disadvantage.

No IT-security incidents seem to occur

Regarding the occurrence of incidents at private banks it can be said that according to the interviewed private banks the frequency of external attacks on the confidentiality, integrity or the availability of the online banking system is negligible. This despite the fact the banks acknowledge the fact that there is an increase of security attacks and threats on the Internet. It is unknown if the respondents where not talking about the occurred incidents, the respondents do not know if incidents are occurring or incidents really do not occur.

Experts think a method which combines the advantages of qualitative and quantitative approaches to the calculation of the benefits of IT-security measures is helpful.

IT-security investments are mostly justified based upon qualitative arguments. The need for IT-security measures is motivated by mentioning the threat which must be addressed with these measures. The experts at the private banks think quantitative methods which measure the benefits of IT-security investments can help to justify IT-security investments but can not replace the qualitative arguments. By quantifying (even if this is not very precisely done) the benefits of IT-security measures external data can confirm the use of these measures that is expressed with qualitative arguments. A problem then is the fact private banks do not have enough information about the security risks in online banking systems in order to quantify these benefits. For these reasons a fuzzy model can be the solution. First a fuzzy model can translate qualitative linguistic terms into quantitative measurable terms. Second because a fuzzy model is based upon cumulative expert knowledge no huge amounts of security statistics are needed in order to make a model which can quantify the benefits of IT-security investments. An important final remark to the fuzzy model is the fact there must be an expert feeling of which linguistic term can be mapped upon a range of quantitative terms. As can be seen in with this research this could me hard because the experts must be selected with care in order to get enough information to construct a fuzzy model.

The resulting fuzzy model

The goal of this research was to describe the relation between IT-security incidents and reputation loss and to explore ways to model this relation. Out of the proposed fuzzy model in figure 25 in combination with the interview answers the respondents gave, the resulting fuzzy model is constructed that is displayed in figure 26.

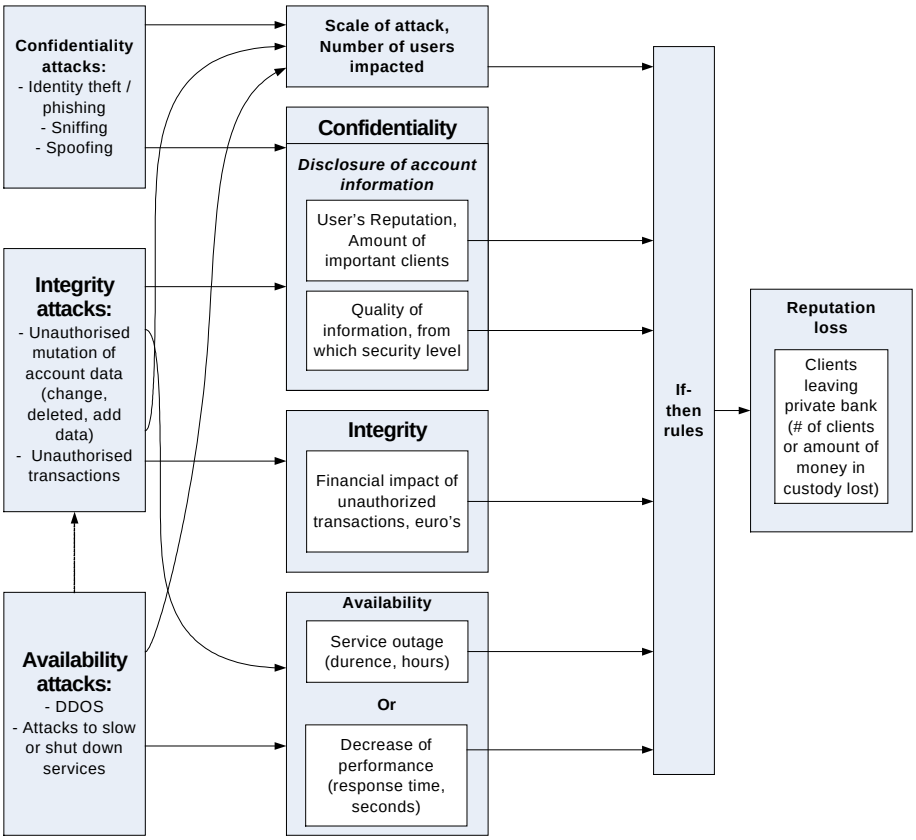


Figure 26: Resulting fuzzy model

The proposed indicators for the impact of IT-security incidents to the availability of the online banking system, i.e. “Service Outage” and “Decrease of performance”, are confirmed to be good indicators. Because the non-repudiation of transactions and account data is not an issue for the clients the indicators that can be seen in figure 25 for the non-repudiation were deleted as can seen in the resulting model. For the impact of incidents on the integrity of the system the indicator “financial impact of unauthorized transactions” is supposed to have a direct positive effect to the probability of clients leaving the bank and therefore stays in the concluding model. Also the security level of the information which is disclosed is confirmed to be an indicator for the impact of incidents to the confidentiality of the system. Another indicator that is regarded to be important to model the impact to the confidentiality an incident has, is called “User’s Reputation”. This indicator describes that if the information of a more important and public client is disclosed, it is more likely this incident will get media attention and therefore would influence the amount of reputation loss. The indicator is measured with the help of the number of important clients a private bank has.

The “number of unauthorised transactions” and “Quantity of information” were only regarded to be of importance for the probability of media attention for the incident. According to the respondents the client will lose trust in the system because the incident is happening and it is not important anymore what the scale of an attack is. Because of this finding the two earlier mentioned indicators for the scale of certain attacks could be combined into one indicator called “Scale of attack”. This indicator is measured with the help of the number of users which are victim of a certain IT-security incident.

Despite the fact the respondents were not able to construct the membership functions and the IF-THEN rules they could express the priority of the CIA aspects in the perception of the client. For a level 2 system, the confidentiality of the online banking system is regarded as the most important aspect because this system is expected to secure the user’s information and this is in essence the basis of the private banking sector. The integrity of the system comes at the second place because clients will lose their trust in the system when they observe a mistake in their account balance or made transactions but such a mistake would not be as severe as the disclosure of confidential information. On the third place stands the availability of the system because users will be dissatisfied when the online banking system is unavailable or not performing well but this is regarded as less important than the confidentiality and integrity of the system. With regard to these indicators it is thought that the availability is more important than the performance of the system.

For a level 3 system, the order of priority of the confidentiality and the integrity of the system is exchanged because a level 3 system has online payment functionality. Therefore these systems are more vulnerable for integrity attacks and users do have higher expectations with regard to the security of this aspect. In addition, despite the fact the availability of level 3 online banking systems is also on the third place it is regarded as more important than at level 2 banks. When clients cannot perform payments because the system is unavailable this has a larger impact than a client which cannot get account information out of a level 2 system.

The conclusion which can be drawn out of these findings is that the indicators and the relations mentioned in figure 25 can be used for both level 2 and 3 systems. The membership functions for level 2 and 3 systems will differ and therefore these must be constructed separately.

Best practice IT-security solutions do exist.
As can be seen in this research best practices do exist in order to secure the online banking systems. The only drawbacks for such highly secure systems are organisational aspects and the high costs of such implementations. The banks are mentioning that the network security is getting a commodity and therefore is no problem. The most encountered security problems are in the application security and the organisation of security. Finally private banks are investing resources in order to be compliant with new regulations. Private banks are increasingly cooperating with regulators, supervisors and even other private banks in order to get more grip and information on the security of online banking systems. These facts are indicating that the safety of online banking systems will continue to increase in the nearby future.

7.4 Suggestions for further research
Regarding to the model in figure 25, this research has validated the attack categories, the indicators which must be used for the impact of these attacks to the CIA aspects and the indicator for reputation loss. In order to construct the membership functions and IF-THEN rules as described in paragraph 5.4 other information is needed. The experts interviewed at the private banks did not know to which extent clients would leave the bank when a certain attack occurs. The reason for this is that they did not know the opinion of the clients about the impact of IT-security incidents on the indicators for the CIA aspects. This problem could be solved by frequently asking a group of clients questions about the indicators of the CIA aspects. Also, for the private bank it is important to know for which combinations of impacts for the CIA aspects clients would leave their bank. This knowledge can be obtained by asking clients about the reasons they had to leave the bank. With this data the membership functions and IF-THEN rules can be constructed. In this way the relation between IT-security incidents and reputation loss is modelled and quantified. After this step typical cases of reputation loss caused by certain IT-security incidents can be constructed. For each typical case the private bank can assess with the help of the fuzzy model how much reputation loss would be the result. The last step would be to influence the indicators in a positive way in order to decrease the resulting reputation loss. This can be done by reasoning which IT-security measures are needed.

In the above mentioned manner a fuzzy model can be created that can help IT-security managers to show the need for security measures in online banking systems at private banks. Managers can justify the need for measures by showing how much damage an incident could cause without these measures. In the end the manager can justify which IT-security measures must be selected with the help of qualitative terms which can be enhanced by the proposed quantitative savings coming out of the fuzzy model.

Appendix A: PricewaterhouseCoopers

A.1 Introduction

This research is conducted in combination with an internship at PricewaterhouseCoopers (PwC) Netherlands at the department Security & Technology. The experts working in this department have played a significant role in the formation of this research. Next some general information about PwC International, PwC Netherlands and last but not least the department Security & Technology.

A.2 PricewaterhouseCoopers International

PricewaterhouseCoopers refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. As a global organisation, PricewaterhouseCoopers has member firm offices in 769 cities in 144 countries. The aggregated net revenues over fiscal year 2004 (ending 30 June 2004) were USD 16.3 billion. The organisation today consists of about 122,000 people.

PricewaterhouseCoopers has been created by the merger of two firms - Price Waterhouse and Coopers & Lybrand - each with historical roots going back some 150 years. Set out below are some key milestones in the history of both firms:

- 1849 Samuel Lowell Price sets up in business in London
- 1854 William Cooper establishes his own practice in London, which seven years later becomes Cooper Brothers
- 1865 Price, Holyland and Waterhouse join forces in partnership
- 1874 Name changes to Price, Waterhouse & Co.
- 1898 Robert H. Montgomery, William M. Lybrand, Adam A. Ross Jr. and his brother T. Edward Ross form Lybrand, Ross Brothers and Montogomery
- 1957 Cooper Brothers & Co (UK), McDonald, Currie and Co (Canada) and Lybrand, Ross Bros & Montgomery (US) merge to form Coopers & Lybrand
- 1982 Price Waterhouse World Firm formed
- 1990 Coopers & Lybrand merges with Deloitte Haskins & Sells in a number of countries around the world
- 1998 Worldwide merger of Price Waterhouse and Coopers & Lybrand to create PricewaterhouseCoopers

A.3 PricewaterhouseCoopers in the Netherlands

The Dutch member firm of PricewaterhouseCoopers consists of more than 4000 staff members and offers the full range of PricewaterhouseCoopers services from 19 offices in the Netherlands for multinational, big national but also local companies in the middle market. Also services are provided for local, regional and national governments and non-profit organisations.

The core values of PwC Netherlands are:

- Connected thinking, in which by connecting knowledge which is present at a lot of different people in a lot of expertises at PwC is trying to provide innovative a valuable solutions for their clients.
- This knowledge must be shared as well internally with the professionals of PwC as externally with their clients.
- PwC strives to return a better performance of service than the client expects and is always willing to take the responsibility for the quality of provided services.

Since 1 January 2005 PwC has restructured their organisation to reflect the main lines of service knowing Assurance, Advisory and Tax & Human Resource Services with the following characteristics:
- The Assurance department provides companies with assurance about their financial performance. This includes conducting audits and providing advice on topics as how to fill in the financial accounting principles and new developments such as the Sarbanes-Oxley act and the International Financial Reporting Standards (IFRS) standards.
- Advisory consists of approximately 350 staff members. A large number of Advisory staff has broad knowledge of IT audit and risk management.
- Tax & Human Resource Services. The Tax department provides advice about tax regulation and helps to fill in fiscal reporting principles. Therefore the professional working at the Tax department have both broath knowledge about the financial and legal aspects of the Dutch tax system. The Human Resource Services department helps companies to add value to their HR processes.

A.4 PricewaterhouseCoopers Security & Technology
Within the service line Advisory the department Security & Technology is present. This group consist of 17 specialists under the supervision of Tonne Mulder and Otto Vermeulen that focuses completely on technical IT security advice and audit. Also one of the supervisors for this thesis and research, Frans van Buul is part of the department Security & Technology.

The Security & Technology department provides the following services:
- Audit / review. S&T can conduct a security audit as independent assignment.
- Support. S&T provide support regarding IT-security and technology in a broth sense as part of services provided by other departments of PwC (this is what is been meant with connected thinking).
- Identity Management. S&T can provide advice about how the management of user account present at information systems can be optimized.
- Privacy. S&T provide advice and audit services regarding the privacy of personal information about employees or clients of companies.
- Penetration test. S&T can perform penetration test in which they are pretending they are hackers with the goal to assess the quality of the in place IT-security measures and give advice about this.
- Sarbanes-Oxley. S&T can provide support regarding the implementation of the Sarbanes-Oxley act at companies and what IT controls and security must be in place to be SoX compliant.
- Security Management. S&T can give companies advice about how to set up a security policy and how to organise IT-security. Also the compliance with security standards such as ISO17799 fall into this category.

Some of the contracts that were executed by the Security & Technology group over the past year are described below.
- Providing IT audit support as part of the financial audit for more than fifteen organisations.
- Assisting two international organisations (a United States based financial institute and a Thai telecommunications operator) with BS7799 compliance.
- Assisting several Dutch public sector organisations with the design of Public Key Infrastructures.
- Performing network security reviews and penetration tests for organisations in financial services, energy & utilities and public sectors.
- Performing risk assessment and audit for a newly designed, large scale electronic payment system in the Netherlands.

- Assisting in achieving Sarbanes-Oxley 404 compliance in financial services and consumer products organisations.
- Auditing privacy compliance for more than 20 Dutch municipalities.

Appendix B: Regulatory IT-security requirements for online banking systems

B.1 ROB

The ROB concentrates on four key elements (De Nederlandsche Bank 2004):

1. Risk control
2. Organisational measures
3. Information and communication
4. Assessment and judgement

The ROB tries to make recommendations which banks must apply to protect themselves against risks which could damage the financial performance, financial position, business continuity and reputation of the bank.

IT-security risks which could cause the damages described above and recommendations to prevent these damages are set out in the ROB. The following IT risks are defined:

1. Strategic risk. The risk of shortcomings in respect with the tuning of the strategy and the implementation of the strategy.
2. Control risk. Insufficient adaptation and maintenance of IT.
3. Risk of exclusivity. Insufficient protection against unauthorised access to the systems.
4. Integrity risk. Information is not correct, complete or on time.
5. Audit risk. IT- control instruments are not in place.
6. Availability risk. IT is not available in a sufficient manner.
7. User risk. IT is not correctly used.

In Article 57 the ROB gives some IT-security requirements:

- Specific IT-security measures must ensure that the exclusivity and integrity risks are minimised.
- If IT is used to perform electronic transactions banks should spend extra attention to secure these transactions.
- With regard to the technical verification and protection measures banks should implement so called “sound practices”.
- With regard to the availability of electronic banking systems, banks must ensure the availability of the mentioned systems by implementing IT-security measures such as back-up and recovery procedures and emergency plans or the redundant implementation of important systems.

B.2 Basel principles for managing risk in online banking

The Basel committee categorised 14 key risk management principles into three categories to which financial institutes like private banks must implement in order to mitigate IT-security risks. (Basel Committee on Banking Supervision 2003; Glaessner et al. 2002).

Risk management challenges (principles 1 to 3)

1. Management oversight. Effective management oversight of the risk associated with e-banking needs to be in place, and online banking risk management should be integrated with the overall risk management
2. Management of outsourcing and third-party dependencies. Comprehensive, well-defined, ongoing oversight is needed for managing outsourced relationships and third-part dependencies supporting online banking, including prior due diligence.
3. Appropriate measures are needed to ensure proper segregation of duties in online banking systems, databases and applications.

Security Controls (principles 4 to 10)

4. Appropriate authorization measures and proper controls need to be in place for online banking systems, databases, and applications.
5. A clear audit trail is needed for all online banking transactions.
6. Banks should authenticate the identity and origin of all entities, counterparts and data transmitted over the Internet. Failure on the part of the bank to adequately authenticate clients could result in unauthorised individuals gaining access to online banking accounts and ultimately financial loss and reputation loss to the bank through fraud, disclosure of confidential information or involvement in criminal activity.
7. Non-repudiation should be ensured to hold users accountable for online banking transactions and information. This must be done by ensuring the non-repudiation and accountability for online banking transactions.
8. Comprehensive security control. Banks should ensure the appropriate use of activities and properly safeguard the security of online banking assets and information.
9. Integrity of transactions, records, and information. Banks should prevent unauthorized changes to and ensure the reliability, accuracy and completeness of online banking transactions, records and information. Data integrity refers to the assurance that information that is in-transit or in storage is not altered without authorisation. Failure to maintain the data integrity of transactions, records and information can expose banks to financial losses as well as to substantial risk to legal action and reputation loss. Common practices used to maintain data integrity within an online banking environment include the following:
    - Online banking transactions should be conducted in a manner that makes them highly resistant to tampering throughout the entire process.
    - Online banking records should be stored, accessed and modified in a manner that makes them highly resistant to tampering.
    - Online banking transaction and record-keeping processes should be designed in a manner as to make it virtually impossible to circumvent detection of unauthorised changes.
    - Adequate change control policies, including monitoring and testing procedures, should be in place to protect against any online banking system changes that may erroneously or unintentionally compromise controls or data reliability.
    - Any tampering with online banking transactions or records should be detected by transaction processing, monitoring and record keeping functions.
10. Appropriate disclosure. To avoid the risk of legal action and reputation loss, banks should have adequate disclosure for online banking services. Confidentiality is the assurance that key information remains private to the bank and is not viewed or used by those unauthorised to do so. Misuse or unauthorised disclosure of data exposes a bank to both reputation and legal risk. To meet these challenges concerning the preservation of confidentiality of key online banking information, banks need to ensure that:
    - All confidential bank data and records are only accessible by authorised and authenticated entities.
    - All confidential bank data is maintained in a secure manner and protected from unauthorised viewing or modification during transmission over public, private or internal networks.

- The bank's standards and controls for data use and protection must be met when third parties have access to the data through outsourcing relationships.
- All access to restricted data is logged and appropriate efforts are made to ensure that access logs are resistant to tampering.

Legal and Reputational Risk Management (Principles 11 to 14):

11. The confidentiality of client information and adherence to client privacy requirements should be ensured. Banks generally have a clear responsibility to provide their clients with a level of comfort regarding information disclosures, protection of client data and business availability that approaches the level they would have if transacting business through traditional banking distribution channels.
12. Business continuity and contingency plans to ensure the availability of systems and services. Plans should ensure that online banking systems and services are available to clients, internal users, and outsourced service providers when needed. Incident response plans should be in place to manage and minimize problems arising from unexpected events, including internal and external attacks that hamper the provision of online banking systems and services.
13. Bank supervisors should assess banks' management structures, practices, internal controls, and contingency plans for e-banking.
14. Banks should have an in place incident response planning in order to react on security incidents in a well manner.

Appendix C: IT-security measures for online banking systems

C.1 IT-security measures against confidentiality attacks

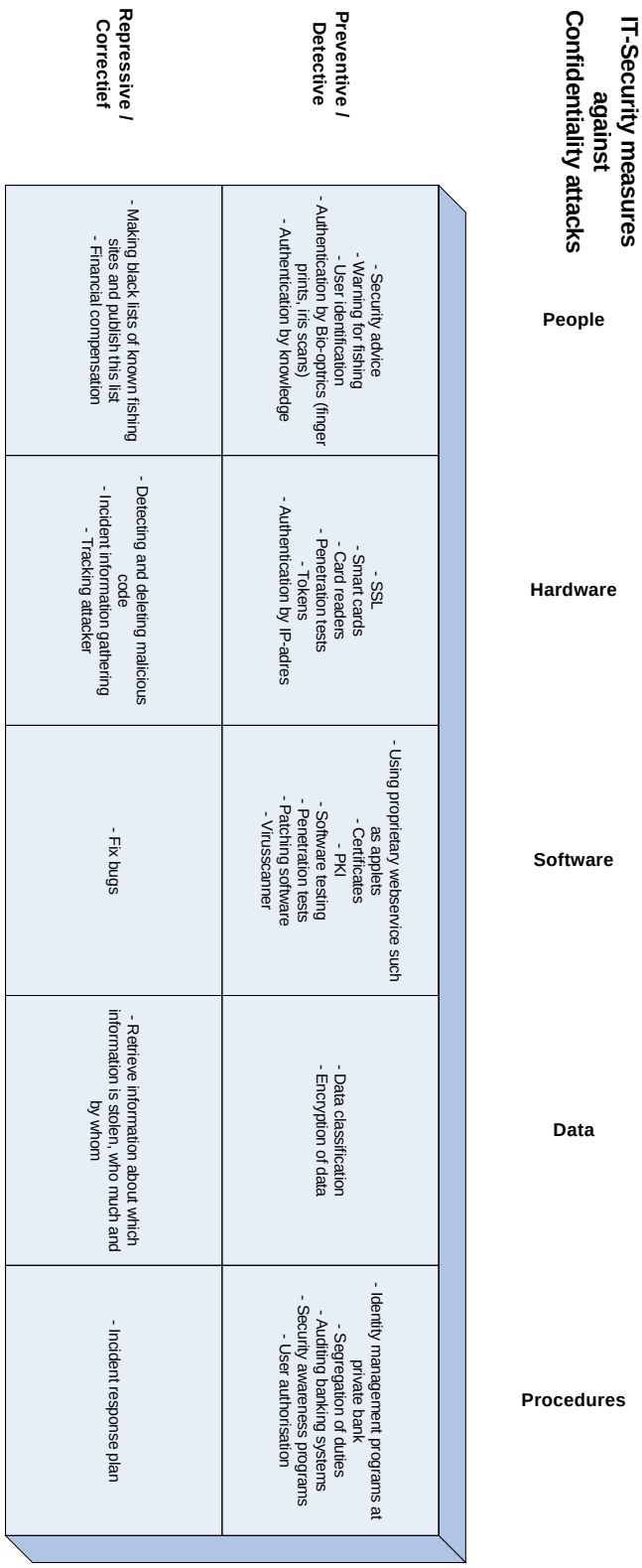


Figure 27: IT-security measures taken against confidentiality attacks

User identification and authentication
In online banking systems often a user ID which the bank has defined is used. This could be a combination of account number and expiration date of the bank card or a random user ID created by the bank. In this way straightforward such as the users name are ruled out.

Banks often use the something users know or something the users have principle. The bio-optics are very expensive. Often also tokens and smartcards are very expensive. Therefore the most used authentication mechanisms in online banking are passwords and card readers. If passwords are used these are mostly passwords which users themselves create. With the help of card readers a challenge-response mechanism can be made. The bankcard is inserted into the card reader and the user must enter his or her PIN, which is the same as the PIN which is used at the ATM. The card reader then makes a unique code which must be entered in to the online banking website. This is what called two-factor authentication, a combination of something a user has (the bank card and the card reader) and something the user knows (the PIN). In this way the user does not have to enter his or her PIN on the PC and the PIN is therefore safe for key logging software. Furthermore one time passwords are used.

Data classification
To ensure the confidentiality of the online banking systems at private banks it is very important to know which data is present in the system and how important that data is. The purpose of data classification is threefold. First it is important to know which data is present in the online banking system. Second it is important to evaluate which impact the loss, damage or disclosure of certain data out of the system is. The impact of such incidents could include a negative influence on the bank's operations, reputation and profitability (OCC 1998). When the priorities of importance of data in the systems are set, the proper security measures could be implemented. For the classification of data at private banks the following classification could be used (Overbeeke et al. 2003; Weise and Martin 2001):

- Top secret or Secret. Examples of such data could be proprietary company data or confidential company data. Proprietary data is data which has an economic value to the private bank. Because of this, if this data is disclosed the information stored in this data will lose its economic value with financial loss as a result. Confidential company data is data which must be protected against disclosure regardless of the economic value of this data. For instance this could be data which a company is obligated by law to protect from disclosure
- Confidential or restricted data. An example of such data is confidential client data which can only be access by specific authorized internal or external entities. An account manager of a private client is an example of an internal entity which is authorized to access account information of that client. Furthermore of course the client himself (as the only external entity allowed having access) is authorized to access his account information.
- Unrestricted. An example of such data could be public company data about the private bank. Any external or internal entity could access this data.

SSL and PKI
There are many different methods of encrypting data with different types of algorithms. The scope of this thesis restrains from mentioning all these methods. To ensure attackers can not eavesdrop for data send via the Internet from the user's browser to the private banking systems in most cases the HTTPS protocol is used. Often the SSL (Secure Socket Layer) protocol is used. The use of the SSL protocol to set up a secure channel for data exchange between the user and the private bank had two major advantages. First

data is kept secret and second tampering with this data is detected. In this way SSL can be a solution against confidentiality and integrity attacks (Claessens et al. 2002). For the authentication of the communication partners a so called certificate is used. A certificate usually contains the following information: the identity of the certificate holder, the public key of the certificate holder, the identity of a Certification Authority, expiration date of the certificate (Overbeeke et al. 2003). A certificate states that a bank is the bank it claims to be. To ensure this a so called PKI (Public Key Infrastructure) is needed. A Certification Authority assesses the identity of the bank and when it thinks the identity of the bank is ok the CA signs the certificate. The identity of the CA is ensured by a root CA. In this way a so called certification path exists of organisations which ensure each others identity (Glaessner et al. 2002; Overbeeke et al. 2003). Some problems with SSL and the PKI are defined by (Santos 2000):

- Users don't check certificates. In order for a user to be sure a secure channel is set up with a website from the private bank, the user must check the certificate for identity information. In practice internet browsers are making it easy for users by automatically accepting certificates with certain signatures.
- Anybody can apply for a certificate and receive one.
- The user doesn't have to authenticate with the use of a certificate although the option is present.

After the handshake in which the user must accept the certificate of the bank (the user acknowledge that he or she knows the bank is the bank which it claims to be) the connection between the user's browser and the web server of the bank is encrypted. The purpose of the handshake is three-fold: the user and the bank need to agree on a set of algorithms to encrypt the data, the bank can authenticate itself and to agree on the keys used for encryption (Claessens et al. 2002).

C.2 IT-security measures against integrity attacks

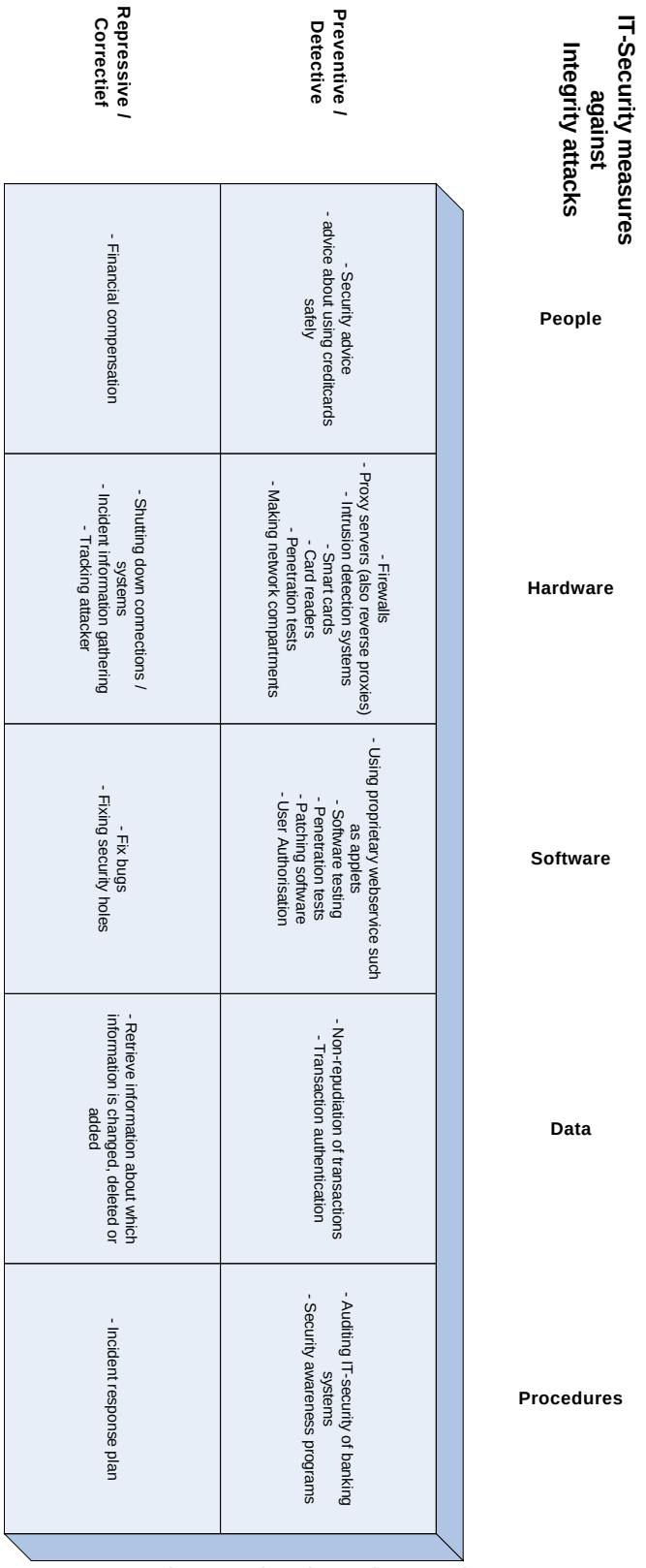


Figure 28: IT-security measures taken against integrity attacks

User authorisation

In order to be sure no unauthorised transactions could be performed authorisation schemes are implemented. First some roles in the system are assigned. Second for each role it must be determined which access rights to data in the online banking system are needed. After this certain employees at the private bank could be assigned with certain roles. The in paragraph 3.5.1 described segregation of duties must be implemented in order to prevent conflicts of interest.

In general two kinds of access principles can be distinguished:

1. Discretionary Access Control (DAC). With this approach user's can give and take away access rights to other users. When using the DAC principle groups of objects and persons are defined in such a way that when a person has access to a file in a certain group the person can also access other files which are in the same object group. Furthermore a person in a certain group has the same access rights to certain objects as the other members of the group. The DAC principle has two major shortcomings. First the access rights to files are not granted by a central identity at the private bank, instead this is these rights are given by the owners of the files. Second malicious code could copy the access rights to itself in order to have the same access rights as the user of the files (Overbeeke et al. 2003).
2. Mandatory Access Control (MAC). This principle doesn't allow users to grant access rights. To implement the MAC principle first all files and persons are classified in one of the following categories: "top secret", "secret", "confidential", "restricted" and "unrestricted". An example of an access rights system based on the MAC principle is the Bell LaPadula model which is based upon two rules. The first rule is that a person can only access files with an equal or lower security clearance (also called the "no-read up property"). The second rule is that a person has no rights to write to files with a lower security clearance (also called the "no write down property"). In this way malicious code can not write to data with a lower security clearance (Overbeeke et al. 2003).

Firewalls

In general three types of firewalls can be distinguished:

1. Packet filter firewalls. This type of firewall allows traffic to pass trough to the private bank's internal systems on the basis of the verification information which is situated in the header of an IP-package. In networks which use the IP-protocol data is send in packages with a certain destination (IP-address). In the header of an IP-package also verification information about the source and other properties of the sender and the data send. On basis of the verification information the firewall consults a table with filter rules if the data may be passed through to the internal network. Some firewalls filter on basis of the application protocol which is used. This method of filtering is called "state full inspection" and in that case the firewall will also record which connections are active (Overbeeke et al. 2003).
2. Proxy firewalls. These firewalls are also called application gateways. Such a firewall intercepts the application session and determines on basis of defined filter rules if the application session is allowed. A special application in the firewall called a proxy will set up the actual connection with the private bank's internal systems. An important difference with packet filter firewalls is the fact that proxy firewalls can inspect the content op IP-packages while a packet filter firewall will only look at the verification information in the header of the package (Overbeeke et al. 2003).
3. Combinations of packet filter and proxy firewalls. In this case the first step is to filter IP-packages on the basis of the verification information with the help of a packet filter firewall and after this a proxy firewall will filter on application sessions.

IDS

So called Intrusion Detection Systems (IDS) have the task to monitor the internal network of the private bank for awkward network traffic or other occurrences. An IDS can also help private banks to set up database with incident descriptions (OCC 1998). Furthermore the monitored network traffic (which is the same as the actual existing network traffic) can also be compared with the traffic which is suspected because of the implemented measures. On the basis of security warnings which the IDS can deliver a private bank could decide to shut down parts of the network and systems in order to prevent further damage.

Non-repudiation mechanisms

Several mechanisms are in place to ensure this. First log files can record the place, time and the computer from which certain transactions are performed by a user. The recording of the occurrence of the transactions is important because of the evidence which could be needed in case of a security incident. Another security measure to secure the non-repudiation of transactions and changes in the online banking system is the use of transaction authentication. In this way changes in the system performed by executing transactions can be recorded. Transaction authentication is usually implemented with the help of a TAN (Transaction Authentication Number) (Wiesmaier et al. 2005). Also SSL helps to secure the non-repudiation of transactions because it can protect the integrity of the transactions and thus no properties of the transaction can be changed.

C.3 IT-security measures against availability attacks

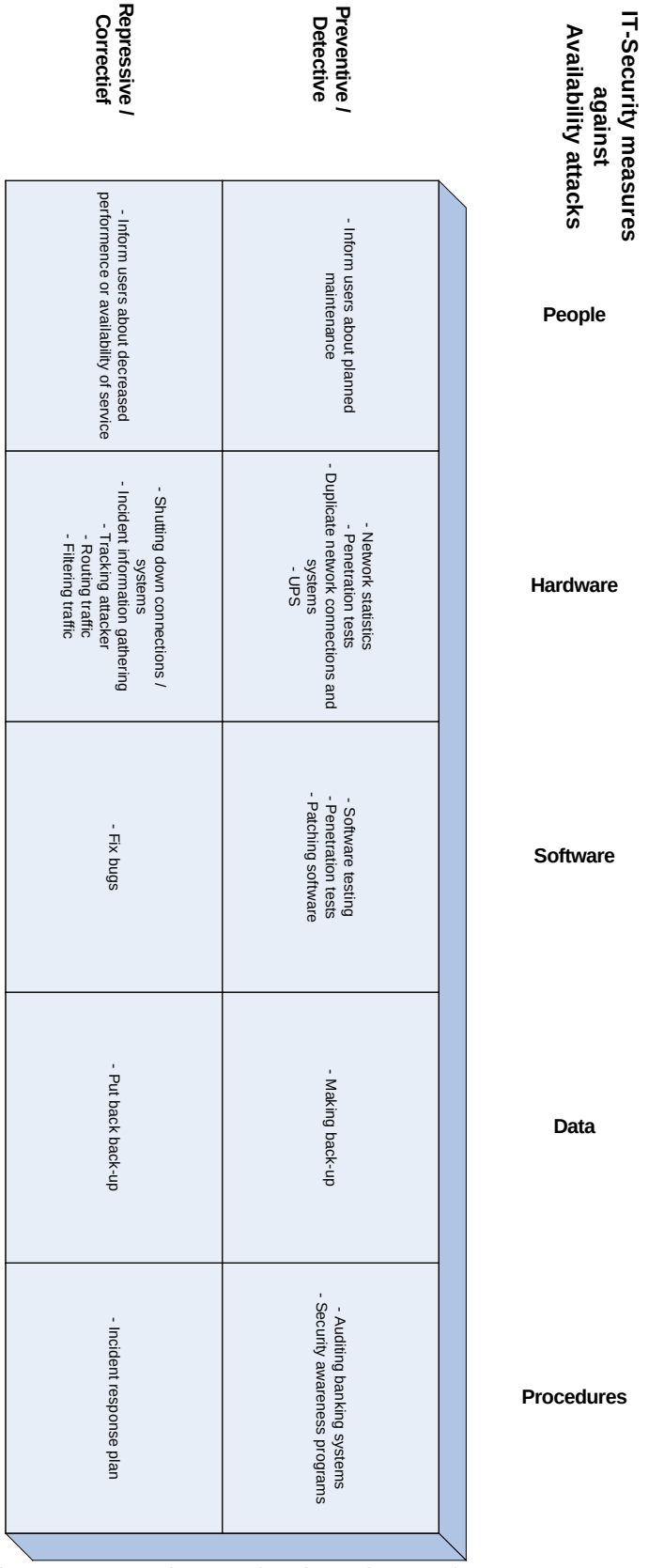


Figure 29: IT-security measures taken against integrity attacks

Data backup

There are different kinds of backups knowing:

- Full backup. Certain software and data is backed up fully.
- Partial backup. A part of certain software and data is backed up.
- Incremental backup. Only software and data which is changed or created after a certain point in time is backed up and added to the existing backup.
- Differential backup. Each part of the software and data which is created or changed after a certain point in time is backed up upon the last version of the backup (the old backup is overwritten).

In practice hard disks which are present in online banking systems are mirrored onto another hard disk present in the system. Furthermore the hard disk is frequently backed up onto tapes or other devices (systems).

Appendix D: Description of interview respondents

D.1 Theodoor Gilissen Bankiers N.V.

Theodoor Gilissen Bankiers is a pure private bank founded in 1881 which is active in the Dutch private banking market. The bank is became a part of the KBL Group European Private Bankers in 2003, which has 4200 employees in 11 countries in Europe. The main reason to become part of this European private banking network was the economies of scale for compliance, IT and knowledge management this would provide. In 2005 Theodoor Gilissen Bankiers has taken over Stoeve, which is a stock exchange bank. The bank is operating independently in the private banking market and does not provide credits to companies quoted on the stock exchange and does not provide services regarding the issue of stocks. The services offered by Theodoor Gilissen Bankiers are:

- Private banking and asset management services to wealthy individuals (payment transactions, loans, mortgages, brokerage, participating in the stock market and wealth management). These services are also provided for non-profit organisation and institutional clients.
- Brokerage services for professional relations.
- Stock exchange service insourcing for external asset management services.
- Cooperate finance services for companies. This includes services like financial and strategic advice.

In the private banking segment Theodoor Gilissen Bankier is targeting on individuals with a free capital between 1 and 5 million. This is considered as the upper class of wealthy individuals. Next to this Theodoor Gilissen Bankiers has almost the whole market of insourcing services for independent wealth managers. Because independent wealth managers do not have a banking licence they must refer to a bank for performing banking services for their clients. Theodoor Gilissen Bankiers has specialised in performing banking services for independent wealth managers by subscribing the clients of the wealth managers as their own and performing banking services in order of the wealth managers. Theodoor Gilissen Bankiers also provide advising services (such as compliance issues independent wealth managers could encounter) for this group.

Operational results (x1000 euro)	2004	2003	2002	2001	2000
Income	41123	41746	41339	57112	73563
Operating expenses	39134	38562	43037	40844	36190
Net profit	2223	2701	-927	11460	22302
Employees	188	191	241	257	223
Profit margin	5,41%	6,47%	-2,24%	20,07%	30,32%

Figure 30: Table with operational results of Theodoor Gilissen Bankiers in the period 2000-2004

As can be seen in figure 30 the turnover of Theodoor Gilissen Bankiers was 41.1 million euro in 2004 against 41.7 million euro in 2003. The earnings decreased from 2.7 million euro in 2003 to 2.2 million euro in 2004. The capital under custody was 4.5 billion euro in 2004 from 4.1 billion in 2003. Furthermore the income and net profit decreased dramatically in the years 2000 and 2001. Since 2002 the income was steady and this was also the case with the profit for 2003 and 2004. This is also described by the profit margins (the percentage of net profit of the income) in the last years.

At Theodoor Gilisen Bankiers two interviews were held with Henk Bout. Mister Bout is the head of the internal auditing group at Theodoor Gilisen Bankiers. In this function mister Bout is responsible for managing the internal controls and the general IT-controls at the

bank. Because of that last mentioned function he also knows a lot of the IT-security Furthermore mister Bout Mister Bout is also a registered EDP-auditor. Because not all questions were answered in the first interview a second interview was held with mister Bout.

D.2 Insinger de Beaufort

Insinger de Beaufort is a medium sized specialized private bank. Insinger de Beaufort is a fully independent bank for a part owned by the employees.
This list is displayed below: Insinger de Beaufort is offering the following services:

- Private banking services to wealthy individuals. This group of clients is divided into three kinds of services knowing wealth management, investment advice and execution only.
- Portfolio management for institutional clients.
- Corporate finance services for small and mid cap companies which are quoted on the stock exchange.

Insinger de Beaufort is targeting at wealthy individuals which a free capital between 250.000 and 500.000 euro. In their client portfolio old and new money clients are present. Furthermore a big part of their clients are international active.

Operational results (x1000 euro)	2004	2003	2002	2001	2000
Income	77100	91900	148100	122000	111700
Net profit	3200	98700	3100	5000	19100
Employees	436	434	1078	1203	920
Profit margin	4,15%	107,40%	2,09%	4,10%	17,10%

Figure 31: Table with operational results of Insinger de Beaufort in the period 2000-2004

As can be seen in figure 31 the turnover of Insinger de Beaufort was 77.1 million in 2004 against 91.9 million in 2003. The earnings of the bank were 3.2 million in 2004. The capital under custody has increased from 4.4 billion in 2003 to 4.9 billion in 2004. In the last past years the income has decreased but the net profit stayed stable which can also be concluded from the profit margin. In 2003 the trust group activities of Insinger de Beaufort were sold which explain the large net profit in that year.

At Insinger de Beaufort Francis Pickott was interviewed. Mister Pickott has the function of head of the Risk assurance department at Insinger de Beaufort. In this function mister Pickott has the supervision of risk analyses process of the bank. Risk analyses are performed for all business risks defined in paragraph 4.3.1 including IT and IT-security risks. In this way mister Pickott has expertise regarding the IT-security risks of online banking systems and the business aspects of IT-security.

D.3 Kempen & Co.

Kempen & Co. is a private bank which is targeting at so called super wealthy individuals (more than 1 million of free capital) with their private banking services. Furthermore Kempen & Co. is very active on the stock market. Because of the specialised knowledge present at Kempen & Co. regarding trading on the stock exchange they are now insourcing stock exchange services for other banks such as the Friesland Bank. Kempen en Co. was taken over by Dexia in 2001 but after the legio lease affair (clients which were leasing stocks to make extra profit but with the collapse of the stocks were in dept at the bank instead) a management buy out was arranged to become independent once again (the company is now in the hands of the employees, management, Friesland Bank, Hall investments and NPM capital). The banks had a turnover of 68.5 million euro in 2004 against 67.1 million in 2003. The earnings were 9.7 million in 2004. The capital under

custody increased to 5.34 billion euro in 2004 from 4.8 billion in 2003. The services performed by Kempen & Co. are:

- Private banking services to wealthy individuals with more than 500.000 euro of free investable capital. This include wealth management, payment services and the offering of all mainstream financial products such as mortgages and loans.
- Stock exchange services to wealthy individuals who are execution only clients and clients with an investable capital of more than 1000 euro. These services are also performed for other banks, such as Friesland bank. In this category of services also information delivery about companies quoted at the stock exchange is offered.
- Corporate finance service to companies.

At Kempen & Co. Alfred Rijnders was interviewed. Mister Rijnders is the Security Officer for Kempen & Co. In this function he has a both a supervision as a management function with regard to the IT-security. He needs to advocate the security of online banking systems internally but also need to make decisions with regard to concrete investments in IT-security. Because of his function mister Rijnders is both expertise in the technological and business aspects of IT-security.

D.4 Delta Lloyd private banking

Delta Lloyd Bankengroep is part of Delta Lloyd NV, which is in turn part of Aviva. The Delta Lloyd Bankengroep is active in the Benelux with the following businesses:

- Delta Lloyd Bank Belgie.
- Bank Nagelmackers 1747, which is a private bank in Belgium which is taken over by the Delta Lloyd group.
- Delta Lloyd securities, which is participating in the stock exchange market.
- Delta Lloyd Bank Nederland. The bank works with independent agents, who offer private individuals attractive mortgages, loans, savings and investment products. This bank also provide private banking services for wealthy individuals such as asset management. Under the trade name OHRA bank, Delta Lloyd bank also offers clients direct telephone and on-line access to flexible banking products, including consumer credit and savings and investment products.

Delta Lloyd Bankengroep wants to a leading provider of financial products and services on the Benelux market. This is done by offering banking and insurance products to private individuals and business owners/ managers. To provide the insurance products other insurance departments of the Delta Lloyd Group are involved.

The turnover of the Delta Lloyd Bankengroep increased from 141.4 million euro in 2003 to 146.5 in 2004. The earnings decreased from 12 million in 2003 to 7 million in 2004. The capital in custody were 7.1 billion euro in 2004 against 6.4 billion in 2003. Delta Lloyd private banking is targeting at wealthy individuals with an investable capital of more than 500.000. The bank is offering wealth management and execution only private banking services to these clients.

At Delta Lloyd Marcel de Groote and Diederik Kool were interviewed. Mister de Groote has the function of business consultant at Delta Lloyd Banking Group. In this function he gives advice of implementing online banking systems in the organisation. Mister de Groote therefore has some expertise regarding IT-security issues coming up with the implementation of online banking systems. Furthermore he has knowledge of the requirements the bank and the users of the system have regarding online banking systems. In order to get more information about the IT-security at Delta Lloyd bank also Diederik Kool, security officer at Delta Lloyd Bankengroep, was interviewed. Because of

his function Mister Kool has expertise about the CIA aspects of online banking systems and performing risk analyses regarding information systems at Delta Lloyd Bankengroep.

D.5 Van Lanschot Bankiers

Van Lanschot Bankiers is the oldest independent private bank in the Netherlands founded in 1737. Van Lanschot has the image of a bank which has full attention for their clients by adding a lot of personal attention to their banking services. This is exactly the reason the bank still is (and wants to stay) an independent bank. In this way the personal level of service can be guaranteed. Van Lanschot bankiers offers a full range of private banking services including:

- Full service private banking by offering payment services (also with the use of a level 3 online banking system), mainstream financial products like mortgages, loans, stock exchange and wealth management services. The target group of individuals of van Lanschot are individuals with more than 100.000 euro of free investable capital. With the take over of CenE bankiers a target group of medical professionals and other independent professions such as lawyers and brokers.
- Portfolio management for institutional clients.

Operational results (x1000 euro)	2004	2003	2002	2001	2000
Income	404511	378329	377904	373465	359738
operating expenses	257698	217250	227636	216434	229325
Net profit	102602	106664	97576	100824	147821
Employees	1970	1853	2010	1854	1660
Profit margin	25,36%	28,19%	25,82%	27,00%	41,09%

Figure 32: Table with operational results of van Lanschot Bankiers in the period 2000-2004

As can be seen in figure 32 the turnover in 2004 was 404.5 million euro against 378.3 million euro in 2003. Despite of this the earnings were decreased from 106.7 million euro in 2003 to 102.6 million euro in 2004. The capital under custody was increased from 7.9 billion euro in 2003 to 11 billion euro in 2004. Van Lanschot shows a steady increase in income in the period 2000-2003 with a mayor increase of income in 2004. In contrast the net profit in 2004 decreased a little because of higher operational expenses. Both the increased income and increased operational expenses could be the result of taking over CenE bankiers because the earnings without CenE bankiers were 119.4 million euro. In this way from 2001 until 2003 the profit margin was around 27 percent which fall back to around 25 percent in 2004.

At van Lanschot Bankiers Jeroen Bakker was interviewed. Mister Bakker is system architectect and software engineer at the software development department of Van Lanschot Bakiers. In his function mister Bakker deals with security requirements when developing software. In this way mister Bakker has expertise of the used security measures in online banking software. Because software is developed with the used hardware architecture at the online banking system he also has expertise of hardware IT-security measures.

Bibliography

Aladwani, A.M., 2001 "Online banking: a field study of drivers, development challenges, and expectations," *International Journal of Information Management* (21), pp 213-225.

Anandarajan, A., and Wen, H.J., 1999 "Evaluation of information technology investment," *Management Decision* (37:4), pp pp 329-337.

Anderson, R., 2001 *Why Information Security is Hard - an economic perspective* University of Cambridge Computer Laboratory, JJ Thomson Avenue, Cambridge, UK.

Avinandan Mukherjee, P.N., 2003 "A model of trust in online relationship banking," *International Journal of Bank Marketing* (21/1), pp 5-15.

Baarda, D.B., and Goede, M.P.M.d., 2001 *Basisboek methoden en technieken* Wolters-Noordhoff, Groningen.

Babbie, E., 2004 *The practice of Social Research*, (10th ed.) Wadworth/Thomson Learning, Belmont, p. 493.

Basel Committee on Banking Supervision, 2003 "Risk Management Principles for Electronic Banking."

Basten, N., and Wijnmaalen, M., 2003 "Greep op security awareness," *IT-beheer* (7).

Beek, J.J.v., and Schut, F.R., 2002 "Ontwikkelingen in de beheersing van ICT in de financiële sector," *compact* (nummer 4).

Bicker, L., 1996 *Private banking in Europe* Routledge, p. 181.

Biene-Hershey, M.v., and Bongers, M., 1997 "IT-audit verdringt EDP-audit - Norea en de verschuivende grenzen van het vakgebied," (nr 43), p pag 41.

Bohm, N., Brown, I., and Gladman, B., 2000 "ELECTRONIC COMMERCE: WHO CARRIES THE RISK OF FRAUD?."

Brule, J.F., 1985,"Fuzzy systems - a tutorial," in: *www.austinlinks.com/Fuzzy/tutorial.html*.

Butler, S.A., and Fischbeck, P., 2002 "Multi-Attribute Risk Assessment," Proceedings from Symposium on Requirements Engineering for Information Security (SREIS 2002).

Carr, N.G., 2003 "IT doesn't matter," *HBR* (may), pp 41-49.

CBS, 1997 "Automatisering en informatie bij bedrijven en overheid," www.cbs.nl.

CBS, 2005a "Statistisch jaarboek."

CBS, 2005b"statline," www.cbs.nl.

CERT, 2002 "Overview of attack trends - CERT Coordination center."

Chan, S., 2001 "Risky E-business," *Internal auditor* (december).

Chapin, D., and Akridge, S., 2005 "How can security be measured?," *information systems control journal* (volume 2).

Claessens, J., Dem, V., Cock, D.d., Preneel, B., and Vandewalle, J., 2002 "On the Security of Today's Online Electronic Banking Systems," *Computers & Security* (21:no 3), pp 257-269.

Committee on Information Systems Trustworthiness National Research Council, 1999 *Trust in Cyberspace* National Academic Press, p. 352.

Comsec information security, 2005"Application Security - the weakest link," www.comsec.co.il.

Cornelissen, A.M.G., Berg, J.v.d., Koops, W.J., Grossman, M., and Udoa, H.M.J., 2001 "Assessment of the contribution of sustainability indicators to sustainable development: a novel approach using fuzzy set theory," (86), pp 173-185.

De Nederlandsche Bank, 2002 "Vermogensbeheer Nederlandse gezinnen onder de loep."

De Nederlandsche Bank, 2004 "Handboek Wtk."

Dubois, D., and Prade, H., 1998 "An introduction to fuzzy systems," *Clinica Chimica Acta* (270), pp 3-29.

EDS, 2005 "EDS U.S. Financial Services Privacy and Customer Relationship Management Survey."

Erwin, D.G., 2002 "Understanding Risk (or the Bombastic Prose and Soapbox Oratory of a 25-Year Veteran of the Computer Security Wars)," *INFORMATIONSYSTEMS SECURITY* (JANUARY/FEBRUARY).

FFIIEC, 2001 "Authentication in an Internet Banking Environment," Federal Financial Institutions Examination Council, United States of America.

Fitch, 2000 "Re-examining private banking," US banker.

Garg, A., Curtis, J., and Halper, H., 2003a "The financial impact of IT Security Breaches: what do investors think?," *Information System security* (march/april).

Garg, A., Curtis, J., and Halper, H., 2003b "Quantifying the financial impact of IT security breaches," *Information Management & Computer Security* (11), p 74.

Geert-Jan Smits, J.S.B., 2004 "De beste Internetbank van Nederland," *BankingReview* (December), pp 34-43.

Glaessner, T., Kellermann, T., and McNevin, V., 2002 "Electronic Security: Risk Mitigation In Financial Transactions," Public Policy Issues, The World Bank.

Harris, J., 2003 "How to Prevent Cyber Sabotage," SANS institute.

het Financieele Dagblad, 4 July 1997"Merrill Lynch richt vizier op Nederland."

het Financieele Dagblad, 16 June 2003"IT-inbraken kruipen uit taboesfeer."

het Financieele Dagblad, 18 June 2005"Private bank zonder pluche of marmer."

Huyveneers, S.C., 2001,"eBanking risico's in the New Economy een beheersingsaanpak," in: *Faculteit Bedrijfskunde*, Rijksuniversiteit Groningen, Groningen, p. 99.

ISF, 1997 "SPRINT user guide," European Security Forum.

ISF, 2005a "The information security status survey 2005," Information Security Forum.

ISF, 2005b "ROSI Return on Security Investment Workshop Report," Information Security Forum.

Jaquith, A., 2002 "The security of Applications: not all are created equal," @stake.

Karjaluoto, H., Koivumäki, T., and Salo, J., 2002 "Individual differences in private banking: Empirical evidence from Finland," International Conference on System Sciences (HICSS'03), Proceedings of the 36th Hawaii.

Kasabov, N.K., 1996 *Foundations of Neural Networks, Fuzzy Systems, and Knowledge Engineering* The MIT press, Cambridge.

Krempl, S., 2005 "De halve waarheid," *C't magazine* (nr 7/8).

Lin, Z., Li, D., and Huang, W., 2003 "Reputation, Reputation System and Reputation Distribution - An Explorative Study in Online Consumer-to-Consumer Auctions," *Current security management & Ethical issues of information technology table of contents*), pp 249 - 266.

Lötgerink, C.W., 2004"Maturity model for information security, A method for benchmarking the Dutch financial sector," in: *Faculty of Economics and Business Administration, Information Systems and Management*, Tilburg University.

Lucas, K., 2005 "Spyware and The Next Level of Spyware Mitigation," East Carolina University.

Miller, R., 2005 "Banks shifting logins to non-SSL pages," www.netcraft.com.

Mishra, A.K., and Lucknow, M., 2005 "Internet Banking in India-Part I + II," http://www.banknetindia.com/banking/ibkg.htm http://www.banknetindia.com/banking/ibkg1.htm.

Mol, X., 2002"Assurance voor online financiële dienstverlening: Vergroting van de verwachtingskloof ?!?," in: *EURAC B.V.*, Erasmus University Rotterdam.

Moulton, R.T., and Moulton, M.E., 1996 "Risk Management: A checklist for Business Managers," *Computers & Security* (15), pp 377-386.

Mrdovic, S., 2004 "E-banking fat client security analysis," International Conference on telecommunications "BIHTEL 2004".

Mukherjee, A., and Nath, P., 2003 "A model of trust in online relationship banking," *International Journal of Bank Marketing* (21/1), pp 5-15.

Munck, S.d., Stroeken, J., and Hawkins, R., 2001 "E-commerce in the banking sector," TNO Stategy, Technology and Policy.

Novell, and IT Topmanagement, C.T.P., 2002 "Ondernemen met IT, een onderzoek onder Nederlandse managers naar hun IT-security strategie."

OCC, 1998 "Technology risk management: PC banking," *Office of the Comptroller of the Currency* (98-38).

OCC, 1999 "Infrastructure threaths from cyber-terrorists," *Office of the Comptroller of the Currency* (99-9).

Oscarson, P., 2003a "Actual and Perceived Information Security - A first Outline," Department of Business Administration, Computer Science, Economics and Statistics at the Obrebro University in Sweden.

Oscarson, P., 2003b "Graphical Conceptualisations of Fundamental Concepts within the Information Security Area," Rebro University, Sweden.

Overbeeke, P., Lindgreen, E.R., and Spruit, M., 2003 *Informatiebeveiliging onder controle* Pearson Education Uitgeverij BV.

Payne, S.C., 2001 "A guide to Security Metrics," SANS Institute.

Pennathur, A.K., 2001 "Clicks and bricks: e-risk management for banks in the age of the Internet," *journal of banking & finance* (25), pp 2103-2123.

PricewaterhouseCoopers, 2004 "Uncertainty tamed? The evolution of risk management in the financial services industry."

PricewaterhouseCoopers, 2005a "Global Private Banking / Wealth Management Survey."

PricewaterhouseCoopers, 2005b "The Global State of Information Security 2005," CIO magazine.

PricewaterhouseCoopers, 2005c "private sector maakt zich op voor radicale veranderingen."

PricewaterhouseCoopers, and Wilmer, C.P., 2003 "PricewaterhouseCoopers economic crime survey 2003."

Ridderbeekx, E., and Berg, J.v.d., 1998 "Internetbeveiliging, een beheerperspektief," *Informatie* (40-e jaargang:april 1998), pp pp 46-55.

Santos, A.L.M.d., 2000"The use of Safe Areas of Computation (SAC) for secure computing," in: *department of computer science*, UNIVERSITY OF CALIFORNIA, Santa Barbara.

Sathye, M., 1999 "Adoption of internet banking by Austalian consumers: an emperical investigation," *International Journal of Bank Marketing* (17/7), pp 324-334.

Schechter, D., 2004 "Computer Security Strength & Risk: A Quantitative Approach," The Division of Engineering and Applied Sciences, Harvard University.

Shaw, G., 2005 "Identity Theft: Managing the Risk," Insight Consulting.

Spivey, J., 2001 "Banks vault into online risk," *Security management* (january), pp 132-138.

Steen, J.v.d., 2004"How to be successful in the private banking business? : a thesis about value creation in the Dutch private banking business," in: *Rotterdam School of Management, department of Finance & Investments*, Erasmus University Rotterdam, Rotterdam.

Stellinga, M., 2005 "Pasfraude via het web," *Elsevier* (61:29, 23 juni).

Stewart, A., 2004 "On risk: perception and direction," *Computers & Security* (23), pp 362-370.

Vrede, T.d., 2005 "Basel II richtlijn blijkt lastige klus," *Automatiseringgids* (29-07).

Weise, J., and Martin, C., 2001 "Data security policy - structure and guidelines," Sun microsystems.

Wiesmaier, A., Fischer, M., Lippert, M., and Buchmann, J., 2005 "Outflanking and Securely Using the PIN/TAN-System," *Department of Computer Science, Technische Universitat Darmstadt* (May 2005).

www.security.nl, 22-06-2005 "Internetbankieren onvoldoende beveiligd op."

Yazar, Z., april 2002 "A qualitative risk analysis and management tool -CRAMM,").