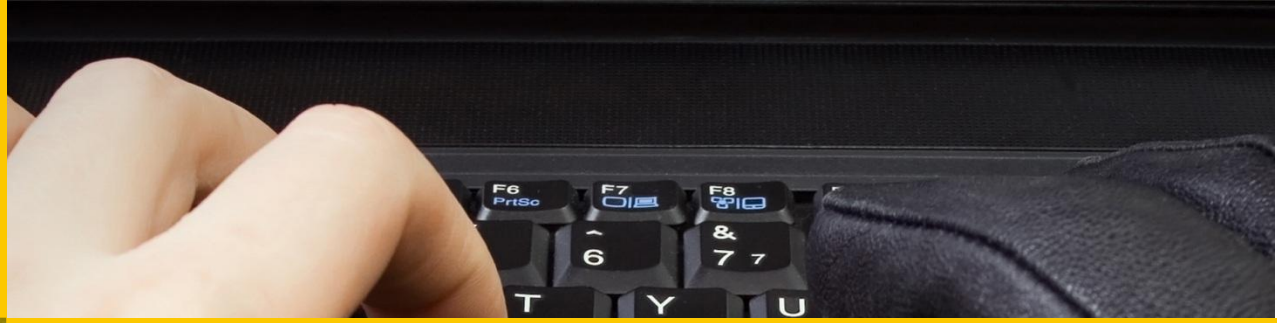
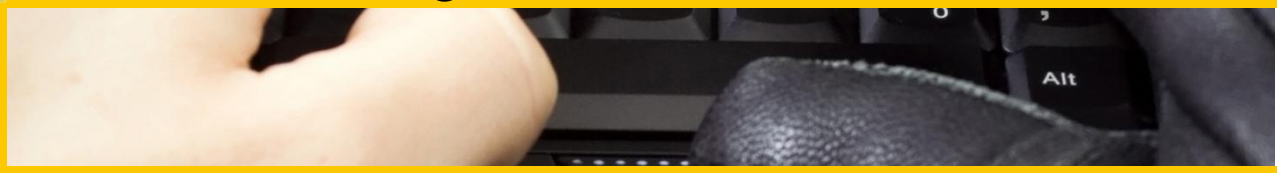


Improving External Control of Online Web-based Banking Fraud in The Netherlands



Loek M.W. van Gool

Erasmus School of Economics

ERASMUS UNIVERSITEIT ROTTERDAM

Master Thesis Economics & Informatics

Economics & ICT programme
Student ID: 283517
Supervisor: Dr. Ir. R. Mersel
2nd Supervisor: Dr. S. El Aoufi

September 2011

Abstract

Ever since the birth of the Internet, people have been using it more and more for accomplishing their daily tasks. One popular applications of the World Wide Web is online banking, a practice which is especially popular in The Netherlands. Online banking, however, is not without its risks: criminals have armed themselves with in-depth technical and even psychological knowledge in order to gain access to banking accounts of unsuspecting users.

This research seeks to gain insight in the Dutch online banking security systems in order to find its strengths and weaknesses. The external security controls that have the potential to increase control over online web-based banking fraud (OWBF) risk without yielding too high a cost are especially of interest. Additionally, it aims to quantify the performance of the Dutch banking sector relative to its peer countries through criminal statistical database research and provide in insight in the (international) cooperation between banks, consumer organizations and banking lobbyist.

A number of experts from the field of financial security have been questioned using semi-structured, in-depth interviews. From this interview, a qualitative discussion is derived that aims to find potential security improvements to Dutch online banking, technological, social, cultural or organizational.

This research finds that the current security controls are very effective at their job, and that most if not all banks are well within their set limits (risk appetite). However, a number of controls have been found that could increase control of OWBF threats without violating any of the trade-offs: out of band authentication, signing of token keys (these two are also referred to as "What You See Is What You Sign" or WYSIWYS) and reversing the trust relationship between the bank and the customer.

This research also suggests future research to be based on quantitative methodologies so it can include a statistically significant number of respondents using more closed questions. Furthermore, there is a need for further research into a few of the security controls that could not be verified within the scope of this research and that have the support of one expert only. Finally, there is a clear need for international comparability of criminal statistics and definitions of OWBF, a need which still exists today.

Acknowledgments

I would like to thank anyone who contributed to this project, either direct or indirect: Mr. Mersel, my wise supervisor, for his constructive commentary and helpful contacts; Mr. El Aoufi, for his extensive constructive commentary as my second supervisor. Also, I would like to thank all interviewees for their precious time and valuable input. Furthermore, I would like to thank my friends and roommates for giving helpful tips and getting me coffee.

Table of contents

List of tables

List of figures

1 Introduction

Along with the explosive expansion of the Web in the late 1990s and 2000s, the world has seen a strong growth of online Web-based banking fraud or *OWBF* (NVB, 2011; Bundeskriminalamt, 2009; Federal Trade Commission, 2008; Internet Crime Complaint Center, 2009). OWBF attacks occur online, often involve a multiple of countries at once and exploit the most recently discovered technical weaknesses. Hence, this relatively new form of crime poses significant risk and requires a new form of security control. Quantitatively assessing the occurrences and damages caused by OWBF is a logical first step. However, only a few Western countries have been forthcoming in publicizing statistical information about the occurrence of computer-related crime in their territories. Most data have not reached adequate levels of granularity, trustworthiness or comprehensiveness. The Netherlands is a country where data on both the occurrences and damages caused by OWBF are brief and unaudited (NVB, 2011).

This research argues that while the mitigation of internal security risk is arguably decent, there is still a considerable amount of damage incurred as a result of OWBF crimes. If the internal controls are adequately effective, than by exclusion the external ones must be ineffective. It is the aim of this research to qualitatively explore the effectiveness and possible ways of improving of external risk mitigation through the perspective of a number of large Dutch banks, bank IT advisories or banking lobby organizations.

1.1 Importance of research

According to recent data on Dutch Internet penetration, its use of both the Internet itself and online banking specifically are among the most widespread in the world (comScore, 2010; Innopay, 2010; Internet World Stats, 2009), as can be seen in Table 1. Meanwhile online banking fraud has also been on the rise in many other Western countries, based on both occurrences and damages per occurrence (Federal Trade Commission, 2007; Innopay, 2010; NVB, 2011; Bundeskriminalamt, 2009; Financial Fraud Action UK, 2010). These data suggest that a continuing acceleration of online banking fraud may be likely. This evidence raises a number of concerns: if online web-based banking (*OWB*) activity has increased or will increase to the point that it becomes the main method of banking in The Netherlands for both organizations and individuals, are the risks of OWBF still sufficiently managed, now and in the future?

Country	Online banking penetration (%)	Internet penetration (%)
Canada	64.8	74.9
The Netherlands	60.7	85.6
France	56.6	69.3
Sweden	53.9	89.2
UK	51.1	76.4
New Zealand	49.8	83.1
Belgium	47.0	70.0
Spain	46.5	71.8
US	45.1	76.3
Australia	44.2	80.1

Table 1: Top 10 online banking penetration & Internet penetration countries (comScore, 2010; Internet World Stats, 2009)

1.2 Research scope

This research aims to explore the current state of external risk mitigation of OWBF risk in The Netherlands, and possible ways of improving it, through the eyes of security experts. Using a qualitative and in-depth method, it is not the aim of this research to find evidence that is generalizable to the entire population of security experts.

For an international comparison, other Western countries with significant retail banking sectors will also be subject of this research to be used as a frame of reference. Poor, technologically less developed, small or otherwise limited countries will not be considered, nor is the list of countries meant to be exhaustive.

Research of any time period may be considered, but given the fast-changing nature of the Internet more recent sources may offer an advantage, especially considering the recent rise of online crime in general. Most sources will be available in English, but given the list of non-English speaking countries and the fact that crime statistics may be considered an internal affair, non-English sources are not excluded from this research.

No limit is placed on the age of the used research. However, any source will need to have significant importance and relevance in today's world, and more recent research should be prioritized. To be able to exclude as little resources as possible, the latest possible date limit for any literature sources is set to September 1st, 2011.

1.3 Thesis structure

The structure of this thesis is as follows. In this chapter the general introduction, importance and scope of this research is defined. Chapter 2 contains a review of the current literature on OWBF and current criminal statistics from several peer countries. Chapter 3 explains the choice of research methodology, research questions, interview design, et cetera. Next, Chapter 4 through 7 contain the expert interviews. Chapter 8 includes a thorough discussion of the interview results. Chapter 9 presents the thesis conclusions, limitations and suggestions for future research.

2 Background

Introduction

In this section, both an academic literature overview and the current international OWBF situation are presented. First, the terms cybercrime and online Web-based banking fraud are defined. Then, a list of current attack methods and supporting tools follows. Subsequently, IT Enterprise Risk Management (*ERM*) and the IT security controls frameworks as they relate to OWBF are covered. Then, the actual mitigation of OWBF risk through information security controls is discussed. Then, the investigation into the current OWBF situation at peer countries is presented. This section concludes with a discussion of findings and directions for this research.

2.1 Online web-based banking fraud (OWBF)

OWBF is a subset of a broader category of crime known as *cybercrime*. There has been some debate on the exact definition of cybercrime and its meaning has possibly changed as a result of the evolution of the Internet itself. For instance, in Australian law, the term cybercrime describes a narrow set of offences against data and computer systems (Government of Australia, 2001), while other organizations have proposed wider definitions (Council of Europe, 2001; Zeviar-Geese, 1997-1998). These latter definitions describe cybercrime as an umbrella term by adding for example cyber stalking, any unauthorized access to systems and child pornography to the first mentioned, more narrow definition. An overview of different definitions is presented in (Australian Institute of Criminology, 2011).

One of the implications of the narrow definition is that cybercrimes cannot be committed against humans. Because some online banking fraud methods have a strong social component, the usage of a narrow definition may exclude cases of social online banking fraud, such as phishing, that are still perceived to be OWBF crimes by numerous cybercrime organizations (NVB, 2011; Financial Fraud Action UK, 2010; CyberSource, 2011). Hence, a narrow definition is not preferable in this case.

In a recent proposal, the broad definitions of cybercrime were generalized in a single umbrella definition which is the one used for this research:

> **Cybercrime:** Any crime that is facilitated or committed using a computer, network, or hardware devices (Gordon & Ford, 2006).

Gordon et al. also propose a separation between two broad types of cybercrime:

- **Type I** generally requires a limited number of events and is often facilitated using malicious software, such as key loggers or Trojan horses. Type I crimes tend to be aimed

at financial gain through the acquisition of secret or private information that can be used to identify or authorize an entity, such as credit card numbers or account credentials.

- **Type II** cybercrime generally requires multiple events and is often supported with the use of non-malicious software, such as instant messaging programs. Type II crime perpetrators tend to have a more personal or political motive like cyber stalking or cyber terrorism. Type II cybercrimes typically do not directly provide financial gains for the perpetrator (but may still cause financial losses for its victims).

As OWBF is primarily conducted to provide financial gain for the perpetrator, Type I is the type of cybercrime most relevant to this research.

The discussion of cybercrime definitions and categorization has a longer history than presented thus far. Another categorization of cybercrime was proposed by (Carter, 1995; Davis & Hutchison, 1997).

Cybercrimes are also categorized by role of the computer:

1. Cases in which the computer is the **object** of the crime such as attacks on IT infrastructure or unauthorized use of systems.
2. Cases in which computers are a **tool** used to conduct 'real-world' crime such as fraud or harassment.
3. Cases in which crimes are **computer-supported** in which otherwise 'real-world' crimes are executed using the computer just for communication or office productivity.

For this research, an exclusion based on the computer being either the object or tool unnecessarily risks ignoring some forms of cybercrime that are still important to this research. Arguably, in many cases the computer will be the object of the crime. However, since OWBF cases may also have a significant social factor, it seems overly strict to exclude the second category. The computer-supported category is excluded from this research because for OWBF to occur a breach in IT infrastructure security is required, which is not guaranteed in computer-supported attacks.

Within online financial fraud, another distinction can be made between cases with and without the direct involvement of retail banks. For this research only the former type is relevant. An example of online non-banking fraud is failure to deliver items purchased through online auction websites.

Finally, a distinction is made between online web-based banking and online banking without the use of a Web browser but rather with some kind of custom application running on the customer's computer and communicating with the server through any open or closed protocol. The security control situation in non-Web browser based banking may be very different versus that of banking

in Web browsers. As its security measures are generally closed-source and unknown and its usage in The Netherlands is low (see Table 2), non-Web browser based banking is excluded from this research.

Bank	Private accounts	Business accounts
ABN AMRO Bank	Web browser based	Web browser based & application based
ING Bank	Web browser based	Web browser based
Rabobank	Web browser based	Web browser based
SNS Bank	Web browser based	Web browser based
Friesland Bank	Web browser based	Web browser based

Table 2: Online banking methods at the largest Dutch retail banks (ABN AMRO, 2011; ING Bank, 2011; Rabobank, 2011; SNS Bank, 2011; Friesland Bank, 2011).

Therefore, the definition of OWBF as it is used in this research is:

> **Online Web-based banking fraud (OWBF):** the cases of cybercrime where the main goal of the activity is financial gain for the perpetrator through fraud, where a retail bank is involved and where IT infrastructure is used as the object or tool to achieve the fraud and where the Web browser's involvement is material.

2.2 Methods, threats and risks

This section will first identify the different methods and tools that are used to execute online banking fraud today. Secondly, the management of these risks is discussed.

2.2.1 Methods and tools

Fraud on the Internet is a numbers game: usually large pools of potential victims are attacked with a very low relative rate of success (Federal Trade Commission, 2008). Of course, all kinds of security controls and checks such as email blacklists or manually checking the URL of the Internet browser are in use on a day to day basis. Fraud requires for some kind of flaw to exist, either in a human being or in a system (usually software), or both. Because software is continuously updated and humans are made aware of risks through awareness programs, attackers must find new exploits in order to stay in business. This has led to a continuing cat-and-mouse game between the (organized) criminals and various public and private IT security and justice organizations.

A distinction between methods that are primarily social and ones that are primarily technological in nature can be observed:

1. Methods that use hardware and software to execute their attacks without (much) direct action by humans. This does not exclude attacks that were made possible by indirect

human action. An example of human actions that indirectly cause these OWBF attacks is the accidental installation of malicious software that in turn executes an attack.

2. Methods that do use hardware and software to execute their attacks, but also require direct action from a human being. An example is phishing, were the user is motivated to manually enter his or her account credentials in an illegitimate website. In those cases, the technological component is inferior to the social one.

From this distinction, two new concepts are derived:

> **Technological OWBF threat:** an OWBF threat which is based on a technological weakness, with or without the help of a social component. A technological threat is also known as a security exploit.
>
> **Social OWBF threat:** an OWBF threat which is based on a social weakness, with or without the help of a technological component. This does not, however, require the involvement of multiple humans as the title might suggest. A social threat may also be known as a human or organizational threat. For the purpose of this research, these are all equal.

To understand the security controls that mitigate the risk of OWBF, it is necessary to first understand the different methods that are in use today. These methods are constantly evolving, but most perpetrators use one or more of the following general attack methods.

Phishing

Phishing, in the financial banking sense of the term, can be described as:

> **Phishing:** a form of social engineering in which the attacker attempts to lure the user in a false sense of security in order to obtain his or her vital credentials that can be used to engage in a financial transaction that is not intended by the user (Jakobsson & Myers, 2006).

In general, a personal message is sent through email or instant messaging that mimics the appearance of an entity that is trusted by the user, typically including artwork and slogans of the bank. An example of a phishing email that mimics an authentic message from a retail bank is given in Figure 1. Lead to believe that he is visiting his bank's Web site, the user is actually directed to a cloned Web site that was created for the sole purpose of catching (phishing) the credentials of users. Often, the user is not aware of the identity theft until the fraud has occurred. Phishing is an increasingly popular method to conduct fraud through identity theft (Financial Fraud Action UK, 2010; GOVCERT.NL, 2010). As phishing requires user actions, it is classified as a

social OWBF threat. As phishing occurs outside of the boundaries of the banking system, it is classified as an external threat.

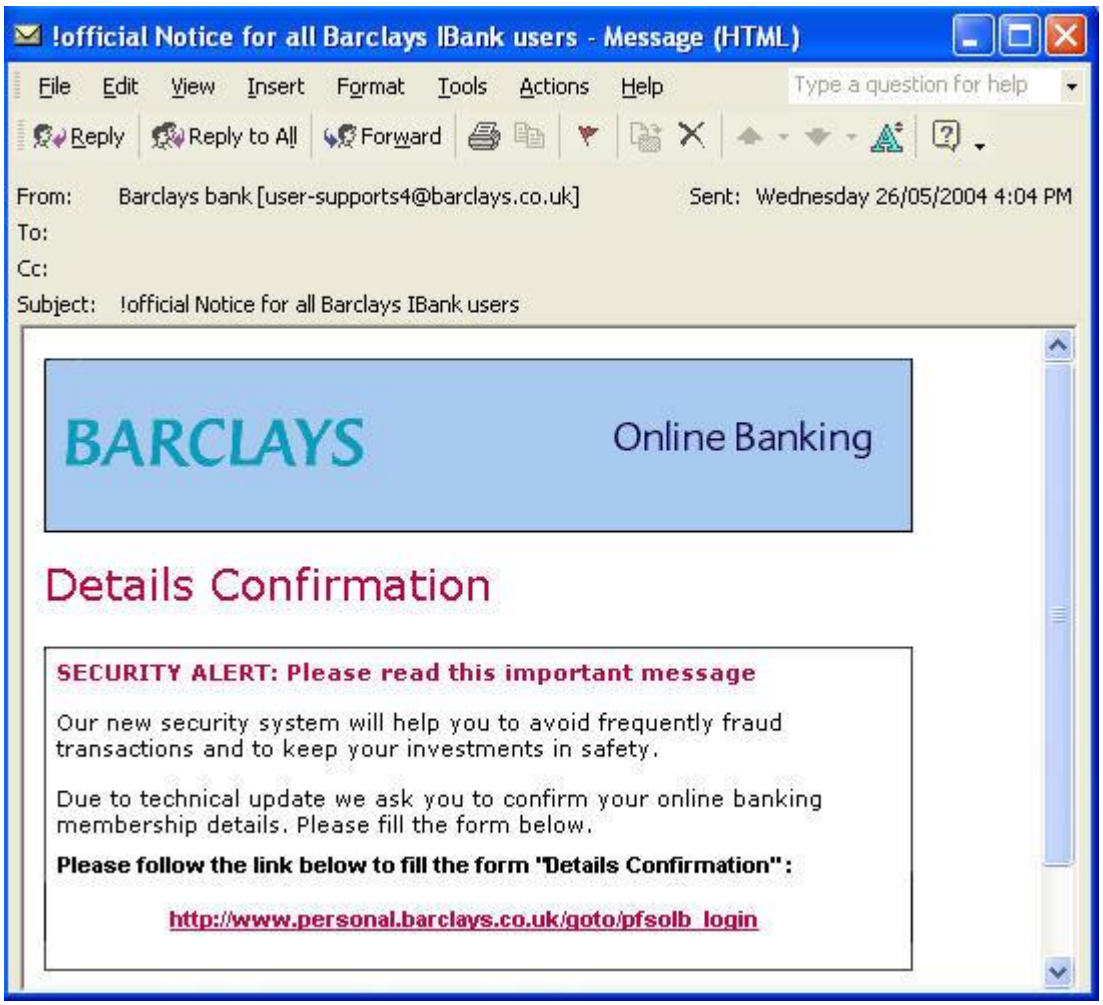


Figure 1: Phishing email example (FraudWatch International, 2011)

Malicious software

Malicious software is software that is designed to exploit vulnerabilities in other programs.

> **Malicious software (or crimeware, malware):** software that performs illegal actions unanticipated by a user running the software, which are intended to yield financial benefits to the distributor of the software (Emigh, 2006).

This software can manifest itself in many ways such as an online game, a pirated copy of legitimate software, or perhaps an electronic greeting card. Once installed, it can stay on the victim's computer for a long time, mutating and evading detection while trying to steal any vital information that it can find. Because some malicious programs need to exploit people's psychology in order to perform their tasks, the controls required to prevent the use of malicious

software need to be social too, hence sometimes it has a social component in addition to the technological one.

There are numerous types of malware, like Trojans, worms, rootkits, session hijackers, et cetera. An overview of different kinds of malware is discussed in (Emigh, 2006). Furthermore, a distinction can be made between malware that executes attacks itself and malware that enables other forms of attack by sending spam or spreading other malware. In that case malware often turns the victim's client computer in a bot in a botnet (Emigh, 2006), as discussed more thoroughly in "Botnets" in this paragraph. As malicious software exists outside of the boundaries of the banking system, it is classified as an external threat.

Man in the Middle (MITM)

In a MITM attack, the communication between the client (customer) and server (the bank) appears to be confidential and correct, while actually there is an attacker 'in between'. An overview of the different types of MITM and possible protection options is given in (Oppliger, Rytz, & Holderegger, 2009). In short, the attack happens as follows. In normal operations the client and the bank communicate directly. In a MITM attack, the attacker places himself in between two trusting parties, allowing him to view and alter any communication between two victims in real-time while it still appears to be confidential and correct to both parties. A graphical representation of a MITM attack is shown in Figure 2.

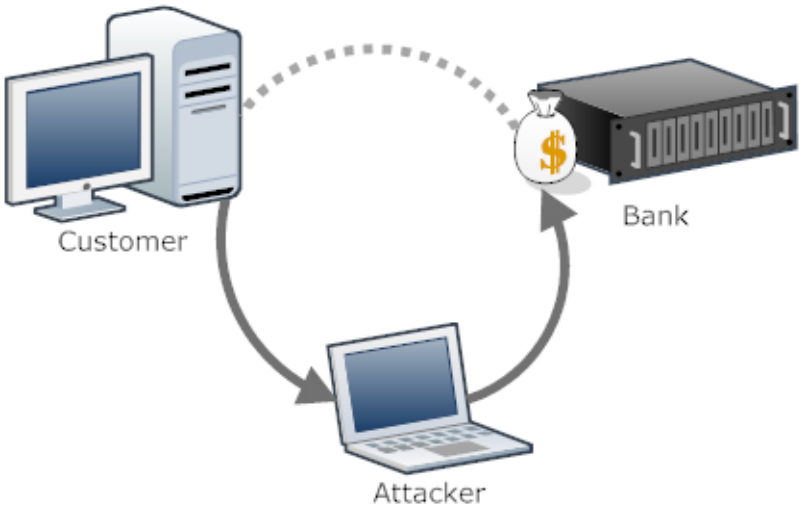


Figure 2: Communications of a MITM channel-breaking attack

Oppliger et al. identify three different classes of Man in the Middle attacks (Oppliger, Rytz, & Holderegger, 2009):

1. **Credential-stealing attack:** in this attack, users are lured into a false sense of security and in this process their account information is obtained by the attacker. This is a subset of the realm of phishing attacks discussed earlier. Credential-stealing attacks need no further distinction in this research.
2. **Channel-breaking attack:** in this type of attack, the attacker breaks the secured encrypted connection that exists between the client and the bank. From this position, it is capable of presenting or capturing all information that is transmitted. MITM Channel breaking attacks are visualized in Figure 2.
3. **Content-manipulation attack:** malicious code on the client's machine manipulates the information that is communicated between the client and the bank in real-time. This way, a client can be presented with information that was altered and has thus lost its integrity. This is also known as a 'Man in the Browser' attack and is an implementation of the malicious software attack discussed earlier. Hence, it is discarded for this research.

As said, only the second of these three classes presents a new attack method. The others are found in other tools and thus discarded. As MITM attacks occur before the communication enters the boundaries of the banking system, it is classified as an external threat.

Tools

A number of tools can be identified that are vital to OWBF attacks. These support OWBF attacks but do not directly execute attacks themselves.

- Botnets

  A botnet is a network of *bots*, computers that are infected with malware that are controlled by a human. A botnet is "the army that responds to the will of the commander" (Abu Rajab, Zarfoss, Monrose, & Terzis, 2006). Bots are closely related to malicious software and spam messages, as the bots computer routines are a form of malicious software and botnet software can spread using spam and illegitimate websites.

  The bots can submit any personal data that exists on the infected bot and provide the commander with its resources, like computer processing time, memory and bandwidth. Botnets are used for spamming, software piracy and identity theft, among other uses (Honeynet Project and Research Alliance, 2005). Botnets are social because human action may be required to spread them, and technological because they can also operate using only technology. As botnets exist outside of the boundaries of the banking system, it is an external threat.

- Illegitimate websites

  Illegitimate websites facilitate certain attack methods. An illegitimate website may be a teaser site that aims to lure in users to collect email addresses for spamming, or tries to make the user download malicious software under false pretense. It could also be a faked banking website that facilitates phishing. However, illegitimate websites are not always social threats in nature. Since they are also used to command botnets, they also have a technological component. Moreover, there is the possibility that they are hosted, created or managed without human action. Therefore, this tool is both social and technological. As illegitimate websites exist outside of the boundaries of the banking system, it is classified as an external threat.

- Spam

  Spam is the name given to an unsolicited message sent in bulk. Most often, these are emails, but other uses include instant messaging spam, Internet forum spam, and social networking spam. The definition of spam as used in this research is:

  > **Spam:** An electronic message is classified as "spam" if (1): the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (2): the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent (The Spamhouse Project, 2011).

  Spam is not a very direct way of committing OWBF. However, some methods require a way of contacting a large list of users with the least effort (bulk). Phishing is one of these methods and may use spam messages to achieve this. Therefore, spam is a tool for committing OWBF.

  Despite numerous technical attempts to filter out spam messages, this process is still not very dependable (Damiani, De Capitani di Vimercati, Paraboschi, & Samarati, 2004; Luca Becchetti, 2008). Botnets and malware play a part in the distribution of spam. As spam is sent and read outside of the boundaries of the banking system, it is an external threat.

In Table 3, the risks that have been identified are listed and joined with identified attack methods. They will be used in the next paragraph to group the identified security controls.

Risk	Attack method(s)
Broken confidentiality	Phishing, Social engineering, malicious software
Broken integrity	MITM channel breaking, security exploits, malicious software

Table 3: Risks of identified attack methods

Propagation methods

A propagation method describes the way in which an entity is attacked. A literature search has identified three propagation methods that are used:

1. **Social engineering:** convince the user that the attacker is actually an entity that the user trusts, such as his bank or the government. In a social engineering attack, the user willingly provides vital information to the attacker while lured in a false sense of security (Thornburgh , 2004).
2. **Security exploits:** as computer systems are not perfect, they contain security flaws that can be exploited by other applications, scripts, patches or humans. Malicious software seeks to capture vital information without user cooperation by exploiting technological weaknesses.
3. **MITM channel breaking:** based on the same premise as security exploits, it is mentioned separately because of the different nature of the attack. A channel breaking attack takes place on the connection between the customer and his bank, while a security exploit takes place on a computer system.

Identity theft

All three propagation methods perform an activity that, from the perspective of the banks, can be classified as an identity theft. Identity theft is usually defined as unlawful possession of personal identifying information for a fraudulent purpose, but there are multiple definitions in existence. Sometimes identity theft is limited to non-account information (Hayward, 2004), while others use a broader approach that includes any kind of personal identifying information (US General Accountability Office United States, 2002). In this constantly changing field, it is important to use a wide approach in order to cover all cases in which an identity is being faked for financial gain. Therefore, the latter definition of identity theft is preferred in this research, noting of course that all of the aforementioned criteria are met.

> **Identity theft:** any case related to the investigation of false, fraudulent, or counterfeit identification (US General Accountability Office United States, 2002).

Identity theft as a method of online fraud has been on the rise throughout the developed world with an emphasis on financial transactions that involve retail banks (Federal Trade Commission, 2007; Financial Fraud Action UK, 2010; Innopay, 2010).

Figure 3 presents an overview of identified methods and propagation methods with their relationships.

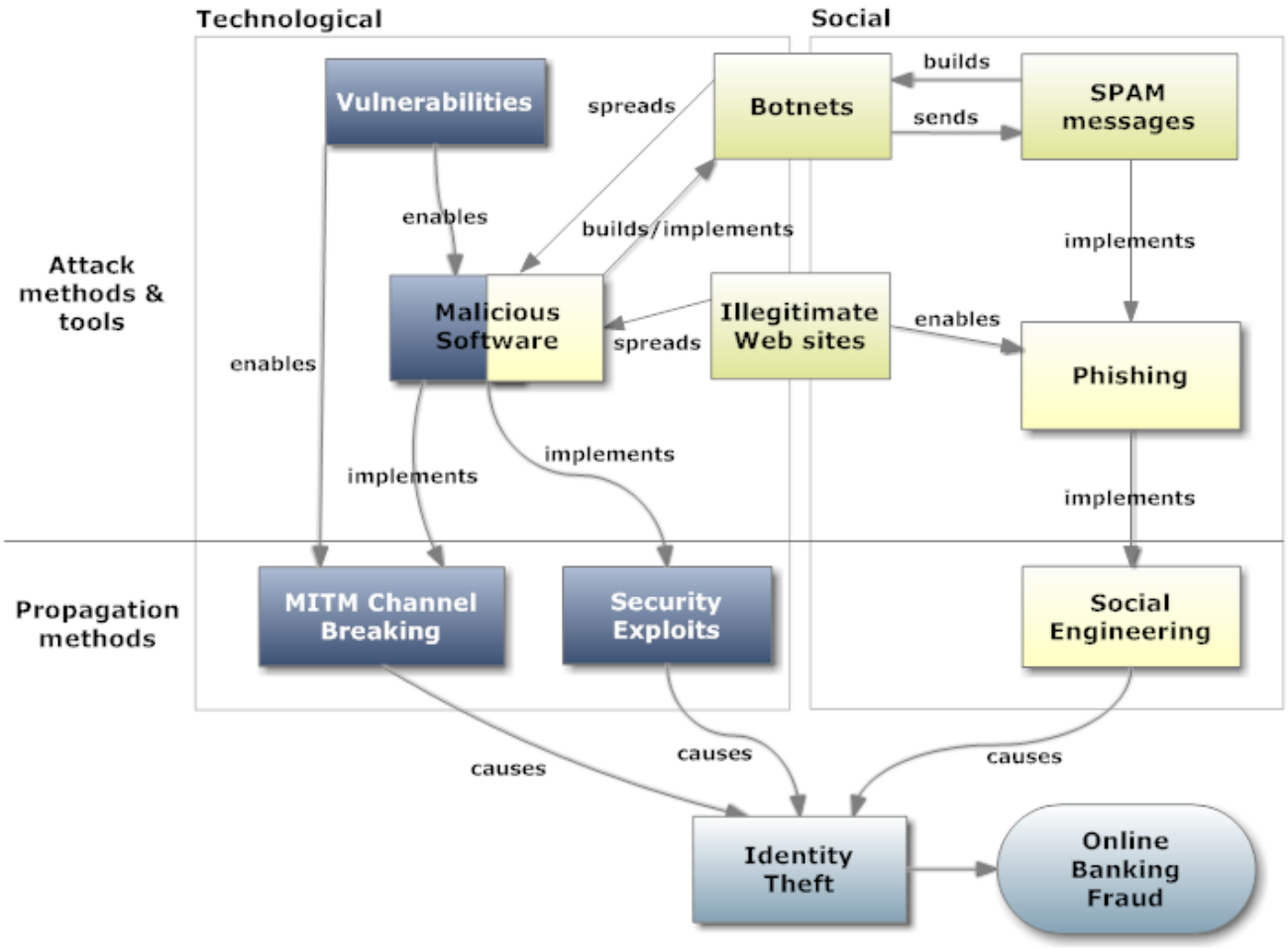


Figure 3: Attack methods and propagation methods overview

2.2.2 Risk management

In information security, Enterprise Risk Management (ERM) aims to manage the risk that an organization faces.

> **Enterprise Risk Management:** a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives (ISO 31000, 2009).

In risk management literature, a range of new terms are introduced that are related but still very distinct from each other. Before discussing the practice of risk management in online banking, these terms and their interactions need to be defined. A number of essential definitions are given by ISO/IEC 27005:2008, RFC 2828: *Internet Security Glossary* and ISO/IEC 13335-1:2004, among others.

> **Asset:** Anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission (ISO/IEC 13335-1:2004, 2004).

> **Vulnerability:** A weakness of an asset or group of assets that can be exploited by one or more threats where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission (ISO/IEC 27005:2008, 2008).
>
> **Threat:** A potential cause of an incident that may result in harm of systems and organization (ISO/IEC 27005:2008, 2008).
>
> **Security control** (or **countermeasure**): An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken (Shirey, 2000).
>
> **Risk:** An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result (Shirey, 2000).

The relationship between these concepts is as follows: Vulnerabilities are imperfections in the system's components (including its users) which could be exploited by a *threat*. Without a threat, there is no damage because there is no exploitation of the vulnerability. If the vulnerability is exploited, it leads to an undesirable outcome, which is the *risk* that the organization faces when it employs the *asset*. Note that this type of risk is fundamentally different from *business risk*, which points to the financial affairs of an organization. *Controls* (or *countermeasures*) are actions, devices, procedures or techniques that can be deployed to lower or neutralize of the threat (ISO/IEC 13335-1:2004, 2004; ISO/IEC 27005:2008, 2008; Shirey, 2000). In the context of OWBF, it is a set of standards to guide organizations and customers in building controls and control frameworks that lower risks of fraud to acceptable levels. The acceptable level of security is part of a trade-off between the level of security and the cost of achieving that level.

To minimize errors and improve efficiency, ERM frameworks have been developed to help organizations analyze, design and deploy their ERM procedures and systems.

COSO ERM Framework

COSO (Committee of Sponsoring Organizations, Treadway Commission) Enterprise Risk Management - Integrated Framework (or COSO ERM framework) (COSO, 2004) is a commonly used framework for implementing ERM. Adoption of an ERM framework is not required, but many organizations are encouraged by the requirements from the PCAOB (PCAOB, 2007). The COSO ERM framework lets organizations define their risk appetite, or the level of risk they are willing to endure, and adjust their risk strategy accordingly.

Risk appetite

In COSO, the risk appetite is the amount of risk that an organization is willing to expose itself to. There is a trade-off between the levels of security and the cost of achieving those levels. Diminishing too much risk will lead to excessive costs that outweigh the lower risk exposure.

The COSO ERM framework identifies both an internal and an external environment. Both need to be addressed by risk identification and risk analysis (COSO, 2004).

2.3 Physical environment of online banking

At this point it may be beneficial to consider the physical environment of online banking and identify the two types of threats that risk management identifies. Online banking in essence typically involves a **customer**, a **server** and an **Internet connection** as visualized in Figure 4. Also, the excluded external attack on the banking infrastructure and hard-/software rigging are illustrated.

There are a few types of attacks that are possible but are not considered by this research:

1. External attacks on infrastructure: attacks that seek to (temporarily) disable security systems from outside the physical system environment. This includes direct hacking into the system to reroute funds or do other damage.
2. Hard-/software rigging: the insertion of malicious computer instructions or the delivery of defective computer hardware aimed to provide opportunity for OWBF.

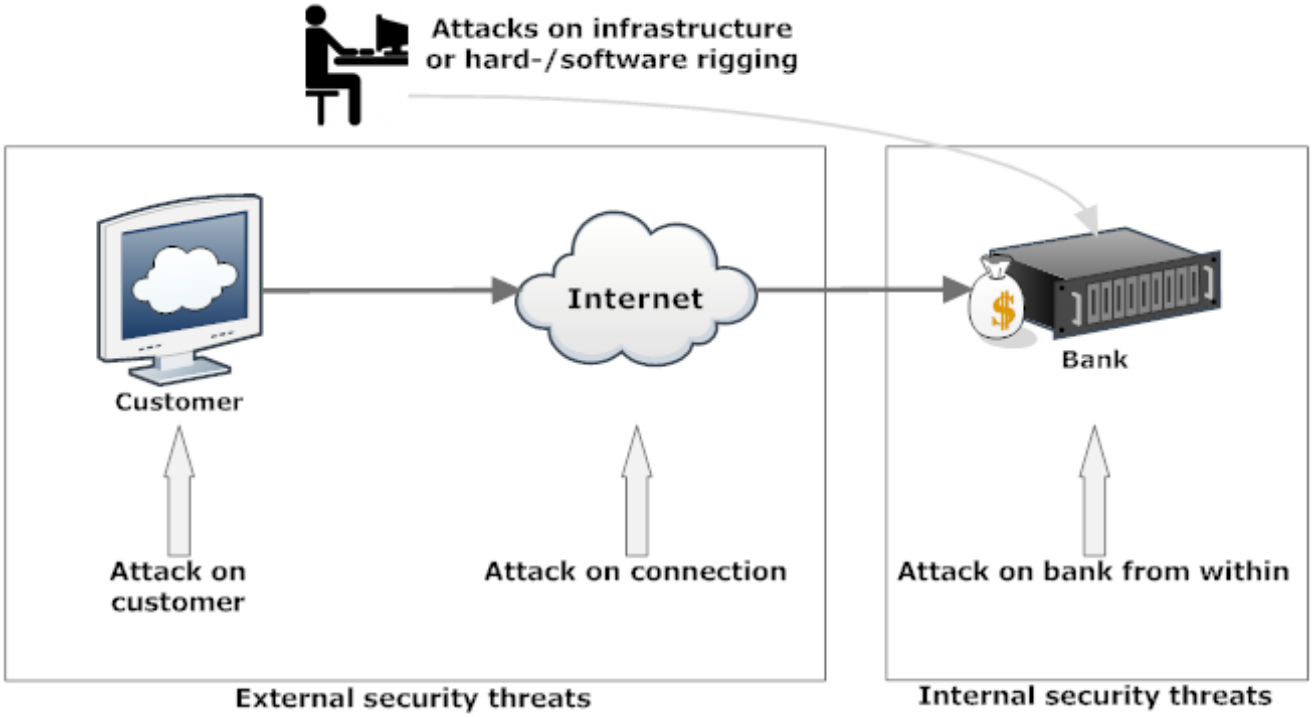


Figure 4: Physical environment of online banking

2.4 Risk mitigation and security controls

According to ISO 31000, one of the first steps in risk analysis is the location of the threat, specifically whether it is **internal** or **external** from the organization's perspective (ISO 31000, 2009). From the organization's perspective, the level of control that can be exercised over its own internal processes is larger than over the external processes in the rest of the world. Therefore, in this research a separation between the mitigation of internal and external risk is used. First, the internal security controls and control frameworks will be briefly discussed as a reference point. Then, the possibilities of managing external security through external security controls will be discussed.

Internal security control frameworks

Internal risks are mitigated using internal security controls. In order to manage, control and develop security controls, many organizations employ an internal control framework. A control framework is used to guide the organization of security controls. Large organizations such as banks are expected to adopt a control framework to guide and challenge their internal control efforts, a practice which is also required by legislations such as the Sarbanes–Oxley Act in the United States or local laws that implement directive 2006/43/EC of the European Commission.

There are numerous internal control frameworks in existence. The most cited and perhaps most relevant frameworks are discussed briefly.

1. **COBIT Version 4.1:** COBIT stands for Control Objectives for Information and related Technology and was specifically designed by the Information Systems Audit and Control Association or *ISACA* for application in IT security and control. There are four broad domains defined within COBIT (ISACA, 2007):
    - **Plan and Organize**
    - **Acquire and Implement**
    - **Deliver and Support**
    - **Monitor and Evaluate**

    These four domains result in 34 high-level control objectives. COBIT then defines over 300 lower-level objectives that should be met in order to successfully implement the framework.
2. **COSO Internal Control - Integrated Framework:** COSO Internal Control - Integrated Framework is perhaps the most popular internal control framework (Shaw, 2006). Note that this framework is different from the COSO ERM Framework which was discussed earlier.

COSO focuses on five components:

- **Control environment:** promotion of control by the organization leaders.
- **Risk assessment:** identify all risks of all entities.
- **Control activities:** build controls to mitigate the risk.
- **Information and communication:** continually inform and communicate information about the controls to stakeholders.
- **Monitoring:** gather information about the control system in order to improve them.

COSO also states that people form the main component of an organization's internal control and furthermore that guarantees do not exist in information security.

3. **ISO/IEC 27002 (formerly ISO 17799):** This standard was created by the International Organization for Standardization to provide a general model for security of information entities within an organization, along with the other standards of the ISO/IEC 27000-series. This standard is deliberately kept abstract and not an implementation guideline. Furthermore, it should be noted that 27002 is not intended to compete with COSO or COBIT but rather to complement them. ISO/IEC 27002 is the new name of an updated version of the now renamed ISO 17799. There are twelve (ten for ISO 17799) categories with their own subcategories and goals. All categories contain a list of best practices security controls and together form a 'vanilla' general purpose implementation that can be adapted to any organization.

Internal security controls

Perhaps the most widely used security control framework is ISO/IEC 27002. This standard defines three core principles, also known as the C.I.A. triad:

1. **Confidentiality:** information is only disclosed to properly authorized entities.
2. **Integrity:** information is not altered.
3. **Availability:** information is available when relevant.

These three principles cover eleven organizational areas. Although the standard is not meant to set requirements for specific types of implementations in order to make the standard applicable to many different types of organizations, it does define a number of broad areas that need to be covered by security controls:

1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security

5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

These organizational areas are all susceptible to different risks. Typically, an organization will need to assess all risks in all areas, possibly with the help of an external consulting party.

As discussed, the actual security measures themselves are called internal controls. The Sarbanes-Oxley Act identifies four sequential types of internal control: preventive, detective, repressive and corrective.

1. **Preventive:** the first active controls are preventive in nature: password-protected bank accounts and scrambled output of sensitive information (like passwords) on computer terminals are examples of preventive controls. Within Sarbanes-Oxley, fraud deterrence is part of preventive controls as they both aim to stop fraud before it occurs.
2. **Detective:** if the first two types of controls have not been successful in stopping an attack, detective controls can be used to prove a breach after the fact. Examples are access logs, virus scans and scans for suspicious activity.
3. **Repressive:** repressive controls aim to prevent any future security breach from happening. Organizations may respond by denying system access, punishment, job termination or system warnings, among others.
4. **Corrective:** at this stage, the breach has already occurred. Corrective controls try to minimize the damage or to remedy the situation are the only options left. This may include restoring data from backups, blacklisting IPs or employing fallback systems.

Together, if the set of controls is exhaustive and implemented perfectly, these controls form a complete system of protection from all information security threats, either social or technological. A proposal of the process that measures the effectiveness of an organization's information security is outlined in the standard ISO/IEC 27001. Under Sarbanes-Oxley, public organizations are required to comply (by certification) to a standard like ISO/IEC 27001, thus securing the implementation of proper information security practices. When certified, the organizations are required to continuously update and revise their information security and are subject to recertification.

External security controls

As discussed, external security controls are meant to mitigate the risks that a bank does face but has no (complete) control of. Examples of external processes are applications that run on a customer's hardware or the transmission of data between the bank and its customer. The entity usually charged with managing external risk is the Justice Department, which is arguably not a large stakeholder in any particular retail bank and is only responding to actual crimes or substantial suspicions of a crime. Moreover, the Internet does not respect national borders, whereas any national Justice Department has a jurisdiction limited to one particular country.

The aforementioned 27000-family of standards to manage internal risks requires all assets to be under organizational control in order to provide responsibility and accountability for that asset. This hardly applies to the devices and connections that process online banking. However, in practice the banks' coverage of internal control frameworks to manage external risks and vulnerabilities may not be completely absent: for instance, many internal control frameworks require the training of system users which in case of an online bank are not part of the organization itself. So to some extent, some internal controls may manage the risk of external threats.

Suggestions for improving external control

From anecdotal evidence, a number of external security controls in existence that may not be widely deployed in Dutch online banking but could still add to the level of security are identified:

1. Another possible security measure could be the implementation of **multi-factor authentication** where current systems only require one. Multi-factor authentication requires not one but at least two different tokens from the user (Birch, 2004), thus increasing the level of security with every added factor.
2. Setting up a stronger **VPN** connection than the standard SSL with certificate between the customer and the client could improve connection security.

While these controls are well-documented and widely in use, they have not all been implemented throughout all Dutch retail banks. See also Table 4.

	N-factor authentication	VPN type
ABN AMRO Bank	Two-factor, bank card and PIN	SSL with certificate
ING Bank	Two-factor, SMS and password	SSL with certificate
Rabobank	Two-factor, (personal code device and PIN), (bank card and PIN)	SSL with certificate
SNS Bank	Two-factor, personal code device and PIN	SSL with certificate
Friesland Bank	Two-factor, bank card and PIN	SSL with certificate

Table 4: Implementation of possible external security controls (ABN AMRO, 2011; ING Bank, 2011; Rabobank, 2011; SNS Bank, 2011; Friesland Bank, 2011)

Some known external security controls in OWBF

In order to better understand the external risks and their controls the first step is to compile a list of known controls that are in use today. There is no known complete list of security controls. Part of the problem is that one cannot prove that any set of security controls is exhaustive for all possible threats. Several US organizations with compelling IT security risks (including NSA, US Cert, Department of Defense JTF-GNO, the Department of Defense Cyber Crime Center, bank security specialists, among others) have compiled a consensus list of twenty security controls that are argued to be most important (The SANS Institute, 2011). Other controls have been selected from various sources (Goeijenbier, 2010; Raval & Fichadia, 2007). In Table 5, a selection of threats, risks and possible security controls for mitigating external risks is compiled. Also included are the aforementioned security controls that could increase the mitigation of external risk. A distinction is made between social and technological types of security controls, which will be discussed later in this chapter.

2.5 International situation

It is within the scope of this research to assess the current levels, frameworks and controls of online banking fraud practices in The Netherlands. However, its performance relative to peer countries may provide more insight than just absolute numbers. In order to be able to discuss the relative performance of The Netherlands, a clear picture of its position relative to comparable countries must be obtained. Countries of choice include the European nations with reasonable wealth, great Internet and online banking penetration and a strong financial sector (UK, France, Germany, Spain, Italy, Norway, Denmark and Sweden) and non-European wealthy Western nations (USA, Canada, Australia).

Criminal statistics can give a quantifiable and easily comparable picture of the current occurrences and damages per country. For crime statistics to be of value, they need to meet a number of quality requirements. Crime statistics are required to be:

1. **Absolute**. It is necessary to get the absolute number of occurrences and damages or to have relative data that can easily be converted to absolute data.
2. **Complete** (total number of occurrences, total damage, and average damage per case). Incomplete data will hinder the comparison process.
3. **Sufficient granularity**. The data will need to encompass all OWBF crimes in retail banking in that country and only that data for them to be comparable.
4. **Of multiple recent years**. Because conclusions cannot be based on only one year.

However, only a handful of countries provide crime statistics that meet all these requirements, see also Table 6. Therefore, the search needs to be broader than just criminal statistics databases. Security controls and user awareness programs and organizations may provide additional information about the resources that a country puts in for combatting OWBF.

2.5.1 Reliability of criminal statistics

Before trying to interpret OWBF data, the limitations of such data need to be discussed. First, research has repeatedly shown that official crime statistics suffer from accuracy issues. More specifically, they tend to be underreported (MacDonald, 2002; Maltz, 1977; Pudney, Deadman, & Pyle, 2000). These studies have not been able to successfully create models or rules-of-thumb to reliably correct official crime statistics, and have found them to be informative but not predictive of future crime rates. One factor that has been found to be influential in property crime rate reliability is whether the damage suffered was insured. This is rather easy to explain, since insurers will probably require a police report before accepting a case. On the subject of online fraud statistics limitations specifically, it was concluded that those should be generally treated with skepticism (Kabay, 2009).

This research argues that online fraud is not always detected and moreover, not always reported if detected. So, it is improbable that any predictions on the future OWBF crimes can be derived from these statistics. But, if large differences between countries or cultural areas are found, they may well be real and be informative.

Furthermore, it must be noted that a crime report cannot automatically constitute a crime. Every year thousands of false police reports are filed for all kinds of reasons, one being to enable insurance fraud. Hence, governmental criminal statistics are fundamentally different from occurrences and damages that are reported by banks, such as the ones published by the Dutch

Banking Association (*Nederlandse Vereniging van Banken, or NVB)*. However, at the same time it would also be naïve to dismiss all crime reports since many of them will be the result of an actual crime.

Threat	Risk	Security control	Type	Control description
Attacker may steal authentication information	Broken integrity, confidentiality of data	Spam filters at customers	Technological	Spam filters either as Internet Service Provider, e-mail provider or e-mail client software level can prevent an e-mail from posing a threat by preventing the user from seeing it.
		Heighten awareness	Social	Commercials, websites, brochures, et cetera can improve the awareness of users to OWBF and make them more suspicious of their online activity.
		Phishing filters	Technological	Phishing filters in web browsers, ISPs or search engines can warn users before they enter a malicious website.
Attacker may run malicious software	(Indirect and direct) Broken integrity, confidentiality of data	Anti-Malware software at customers	Technological	Anti-virus programs, firewalls, et cetera can prevent automated and social engineering attacks by warning users.
Attacker may run illegitimate website	(Indirect) Broken integrity, confidentiality of data	Takedown of illegitimate websites	Technological	Illegitimate websites have been taken down by banks and other stakeholders (NVB, 2011), preventing them from doing more harm.
Attacker may modify transactions	Broken integrity, confidentiality of data	Encrypted connections (TLS/SSL) and security certificates	Technological	Cryptography prevents tampering with the connection between the client and the bank. Certificates ensure the authenticity of the server to the client. However, clients have been reported to fail to understand certification warnings.
		Entity authentication	Technological	Personal credentials (usually a username and a password) are a secret shared between authorized parties only.
		Transaction authentication	Technological	A secret shared between the bank and the customer carried by a mobile text, hardcopy or electronic device ensures authenticity of the user.
		Electronic Data Interchange (EDI)	Technological	Agree on a secure communication protocol between bank and client.
		Two-factor authentication	Technological	Two-factor authentication requires not one but two different tokens from the user (Birch, 2004), thus increasing the level of security.
		Virtual Private Network (VPN)	Technological	Set up a private encrypted connection between hosts over the Internet.

Table 5: Some known security controls for managing external OWBF risks (The SANS Institute; Goeijenbier, 2010; Raval & Fichadia, 2007)

2.5.2 Current situation in Western countries

In this section, an overview of the current OWBF situation in peer countries is presented, with an emphasis on the size of the issue, the legal response and the mitigation of risk using external controls. Perhaps the management and/or economic cultural model used is a factor of some importance, therefore the countries are categorized according to their generally accepted main economic and/or management cultures: Anglo-Saxon, Rhineland, Nordic and Mediterranean Europe.

Research has identified three basic types of organizations participating in registering OWBF, each with their own pros and cons:

1. **Government:** all reviewed governments compile and publish national and local crime statistics. However, most do not provide the information with enough detail to assess the level of OWBF activity in that country. Also, not all governments provide data on subsequent years in recent history. Finally, the definitions of OWBF may differ between nations.
2. **Industry:** most countries have a main banking lobby organization. Some bank industry lobby groups provide meaningful crime statistics themselves while others just inform their members and the general public about OWBF. The quality of the crime data differs greatly which influences its reliability. For instance when comparing Dutch and UK industry data: Financial Fraud Action UK provides much more detailed data than the NVB, see also Table 10 in Appendix A. Moreover, the procedures that are part of the methodology of these numbers are usually not peer-reviewed or authorized by any other than the publisher.
3. **Consumer organizations:** many countries have active consumer organizations that inform the public and encourage them to file complaints. However, the reliability of this data is questionable since there is no control mechanism or legislation present to audit the data while the consumer organizations could have incentives to modify or misrepresent the data. Also, it's not always possible to extract the actual crimes from the *attempts*. Finally, consumers might not even know that they have been attacked.

International collaboration

Before discussing the countries individually, it should be noted that the European Union has undertaken a few projects that aim to motivate their member states to create external controls. By discussing them now it becomes unnecessary to repeat the same findings during the per-country discussions.

1. **Safer Internet Centres** (Europe's Information Society, 2009)**:** this program promotes awareness websites as an external control in all European countries that are discussed. Such websites are meant to warn and educate users on the risks of online banking.
2. **Council of Europe Convention on Cybercrime:** in 2001, the Council of Europe's Committee of Experts on Crime in Cyber-space created the Convention on Cybercrime (Council of Europe, 2001), a treaty that aims to counter OWBF by requiring its signers to implement necessary legislation that prohibits and punishes it. This treaty was signed and ratified by all European countries that are compared in this research except for the UK, although the UK claims to be compliant (Council of Europe, 2010). Furthermore, it was signed by Canada and the USA and ratified by the USA (Council of Europe, 2011).
3. An organization that might also be relevant to this discussion is the **European Electronic Crimes Task Force (*ECTF*)**. The ECTF is a collaboration organization between the US Secret Service and the Italian and UK police departments (U.S Department of Homeland Security, 2009; U.S Department of Homeland Security, 2010). Part of the goal of the ECTF is to prevent, among others, online financial fraud through the creation of a collaborative framework. The outcomes, current status or effectiveness of this initiative remains unknown due to the fact that it does not publicly share any more information than a number of press releases. Also it only covers three countries.

Anglo-Saxon countries

The **United States** has multiple organizations tending to registering OWBF (United States Department of Justice, 2004). Perhaps the most relevant for this research is the Internet Crime Complaint Center (*IC3*). This source records the number and nature of complaints that are sent to them by users. Users are encouraged to file complaints even if there has been no actual crime but rather an attempt, and there is no identifiable method of verifying complaints. Therefore, from the IC3 data it's impossible to obtain any reliable OWBF occurrence statistics. Other sources are available but are of a survey nature (CyberSource, 2011) or also rely on complaints (Federal Trade Commission, 2008). No viable governmental source of data was found.

In **Canada** there is no centrally mandated cybercrime statistics recording in the government, according to a recent report (Canadian Centre for Justice Statistics, 2011). Also, the report states the difficulty of working without a central, international definition of cybercrime. Canada's banking lobby organization does not publish any relevant OWBF-related statistics.

Australia also has no usable official OWBF crime data, but does have an electronic crime working group and awareness program (Australian Federal Police, 2011). An identity theft awareness

website created by both the government and the banking industry is available (ABA, AHTCC & ASIC, 2011), but provides no OWBF statistics.

In the **United Kingdom**, the main financial lobby group provides detailed statistics on online banking fraud (Financial Fraud Action UK, 2010). These statistics show a strong rise in the last seven years, and discusses the popularity of phishing attacks and money mule recruiting.

Money mules are an essential part of the OWBF process. The money mules are recruited by criminals to funnel the stolen money to their bank accounts so that the funds can be withdrawn in cash (Moore, Clayton & Anderson, 2009).

There is no data on the number of cases or their average damage caused. Still, it's notable that the statistics on OWBF in the UK are much better than most other countries.

Rhine model countries

As discussed, **The Netherlands** has a very high rate of both Internet and online banking penetration (comScore, 2010; Innopay, 2010). The official governmental statistics agency provides insufficient granularity for this research (CBS, 2010). In a recent report compiled by the country's main banking lobby group, the total OWBF damage in 2010 was reported to be 9.8 million euros (NVB, 2011), which is a very significant increase from the years before. In 2008, the damages totaled to 2.1 million euros, in 2009 1.9 million euros. So this figure almost quintupled in the last year alone. There is no mention in the report about what or how the data was measured.

OWBF is illegal and punishable under Dutch law (Ministry of Internal Affairs, 2010) as in many other countries (see Table 6). Investigation in The Netherlands is carried out by the High Tech Crime unit of the KLPD (Korps landelijke politiediensten, 2010), but there are many governmental bodies involved in the prevention and investigation of online banking fraud, including local police and anti-terrorism units. Numerous measures to inform the public about the threats of OWBF exist from both the government and private organizations endorsed by the government (Rijksoverheid; NVB, 2010).

In **Germany**, the government provides the most usable information on OWBF themselves (Federal Office for Information Security, 2009). This data shows that cybercrime in general is slowly rising. Since these numbers include not only banking fraud but rather all online fraud, it's impossible to reach any solid conclusions using this data. However, it is stated explicitly that online fraud related to banking is a big problem and is expected to grow in the near future.

The only usable statistical government data on OWBF in **France** dates back to 2004, when the Senate asked for them (Sécurité intérieure et des Libertés Locales, 2005), but no additional data is

available for comparison. Furthermore, no viable data was found at lobby organizations or consumer groups.

Nordic countries

In **Norway**, the government does not provide statistical data on OWBF crimes (Statistics Norway, 2011). Also, Norway's banking lobby organization, FNO, does not seem to publish any information related to online banking fraud statistics but does endorse legislation combatting it. Although Norway is no member of the EU, it has signed and ratified the Convention on Cybercrime, thus its legislations and awareness programs are in existence.

Denmark also does not provide usable statistics through its government (Statistics Denmark, 2011) or its banking lobby organization (Finanstilsynet, 2011).

In **Sweden** the official police statistics do not have sufficient granularity to drill-down to OWBF or even cybercrime (BRA - National Council for Crime Prevention, 2011). Also, they only describe reports to the police, which could include unverified claims. Sweden also has a high rate of online banking penetration and thus increasingly relies on it for retail banking.

Mediterranean countries

Spain and **Italy** both publish significantly less crime statistics than their Western European counterparts. There are some relevant reports, for instance from the Guardia di Finanza (Guardia di Finanza, 2011), but they also lack the level of detail needed.

Country	Crime data	Government controls	Regulatory situation[1]
NL	Available from private organization only (NVB, 2011)	Awareness websites	Prohibited and actively prosecuted by ratification of the Convention on Cybercrime.
DE	Available from police records only (Bundeskriminalamt, 2009)		
UK	Available from private organization only (Financial Fraud Action UK, 2010)		Prohibited by law
AU	Unavailable from police records (Australian Institute of Criminology, 2010), or incomplete from other government organization (ACCC, 2010)		
CA	Unavailable		Prohibited and actively prosecuted by ratification of the Convention on Cybercrime.
US	Available from private organization (Federal Trade Commission, 2008)		
NO	Available from police records but insufficient granularity (StatBank Norway)		
SE	Available from police records but insufficient granularity (National Council for Crime Prevention Brå, 2010)		
DK	Unavailable		
IT	Unavailable		
FR	Unavailable for recent years (latest from 2004 in response to a direct request from the Senate)		
ES	Unavailable		

Table 6: Overview of Internet fraud situation per country

[1] An overview of the world's cybercrime laws is available at http://www.cybercrimelaw.net/Cybercrimelaws.html

2.6 Conclusions and direction for research

There has been some debate on the definition of cybercrime. In order to include all relevant cases of online Web-based banking fraud (OWBF) now and in the future, it is necessary to use a broad definition of cybercrime as a basis for the definition of OWBF. The definition given by (Gordon & Ford, 2006) is the one used for this research.

The identified methods used to execute OWBF attacks are phishing, security exploits and man-in-the-middle attacks. Tools that have been identified are botnets, spam messages and malicious software. Two broad categories of OWBF threats have been identified: technological and social. They are sitting on either side of a spectrum and many OWBF attacks have both technological and social aspects. These categories require a fundamentally different type of defense: while technological threats need only adequate technological controls to be almost automatically neutralized, preventing a social threat requires the action or inaction of human being(s), perhaps the customer. This discussion furthermore identifies three propagation methods used in OWBF: two technological methods (Man-in-the-middle attacks and security exploits) and one social method (social engineering). All identified OWBF methods use identity theft to trick the retail bank into thinking that they are actually communicating with the legitimate party while they are not, from the perspective of the bank.

Enterprise Risk Management (ERM) aims to deal with the risks that an organization faces. The COSO Internal Control framework is a common framework to implement ERM. Part of COSO Internal Control is the identification of risks and the deployment of internal controls to mitigate that risk. COSO also identifies external risks that require a response from the organization, but the control over external processes is probably limited. Internal controls and their frameworks have been developed to worldwide adopted standards with mandatory certification for most banks. However, this is not the case for external controls. Still, banks do have some controls at their disposal to mitigate external risk: legislations and awareness programs have successfully been deployed in all discussed countries and the swift ratification of the European Convention on Cybercrime is also worth mentioning.

Legislations like Sarbanes-Oxley, standards like ISO27000 and their implementation frameworks are only concerned with the bank's internal risks and not the external ones. Still, there is some overlap between internal and external security controls, allowing at least some external control. Arguably, the management of internal risk at Dutch retail banks is handled very well since there is little evidence to suggest that any significant security breaches have taken place in recent years, although internal security breaches would possibly not be made

public for commercial reasons. There is evidence that suggests the claim that banks, governments and standards organizations have spent considerable resources towards managing internal risk by implementing various ERM and control frameworks. This suggests that most financial loss due to OWBF is incurred due to lack of effective control of external risk. However difficult, there is evidence that suggests that the banks still have some readily available controls at their disposal, but they are not implemented. The reason for this might be financial, commercial, or something else. Hence, the focus of this research will be external controls of both the social and technological locations, see Table 7.

OWBF security controls	Technological	Social
Internal	Out of scope	Out of scope
External	Relevant	Relevant

Table 7: Types and locations of security controls and their relevance for this research

As discussed, there are many national and international organizations that aim to combat OWBF. There are three basic types of organizations participating in quantifying OWBF: Government, industry and consumer organizations. Unfortunately, there are many different ways of documenting and measuring the occurrences and financial damages of OWBF in use today. There is little evidence to suggest that either national or international organizations are effectively aggregating and comparing criminal statistics between countries or otherwise thoroughly coordinate their efforts. Moreover, there is no framework on which to judge a countries' relative performance to others, hence it becomes increasingly difficult to identify any preferred OWBF strategy. Also, there is still lack of a single definition on cybercrime, and while there is no evidence that this causes practical problems, the creation of a generally accepted definition of OWBF would be a logical first step in the fight against it.

One perhaps simpler task is creating the legislation that allows for individuals and organizations to be prosecuted and punished for OWBF. This legislation was successfully implemented throughout the Western world.

One of the goals of this research is to assess the amount of incidents and monetary damages related to OWBF in various countries. In practice, however, this has proven to be a difficult task, because:

1. There are different methods of recording this data, making direct comparisons difficult.
2. In general, there is not much data publicly available.

See Appendix A: OWBF statistics for an overview of found OWBF statistics in The Netherlands and its peer countries.

3 Methodology

3.1 Introduction

In this chapter, the methodological aspects of the study will be explained. First, the broad research methodology will be presented. Then, the research questions will be formulated. Next, the interview design and interview summaries will be discussed.

3.2 Research methodology

This research aims to deepen the knowledge of the OWBF situation in The Netherlands with an emphasis on the benefits of international cooperation and external controls. The research method of choice is qualitative analysis of individual semi-structured interviews in a single-round setup (Blumberg, Cooper, & Schindler, 2005). This method used involves a number of steps, adapted from (Soy, 2006):

I. **Determine and define the research questions**
II. **Select the experts and determine results gathering and analysis techniques**
III. **Prepare to do the interviews**
IV. **Interview the experts**
V. **Evaluate and analyze the results**
VI. **Prepare the report**

There are a number of known issues that relate to the case study method which are also applicable to structured interviews (Myers & Avison, 2002). These are discussed below in order to understand and disclose this method's limitations.

I. **Controlled observations:** in this type of research, it is improbable or even impossible to perform a completely controlled experiment found in a laboratory-setting. Instead, it is important to take advantage of any natural controls that are in place. For instance, the amount of OWBF activity is assumed to be constant during the results collection process.
II. **Controlled deductions:** this research method lacks the mathematical foundation upon which quantitative research is usually based. The lack of the rules of algebra does put an emphasis on the correct usage of propositions and conditions, since the application of algebraic rules can provide a built-in check against errors which cannot be provided by words and sentences.
III. **Replicability:** these exact cases that are researched cannot reasonably be replicated by independent researchers without access to all the same experts. Note also that the interview subjects of this research are not a sample of a population and thus any

conclusions cannot be generalized. This is an important limitation of the qualitative research method. However, this research could still be used to investigate other cases using the same theory and in the process adding to the knowledge that this research aims to provide. Still, a researcher should be able to replicate the conclusions of this research using the observations as input to test the theory.

IV. **Generalizability:** as discussed, any results are not generalizable to anything else than the experts that are interviewed.

3.3 Research questions

From the literature review and the international background, the main research question emerges:

How can the Dutch banking organizations improve the effectiveness of social and technological external OWBF security control?

From the main question a number of sub-questions emerge:

I. **How effective are the technological external security controls for OWBF?**
II. **How effective are the social external security controls for OWBF?**
III. **How can the effectiveness of the technological external security controls for OWBF be improved?**
IV. **How can the effectiveness of the social external security controls for OWBF be improved?**

3.4 Interview design

While structured interviews offer the advantage of simple analytics of a large number of returns, they do not offer the flexibility that is required. On the other hand, open interviews offer maximum flexibility without any guarantee as to which questions are answered. Hence, using open interviews could make it difficult to compare the different experts with each other. A viable middle-ground is the semi-structured interview, which does require a set of prepared required questions and still offers the interviewer the flexibility to dive into any issue that comes up with additional improvised questions.

The interviews will consist of two parts: the first part sets the context of the expert and the organization. The second part of the interviews holds the specific knowledge that the expert can add to the research. The semi-structured interview design is presented in Appendix B.

3.5 Interview summaries

A summary of the results of each interview will be presented as a single chapter. This chapter will have the following structure:

1. **Introduction:** a general introduction into the expert and the organization he or she works for.
2. **Importance of OWBF:** the perceived importance of OWBF to the expert, his organization and Dutch banks in general
3. **(International) cooperation:** the level and effectiveness of the national and international cooperation between banks, governments, lobbyists and other stakeholders.
4. **Effectiveness of technological and social external controls:** before discussing any improvements, first the current effectiveness is discussed.
5. **Satisfaction of achieved level of risk:** states how the effectiveness of the external controls impacts risk, especially how it relates to the bank's risk appetite.
6. **Suggestions for external security controls:** lists the technological and social external controls that the expert believes may help mitigate OWBF risk.
7. **Summary**

3.6 Epistemological stance

In qualitative research, the list of common classifications of different epistemologies consists of positivist, interpretive and critical studies (Chua, 1986; Myers & Avison, 2002). This particular research seeks to increase the understanding of the OWBF phenomenon as it is understood by security experts in the field. Therefore, a descriptive positivist approach is chosen. Positivism can also be grounded in theory, but that does not satisfy this project's need to understand the current practices and issues surrounding the subject.

Interpretive research does not recognize the objectivity or factuality of reality, but rather focuses on a person's interpretation or subjective meanings of a phenomenon. This, along with the fact that interpretive research requires extensive time in the field, renders it insufficient for this research.

Critical research seeks to find structural contradictions in our social systems in an attempt to overcome them. It is also not viable for usage in this instance, because subjective interpretations that give birth to these contradictions will not adequately answer the research questions.

As is a given when performing qualitative research, the conclusions of this research are not generalizable to the population. Instead, any conclusions can be propositions at best, if generalized to the population. The conclusions will, however, hold for the specific cases.

3.7 Sample selection

Possible subjects for the interviews include any reliable and knowledgeable security expert with experience in OWBF security in Dutch retail banks' online applications. The first and most obvious targets are security managers at the banks. Next, there are multiple large IT advisory companies that perform audits and give advice to the banks on how to improve their OWBF security situation. The Dutch banking lobby or certain governmental agencies such as the Dutch Central Bank ("De Nederlandse Bank", or *DNB*) or the NVB may also be of interest. Subjects will be contacted using email and will be scheduled for one interview of 60 to 90 minutes. Subjects will be carefully selected and questioned in advance of the interview to make sure that they possess the knowledge required to participate in this research.

Appendix C contains an overview of the invitations that were sent out.

3.8 Results analysis

The original interviews are recorded and for every interview a summary is created. As analysis method, content analysis is used (Babbie, 2007). The accompanying analysis unit for that method is lines. Using coding as a way of processing, the summary of each interview is transformed to a set of answers that is comparable with peer interviews. These answer sets are printed as part of this thesis.

The expert interviews (A, B, C) will be held first. This will be the main interviews. The information that is provided to the experts in interviews B and C will overlap with previous interviews, and answers given in any interview will be part of later ones if desirable. The source of this information will not be disclosed during the interview nor will the experts be able to identify the difference between information from the interviewer or from previous experts.

One issue with a single-round interview approach is that the third and last expert will not be able to get his suggestions peer reviewed. Therefore, an extra round of validation is used. After the main interviews and initial validation, another interview (D) will be held with another expert, which will be used to validate the combined answers of the first three experts. This will enable the validation of the suggestions of the third expert, as well as strengthening the validations of the first two experts. Therefore, it offsets some of the limitations of the single-

round interview method. Any statement not verified by (D) will be rejected. Any new statements by (D) cannot be verified and are presented for future research.

This method aims to 'circle around' a scientific question by approaching it from multiple angles by a discussion among peers, thus increasing the understanding of the phenomenon. See Table 8 for an overview of interview input and validation.

Interview	Uses input from	Is validated with
A	-	B, C, D
B	A	A, C, D
C	A, B	A, B, D

Table 8: Interview input and validation

3.9 Disqualified methodologies

In the literature, a number of alternative research methods have been identified (Myers & Avison, 2002; Babbie, 2007) that have been disqualified for several reasons. This section briefly discusses those methods.

- **Ethnographic research:** ethnographic research can be a useful method to describe how a human observer (ethnos) perceives reality in his own subjective ways. A clear issue of using ethnographic research in this instance is the fact that a significant time in the field is required, which is not achievable within this research project.
- **Grounded theory:** in grounded theory instead of hypothesis formulation and testing using collected data, observations are constantly gathered and compared with previous ones (Babbie, 2007). The goal is to formulate new theory based on observations. In essence, this method is the reverse of many other methods. Grounded research is unpractical for this research because its questions are not answered by the study of sequential observations in time. Also, the creation of new theoretical frameworks is not within the scope of this research.
- **Action research:** this method allows for a merger of research and praxis and is very relevant to research in information systems as they usually exist to fill a real-world need. However, it would require a direct observation of OWBF and the procedures of banking security experts, which is impossible to achieve within this research project.

In the next four chapters, the interview summaries of all experts are presented.

4 Interview A: HEC (MS)

Name: *Mr. Dr. M. (Marcel) Spruit*

Positions:

1. *Lector Information Security, chair of Cyber Security & Safety at The Hague University*
2. *Advisor at HEC (The Centre of Expertise)*

Date: *July 14, 2011*

Location: *The Hague*

4.1 Introduction

Marcel Spruit is lector Information Security at The Hague University (*HHS*) and an Advisor at The Centre of Expertise (*HEC*), an independent foundation concerned with issues relating to ICT and management in the public sector in The Netherlands. HEC provides the Dutch governmental agencies with strategic advisory, audits, (interim-) management and education related to information technology (HEC, 2011). As a lector in Information Security at The Hague University (*HHS*), Mr. Spruit performs academic research in applied IT. HHS is a large (under-) graduate school located in The Hague, employs 1.815 people and offers programs to about 21.300 students (The Hague University, 2011).

4.2 Importance of OWBF

OWBF is certainly a concern for the Dutch banks. Although retail banks are not clients of Mr. Spruit, the Dutch Ministry of Finance which oversees the Dutch banks, is. The Dutch government is deeply concerned about cybercrime in general, and OWBF is one of the current issues in cybercrime.

4.3 (International) cooperation

There is certainly room for more effective international cooperation in combatting OWBF. There are even more organizations that are concerned with OWBF than mentioned in this research. But they all have their own agenda, scope and expertise. This has led to difficulties in coordinating the efforts of all these organizations and making them effective. When large numbers of organizations attempt to work together without coordination, the effectiveness of their efforts tends to shrink. An attempt to coordinate these efforts in The Netherlands is a Web site called "*Samen Tegen Cybercrime*" ("Together against cybercrime") (NICC - ICTU, 2011). This particular coordination is based on network structures, which poses its own difficulties (Provan & Kenis, 2007).

But there is also a clear cultural problem with international cooperation: where the Dutch tend to communicate on the same level until some compromise is found (Polder model), other

cultures might opt for the creation of a new organization to oversee the others. There are multiple solutions to this problem for both the Rhine and the Anglo-Saxon models, but there is no single solution for both of them. International cooperation is hard not due to technological or organizational issues, but rather due to political and cultural differences.

4.4 Effectiveness of technological external controls

In general, the technological controls in place today are necessary and perform well. The remaining risk is accepted and falls within the risk appetite. Any further decline of risk will come at too large a cost. Also, there is the trade-off between security and ease-of-use and functionality, which will also be out-of-balance if the banks seek to decrease their risk exposure. The man-in-the-middle attacks are the biggest concern right now.

4.5 Effectiveness of social external controls

The current social controls in place are effective, but do not perform as well as the technological ones. People will always try to find the easiest way to do their banking online. Most people are aware of the security risks and actively seek to minimize their risk. However, there has always been a smaller group of people who are less willing to minimize their risk. The focus of the banks nowadays is to move people of the latter group to the first, using awareness campaigns. However, in the end the risk of social threats is accepted just as the technological ones are.

4.6 Satisfaction of achieved level of risk

It is hard to say what the banks feel is an appropriate amount of risk, even from inside a bank. There will be many opinions and emotions will also play a role.

4.7 Suggestions for external security controls

Basically, there are two types of improvements that banks can implement: those that cost less than the damage they prevent or those that cost more. As a profit-seeking entity, Dutch banks will only implement the former type. This is a result of a security-cost trade-off.

Suggestions are:

- **Technological**
    - **EDI and VPN connections:** first of all, an EDI is a type of VPN connection and not an implementation by itself. Also, the SSL method that is used by all online banking is already a form of VPN. Using other forms of VPN will not solve the inherit problem of MITM channel breaking attacks, and so there is no significant advantage to be gained. The current measures should be maintained as VPN does provide more control.

  - **Multi-factor authentication:** this option may decrease the risk of OWBF a bit, but it does not address the biggest threat (MITM). Hence, it will probably not be worth the effort. The current measures should be maintained.
  - **Anti-virus software:** if banks actively help their customers acquire and install anti-virus software, it could perhaps minimize the risk of falling victim to malicious software attacks. According to (MS), the banks should consider implementing this control.
  - **Dedicated machines:** in theory, an effective technological control would be the usage of a closed box to perform online banking and only online banking. This device would be psychically closed using resin and use secret and closed protocols for communication. This would almost certainly render the 'business case' undesirable for an attacker. However, I do not expect this option to be cost-effective.

- **Social**
  - **Awareness:** any new threats or loss of focus will be a valid reason to start a new awareness campaign, which will reduce the risk of social threat for a while. In this sense, awareness campaigns have a purpose and should be continued. However, intensifying them is not recommended to gain more external control.
  - **Cooperation:** the customers are best served when information is sent by their own banks. The average customer does not know and thus does not trust third-party organizations like the NVB. Therefore, the awareness campaigns could possibly be more effective if communicated by the retail banks instead.

4.8 Summary

As an IT advisor to the Dutch Ministry of Finance, as well as a lector in information security, Mr. Spruit has extensive knowledge about Dutch banking security. He recognizes the importance of effective cooperation in the fight against OWBF, but also mentions the difficulties of cross-cultural and cross-border cooperation. Both the technological and the social external OWBF controls are working well with respect to the security-cost and security-ease of use-functionality trade-offs. Possible improvements include anti-virus software, dedicated machines, awareness and cooperation between banks.

5 Interview B: Ernst & Young (SS)

Name: *ir. S.P. (Shyam) Soerjoesing RE*
Position: *Project manager IT Audit at Ernst & Young IT Risk and Assurance*
Date: *July 19, 2011*
Location: *Amsterdam*

5.1 Introduction

Ernst & Young (E&Y) is one of the informal "Big Four" accountancy and professional services firms in the world. Specifically, E&Y provides Advisory, Assurance, Tax and Transaction services. In numbers, E&Y reported a total turnover of 21.3 billion US dollars in fiscal 2010 (Ernst & Young, 2010), placing them third behind Deloitte and PwC. E&Y's 141.000 employees work in 140 countries, globally. E&Y provides IT Security and Risk Management services to the majority of the Dutch retail banks.

5.2 Importance of OWBF

In his current role as Project manager IT Audit, Mr. Shyam Soerjoesing works for the majority of the big Dutch retail banks and is directly concerned with their IT security issues. Being primarily concerned with auditing financial statements, in his work OWBF is primarily reflected in certain intangible assets such as image and goodwill that banks report on their financial statements.

As far as the relevance to the banks is concerned, this question is difficult to answer by anyone other than the banks themselves. However, a recent E&Y survey among nearly 1600 organizations in 56 countries concluded that the majority of respondents perceived an increase in the level of risk they face due to cloud computing, mobile banking and social networking and about a third of those respondents work in the financial sector (Ernst & Young, 2010).

For Ernst & Young in general, OWBF is very relevant. E&Y's retail banking clients recognize OWBF as an important concern and are in an ongoing battle against organized crime on the Web.

5.3 (International) cooperation

Much of the proposed cooperation is already in place and works well. The banks are continuously seeking to improve their information security measures and policies. A number of organizations, such as the PVIB (Platform for Information Security), play a vital role in combatting OWBF threats, for instance by holding meetings among the security experts of the Dutch banks. However, any change in the security measures is kept secret, if possible. In a

competitive market, security measures are trade secrets and can provide competitive advantages over other banks. It is not security by obscurity.

5.4 Effectiveness of technological external controls

The technological controls of today largely reflect the risk appetite of the banks and are subject to trade-offs with costs, ease of use and quality.

5.5 Effectiveness of social external controls

Really the only relevant social external control is awareness. These are very important in getting a grip on the external risks of banks. The awareness campaigns today are adequate.

5.6 Satisfaction of achieved level of risk

It is not easy to assess the satisfaction of the banks from my position. However, the aforementioned research survey indicates that organizations continue to increase their efforts to prevent OWBF threats (Ernst & Young, 2010).

5.7 Suggestions for external security controls

Dutch banks need to optimize their risk appetite and adjust their security just like any other organization. One of the trade-offs is the aforementioned risk versus costs (SC), also known as risk appetite in COSO. There is also an inherent trade-off between security, ease-of-use and functionality (SFE) associated with these decisions. Any measure that seeks to improve the level of security will only be considered if it negatively impacts ease-of-use or functionality in an undesirable way.

Suggestions are:

- **Technological**
    - **VPN and EDI:** I would agree with (MS) on this alternative. It is important to recognize that MITM of attacks cannot be fully prevented using any known technology such as encryption or certificates. The weakness can be found during the initialization of the connection. During this time, the connection is vulnerable.
    - **Multi-factor authentication:** this method will not add significant security and will decrease the ease-of-use of the application, with the exception of the facial recognition option discussed ahead. The current measures should be maintained.
    - **Custom applications instead of browsers:** using custom applications instead of browsers for Internet based banking will also not solve the problems. These applications can easily be patched using malicious software distributed using existing tools such as botnets and phishing messages.

- **Facial recognition:** one thing that has the potential to add to the level of security without running into too many costs is the addition of facial recognition software in online banking. Nowadays, many if not most online banking devices have a webcam. It could be used to add biometric authentication as an addition to the current methods, requiring any criminal to mimic the appearance of the victim in order to do a transaction. I believe this may be doable with respect to both the SC and SFE trade-offs.
- **Dedicated machines:** this would not work because of the trade-off issues mentioned by (MS).

- **Social**
  - **Awareness campaigns:** in general, these campaigns are essential and executed well with respect to the cost-security trade-off. The banks must account for the fact that at some point, the image of the bank can get hurt if the customer's distrust towards online banking increases. That way, adding more awareness campaigns might hurt the bank's financial position more than the actual OWBF damage does.

5.8 Summary

As a Project manager IT Audit at one of the big four accounting and professional services firms, Mr. Soerjoesing is directly involved in the Dutch financial industry. He recognizes the effectiveness of the current anti-OWBF organizations such as the PVIB. Both the technological and the social external OWBF controls are working well with respect to the security-cost and security-ease of use-functionality trade-offs. One possible improvement that could prove to be very effective is the addition of facial recognition to the online banking transaction process. Awareness campaigns are essential to the fight against OWBF, but care must be taken to not hurt the bank's image in the eyes of the customers.

6 Interview C: PwC (TM)

Name: *Mr. A.J.M. (Tonne) Mulder RE, CISA, CISSP*
Position: *Director Systems & Process Assurance at PwC*
Date: *August 8, 2011*
Location: *Amsterdam*

6.1 Introduction

PwC is also one of the informal "Big Four" accountancy and professional services firms in the world. Its services are Audit & Assurance, Consulting, Tax, Transactions, Crisis Management and Human Resource Services. In numbers, PwC reported a total turnover of 26.6 billion US dollars in fiscal 2010 (PwC, 2011). PwC has a total of 161.000 employees, globally. PwC provides IT Security and Risk Management services to the majority of the Dutch retail banks.

6.2 Importance of OWBF

As a Director Systems & Process Assurance, Mr. Mulder is directly involved in the systems that power financial institutions. He is concerned with trading systems that facilitate the buying and selling of financial instruments by financial institutions. These systems, Mr. Mulder argues, are quite comparable to the systems that power online banking transactions. His work also requires him to be involved in large cases of fraud like the recent CO2 quota fraud.

I believe the relevance of OWBF to the banks is very substantial. Our retail banking clients are very concerned with OWBF. They are, however, bounded by their risk appetite in the form of a trade-off between security and costs. PwC has the majority of Dutch retail banks in its portfolio.

6.3 (International) cooperation

There already is a lot of cooperation in place. But there is certainly an opportunity for more effective cooperation between governments, banks, universities and security specialists. However, one must not underestimate the difficulties of cross-border and cross-cultural cooperation. Additionally, the banks are exceptionally closed to the public.

6.4 Effectiveness of technological external controls

Banks, like any organization, will always prefer to use technological controls to minimize their risk before they use social ones. However, history has shown again and again that no technological control is 100% effective. Banks also must take care not to put too much emphasis on security to the point that the functionality of the application suffers.

6.5 Effectiveness of social external controls

The only effective social control is awareness. It works for the majority of people, so they are reasonably careful online. However, there is always a group of users that is not effectively motivated by awareness campaigns. Part of the problem is that any more campaigning could hurt the reputation of the banks. Banks do not want to risk their name being linked to increased risk. That is why the NVB and the government need to execute most of the campaign. Lastly, Dutch banks are effectively insuring their clients for OWBF risk. This will not add to the level of awareness of those clients.

6.6 Satisfaction of achieved level of risk

As I'm not part of a bank, I cannot determine their satisfaction.

6.7 Suggestions for external security controls

Just as the other experts, Mr. Mulder mentions the existence of the SC and SFE trade-offs that have to be respected.

Suggestions are:

- **Technological**
    - **VPN and EDI:** I would agree with (MS) on this alternative, hence the controls should remain in place and no improvement is to be expected from altering them.
    - **Out of band authentication:** out of band authentication is an effective way of increasing security risk. Basically, out of band authentication involves the usage of a token that is physically separated from the primary communication channel. One example is the online banking application of ING: it requires you to provide a one-time code that is transmitted to the client's mobile phone using a text message. Out of band authentication requires any attacker to tap into a second, different communication line, adding to the difficulty of successfully breaking in. Note that out of band authentication is a form of multi-factor authentication. Using additional authentication factors without using out of band will probably not significantly increase control.
    - **Signing of token keys:** this method is employed by the Rabobank. It involves the total amount of money to play a role in the final token code that is generated, preventing any attacker from piggy-bagging any additional transactions to the list using MITM methods. The usage of this security control should be intensified.

- **Dedicated machines:** the usage of dedicated machines is interesting as a though experiment or within the academic domain, but it would not fit the security, costs trade-off.
- **Risk-based analysis of transactions:** this is a method that is used in the US which has the potential to increase security while not running into one of the trade-offs. It involves moving away from straight-through-processing that is in use in The Netherlands by adding a delay in the processing of transactions. Within this delay, a computer can check the transaction for any suspicious qualities: attributes such as amount, target account, time, et cetera. Any suspicious transaction is flagged and sent back to the client for additional checking. It is true this method would add a delay to any transaction, but it may very well worth it.
- **Anti-virus software:** this method would not work very well. These scanners, while helpful, are outdated by definition and can also be targeted by malicious software to create a false sense of security.
- **Facial recognition:** this is an interesting idea which could work with respect to the aforementioned trade-offs. However, privacy issues will be a problem. While our banks play a very important role in the life of every Dutchman, they get not nearly the same level of trust that is given to the government.
- **Reversing the trust relationship:** the banks have a tendency of requiring the client to identify him to the bank. A more client-friendly approach would be to prove to the client that the bank is who it claims to be. This may be difficult to implement using today's technologies, although there are some options available, like signed SSL certificates.

- **Social**
  - **Awareness:** more awareness campaigns would only add to the distrust that people feel about online banking. It may even lead to competitive disadvantages if one bank is perceived to be less secure than its peers. The current measures should be maintained.
  - **Transparency:** creating a better awareness may be a matter of increasing the transparency around online banking and OWBF, specifically. However, given the relative closed nature of Dutch banking, this may be infeasible.
  - **Password control:** time and again, research shows that the majority of users have the tendency to use ineffective passwords. They are usually easy to guess and identical for a big number of different Web sites. Requiring a minimum length,

numbers, et cetera is only part of the solution; people need to be aware of the risk that they take when using insecure passwords. This is, of course, only applicable in cases where passwords are used as security control, like the accounts at ING.

6.8 Summary

As a Director Systems & Process Assurance at another one of the big four accounting firms, Mr. Mulder is directly involved in the security and audits of financial systems. There is already a lot of cooperation in place, and one must not underestimate the difficulties of cross-border and cross-cultural cooperation. Both the technological and the social external OWBF controls are working well with respect to the security-cost and security-ease of use-functionality trade-offs. Technological controls that could improve control are out of band authentication, the signing of token keys, risk-based analysis of transactions, facial recognition and reversing the trust relationship. Social controls that could improve control include transparency and password control.

7 Verification interview D: Rabobank (PS)

Name: *Mr. P.H. (Paul) Samwel RE*

Position: *Manager Information Risk Management (IRM) at Rabobank*

Date: *September 15, 2011*

Location: *Utrecht*

7.1 Introduction

The Rabobank is one of the three major Dutch retail banks, along with ABN AMRO and ING. It is the only major retail bank in The Netherlands that is not publicly traded. Instead, it is a cooperative bank, owned in essence by its customers. The Rabobank has got millions of private and organizational retail accounts and was the first Dutch bank to offer online banking.

7.2 Importance of OWBF

OWBF is of great importance to a manager of IRM. The Rabobank has had online banking for ten years. But in the last one to three years the number of OWBF attacks has increased significantly which has made the Rabobank shift its priorities from preventive controls towards preventive and detective controls. Securing our OB services requires significant resources from our organization.

7.3 (International) cooperation

Currently, cooperation between OB organizations in both The Netherlands and Europe is well-established, effective and mature. In The Netherlands, the Financial Institutions-Information Sharing and Analysis Center (*(FI-) ISAC*) facilitates a collaborative platform with representatives of all relevant banking organizations. In Europe, this cooperation also exists. Furthermore, there is also cooperation with North-America, although it meets less frequently and the cooperation is less formalized. OWBF security controls have never been used for competitive advantage. FI-ISAC shares information about OWBF prevention and detection controls, new forms of attacks and other security issues.

Mr. Samwel also supports the statistics publicized by the NVB.

Since the cooperation is and has been effective in sharing security threats and controls for years, there is not much room for improvement in this area.

7.4 Effectiveness of external controls

All successful attacks involve both technological and social elements. Technological controls are never 100% effective, while social controls are limited by the user's willingness and knowledge.

Also, I would like to see more preventive controls that are executed with the help of the customer, or at least use more input from them. This is called awareness training 'on the job'. Still, the bank can help with training, but ultimately a bank's control over external processes is limited.

7.5 Satisfaction of achieved level of risk

Rabobank is aiming for a better security than just risk appetite. For commercial reasons, it is important for our clients to feel safe online and trust online financial transactions. The Rabobank is certainly aware of its risk appetite and its performance in this area.

7.6 Suggestions for external security controls

Suggestions are:

- **Technological**
    - **Custom applications:** using custom applications creates another problem, monoculture. Monoculture may improve the perpetrator's business case because any weakness in an application is more valuable if more customers are using that application. In monoculture all customers are using one application, as opposed to the current situation where people use multiple operating systems, devices, Web browsers, et cetera.

      Also, the Rabobank should focus on providing financial services. Creating and maintaining software applications for multiple platforms could require a lot of resources.

      However, on some devices it is very common and logical to use applications instead of the browser, for instance on tablets or smartphones. In those cases, the Rabobank finds it very possible to develop and secure those applications. But the move to custom application should not be made because of security.
    - **VPN and EDI:** it is very much possible to create a VPN connection that is impenetrable to MITM channel breaking attacks. However, this requires the exchange of private keys between the Rabobank and the customers, which would affect the security-ease of use-functionality trade-off. Furthermore, securing VPN connections is not going to solve the OWBF problem because it is not one of the weak points in the system.
    - **Two-factor, multi-factor authentication:** two or more factor authentication is already in place in the Rabobank. Excluding out of band authentication, there is no real security potential in using more factors.

- **Out of band authentication:** using out of band does not cause any serious harm to the security, functionality, ease of use and the security, costs trade-offs. ING already employs out of band authentication by using an SMS code for authenticating transactions, and Rabobank is doing this on a select group of customers and we're looking to increase our use of it.
- **Signing of token keys:** signing token keys with transaction information is another good practice that still has the potential to increase OWBF control. At the Rabobank we use it for large amounts only, but we're planning to use it for all transactions.

  Together, out of band authentication and the signing of token keys are also known as "What You See Is What You Sign", and it is one of the known potential improvements.
- **Dedicated machines:** I agree with the other experts that this is a hypothetical solution which does not respect the trade-offs.
- **Risk-based analysis of transactions:** this control is not new to the Rabobank. We've been analyzing transactions in real-time for years and this is an important security control. This process does not take multiple days, as I do believe the US and Canadian versions also do not. This practice should be continued, but there is not much potential left in this control.
- **Anti-virus software:** this control suffers from the issues that were addressed by the other experts. Moreover, it also creates a monoculture which increases the risks even more. Also, it could lead to practical issues like requiring multiple installations of AV software on one device, which is not desirable.
- **Facial recognition:** using biometric data for OWBF control is not a new idea, my organization has been thinking about this for some time. However, I do not expect it to decrease our risk, since malware could collect webcam images anytime and use it for doing malicious transactions. One biometric that may have potential is a voice recognition control that requires the customer to express a dynamic token, such as the transaction amounts. This is an example of the aforementioned focus on letting users supply more input. Ultimately, however, this is not a very good idea.
- **Reverse the trust relationship:** this is certainly an interesting idea and it's something that the Rabobank would definitely be interested in. It would require

an out of band authentication token that is sent to the customer, proving the identity of the bank. However, there are no known implementations at this time.

- **Reducing the attractiveness of the OWBF business case:** one suggestion that could help decrease OWBF risk is using temporal limits that lower the attractiveness of the business case for any perpetrator. An interesting thing that can be seen in micro transactions is that there is no fraud because the low amounts are not interesting to the criminal. One example of such a temporal limit is the recent lowering of the weekly ATM limit for underage clients at ING to 250 euros. Since any money mule would end up on a blacklist after one transgression, the costs of recruiting and paying a money mule will outweigh the potential profit. This practice is also used in mobile banking, where customers can only send up to 1000 euros (at the Rabobank) and only to known accounts. We're looking for ways to increase or tighten the existing temporal limits even further. This control could potentially decrease OWBF risk significantly. Practical problems and customer satisfaction are handled by allowing custom limits for any customer that wishes them.

- **Social**
  - **Awareness campaigning:** for commercial reasons, the Rabobank has decided to communicate the majority of the awareness campaign through the NVB. We should keep doing campaigns this way, although there is not much potential for decreasing risk in this area. We should focus on training 'on the job' to create more awareness.
  - **Awareness training 'on the job':** training on the job would involve redesigning online banking systems in such a way that customers are more aware of the security risks and how to recognize them. Expecting the user to manually check the identity of an SSL certificate, for instance, is not practical. We have to find more clever ways of making the user more aware of the risks of online banking, in tandem with our goal of requiring more input from the user.
  - **Communication by banks:** awareness campaigns should not be communicated by the Rabobank because of commercial reasons.
  - **Transparency:** the Rabobank already is sufficiently transparent, both to the FI-ISAC and to the public. Transparency is also required for commercial reasons, since it builds trust. We should continue to be transparent.

- **Password control: m**ost banks, including the Rabobank, do not require passwords because they only rely on the user's knowledge while we want them to have a possession token too. It is, however, a good practice for any password-driven security implementation.

7.7 Summary

The Rabobank is one of the major retail banks in The Netherlands. OWBF risk has been quite stable until a few years ago. The cooperation between stakeholders in The Netherlands as well as internationally is very good. One very effective cooperation platform is (FI-) ISAC. The Rabobank has always stated that security issues, including new attacks and new security controls, are to be shared openly between banks, and the awareness campaigns should be communicated primarily by the NVB. As for the current state of OWBF control, the technical controls for OWBF suffer from imperfection as do all technical controls. Furthermore, the social controls have a built-in weakness that we cannot completely control: the customer. The Rabobank is beyond the point of risk appetite, for commercial reasons. VPN connections, risk-based analysis of transactions, two-factor authentication, awareness campaigns, transparency and password control should be maintained as is, and cannot provide any significant additional external control. Out of band authentication, signing of token keys, reversion the trust relationship, reducing attractiveness of the business case and awareness training 'on the job' still have the potential to increase external control.

8 Discussion

8.1 Introduction

In this chapter, the results of the separate interviews will be interpreted and cross-referenced with their peers. First, the relevance of the experts is presented. Secondly, the cooperation of the different anti-OWBF organizations in The Netherlands is given. Then, the international cooperation and situation is discussed. Next, the OWBF tools and methods that were discussed in the literature review are compared to the knowledge of the experts. Then, the trade-offs that were mentioned by the experts are given. After that, both the suggested technological and social suggestions are presented. Then, a suggestion matrix with all relevant suggestions is presented. Finally, the banks' satisfaction with the achieved level of security is briefly discussed.

8.2 Relevance of experts

All four experts work in the field of IT security related to the financial sector. Furthermore, all four have stated to have knowledge of the Dutch retail banking sector and its systems. One expert works for a major retail bank, two experts work for Dutch retail banks indirectly and one has worked with the Dutch Ministry of Finance on retail banking policy. Moreover, all experts have shown to have in-depth knowledge of the security issues related to OWBF. All three advisory organizations that were visited have shown to have the necessary expertise and experience to give advice and consulting services to large financial organizations.

8.3 Importance of OWBF

- **To the experts:** all experts expressed concerns related to OWBF, and most of them are directly involved in the fight against it.
- **To the banks:** the banks are very concerned with the risk of OWBF, but their closed nature can make it difficult for the outside world to notice. All experts agree that the banks are committing much of their resources in the fight against OWBF.
- **To the expert's organizations:** with the exception of one organization (HEC), all questioned organizations are directly involved in fighting OWBF.

8.4 Cooperation in the Netherlands

The experts have mentioned a few more Dutch OWBF organizations than the literature study identified, such as the PVIB or "*Samen tegen cybercrime*". Most experts agree that current efforts to combat OWBF in The Netherlands are quite effective, but could be better if the different organizations were better organized. Their current efforts are hindered by the organizations having their own agendas, goals, information and motivation towards fighting

OWBF. One expert, however, states that the current cooperation is in place, is mature and working well, both nationally and internationally.

8.5 International situation

OWBF crimes often involve multiple countries, and so must the effort of fighting those crimes. The consensus of the experts is that currently there is a lot of international cooperation in place, and that it is having an effect. Most of them also agree that there still is a potential for even more effective cooperation if the organizations were better organized. A number of issues that have been raised by the literature were confirmed by the experts:

- Firstly, the crime statistics are not always comparable between countries. This is partly due to definition issues, but is also a matter of granularity and completeness of the crime data. Attempts to unify the definition of cybercrime and its statistics have yet to reach their goals. However, the one expert working for a major retail bank notes that the Dutch NVB statistics are valid and reliable.
- Secondly, cultural differences seem to play a role. Some of the experts mention the difficulties in cross-cultural and cross-border cooperation.

8.6 OWBF methods and tools

In Figure 3, an overview of the various methods and tools used to commit OWB fraud is given. Although most of the methods have (multiple) synonyms, in general the methods, tools and the relationships between them are supported by all experts and no changes to this model are required. Hence, the model given in Figure 3 (p. 19) was accepted.

8.7 Trade-offs

8.7.1 Security, functionality, ease-of-use (SFE)

One trade-off that was mentioned by all four experts is the trade-off between security, functionality and ease of use. This trade-off sates that an increase in any of the three qualities will result in a decrease of at least one the other two. Perhaps the most important and cited effect of this trade-off is that any increase in security will result in decreased functionality or ease of use of the system.

However, this trade-off was not found in any academic research. The phenomenon is mentioned extensively in non-academic sources and is validated by the interviews, making it an industry best-practice. Figure 5 visualizes this trade-off.

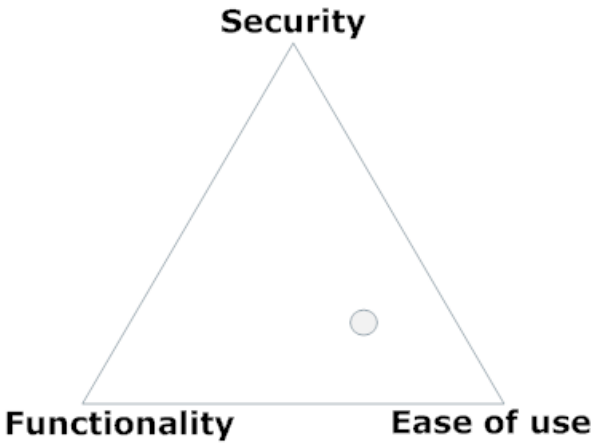


Figure 5: Security, ease-of-use, functionality trade-off

8.7.2 Cost, security (CS)

The trade-off between security and costs to design, implement and maintain the system that supports that security has been well-known for some time (Sonnenreich, Albanese, & Stout, 2005; Cavusoglu, Mishra, & Raghunathan, 2004), and was also confirmed by all experts.

Figure 6: Cost-Security trade-off

8.8 Effectiveness of external controls

All experts supported the hypothesis that the banks are at least at the point of their risk appetite, meaning that any additional level of security would come at too great a cost compared to the fraud it will likely prevent. The expert at the Rabobank expressed his bank's desire to go beyond risk appetite for commercial reasons. Moreover the SFE trade-off is also mentioned as a reason that banks are hesitant to increase their security.

8.8.1 Effectiveness of technological external security controls

Most of the experts also agree that technological security controls are imperfect by design, but still preferable to social controls. Instead, the social external security controls are cited to come only after the technological ones are found to be insufficient to diminish the threat. This is caused by a weakness in social controls that is caused by relying on humans rather than IT systems to execute the security controls, which practice has found to be more predictable.

8.8.2 Effectiveness of social external security controls

Some experts mention the difficulties in implementing social external security controls, since they require knowledge and action from the customers of the bank. This is inherently more difficult and less reliable than technological controls, which are found to be more predictable.

While two of the experts mention the awareness campaigns as the most important social control, they also state that increasing campaign intensity will likely hurt the banks commercially. Moreover, one expert confirms that the banks have jointly decided to execute the majority of their awareness campaigns through the NVB for commercial reasons, confirming the previous statements.

8.9 Suggested technological external security control improvements

In this section, all suggested technological external control improvements are discussed by cross-reference and peer verification. For the sake of completeness, this list includes all suggestions that were discussed, even if the improvement is theoretical, hypothetical or dismissed by the expert himself.

1. **Using custom applications instead of browsers**

   Most communication and security standards used online are open, meaning that their specification is publicly available to anyone. This poses a clear disadvantage over closed standards, since their inner workings are known only to a select number of people. This type of security is also known as security by obscurity and one major Dutch retail bank offers this possibility for a part of their customers (see Table 2). However, based on the expert opinions, this is not an effective way of fighting OWBF. A number of new risks come into play, such as patching of the banking application using malicious software. Also, it creates a monoculture where all customers can be compromised by focusing on a single application, instead of a landscape of applications, protocols and platforms. Custom applications are possible if a bank wishes them for commercial reaons, but they do not increase security.

2. **Using VPN and EDI**

   All experts commented on the fact that all currently known online banking implementations already have some kind of VPN in place, usually with an SSL certificate. As there are many types of VPN connections, there may be a potentially more secure type available. However, none of the experts expect there to be any significant improvement to other VPN types with respect to the aforementioned trade-offs. This is due to the MITM channel breaking attack type, which cannot be

circumvented by any known VPN without using private keys on both ends, a practice which is found to be violating the SC trade-off, confirming (Goeijenbier, 2010; Raval & Fichadia, 2007). VPN controls should be maintained, however, as a vital part of OB security.

Note that EDI is an outdated form of VPN and thus leads to the same conclusion.

3. **Using Two-factor or multi-factor authentication**

   As was shown in Table 4, currently Dutch banks implement a two-factor authentication. In theory, adding more factors to the authentication process can enhance security by increasing the information that a perpetrator must possess in order to commit fraud. However, none of the experts are convinced that this option will significantly improve security with respect to the trade-offs and thus this is not a potential improvement. So, two-factor authentication should be maintained.

   This excludes the usage of out of band authentication, which is discussed below.

4. **Using out of band authentication**

   Out of band authentication is a form of multi-factor authentication that requires the usage of a separate (secondary) communication method to send over authentication data. The idea being, that anyone who has access to the primary communication channel (in the case of OWBF, the Internet connection) cannot gain access without also gaining access to the secondary channel. An example of this is the text message that is sent to customers of ING that authenticates their transactions just prior to confirming them. Some of the experts (TM, PS) think this is a good way of increasing OWBF security and thus this may be a potential improvement. Not all Dutch banks have committed to out of band authentication (ABN AMRO, 2011; ING Bank, 2011; Rabobank, 2011; SNS Bank, 2011; Friesland Bank, 2011), creating a potential for improvement.

5. **Signing of token keys**

   Another potential improvement to OWBF external control is the signing of token keys. This method involves using the total amount of all transactions about to be confirmed by the customer as an input in the authentication. This is supposed to prevent an attack in which the perpetrator intervenes in the transaction and piggybacks additional transactions to the legitimate ones. This method is currently employed by the Rabobank. At least two of the experts (TM, PS) think this is a good way of increasing

OWBF security and thus this may be a potential improvement. The signing of token keys has not been implemented at all banks (ABN AMRO, 2011; ING Bank, 2011; Rabobank, 2011; SNS Bank, 2011; Friesland Bank, 2011), creating a potential for improvement.

6. **Using dedicated machines**

   A dedicated machine for OWBF transactions involves the design, production and deployment of an electronic device (for instance, a smartphone or laptop-like one) that handles the complete online banking application. It includes the complete OWBF transaction, including authentication, graphical interface and communications. Also, the device is physically locked by using a kind of resin that destroys the hardware if forced open.

   The advantage of such a device is clear: one can protect the online banking process from malicious software and MITM channel breaking by using closed off software and protocols. However, this suggestion was made by one expert as a theoretical and hypothetical method of perfect security against MITM attacks, malware and phishing and thus is not a practical suggestion.

7. **Performing risk-based analysis of transactions**

   This method involves delaying all transactions for an (semi-)automated risk-based analysis. This analysis looks at factors such as destination, time, amount, et cetera in order to assess whether the transaction is suspicious. If it is, the transaction is bounced back to the customer for a recheck. At least one of the experts (TM) thinks this is a good way of increasing OWBF security. However, this control is already in place at all Dutch retail banks and cannot be significantly improved upon, according to (PS). Hence, it should be maintained.

8. **Deploying anti-virus (AV) software**

   AV software is a technological control against malicious software and some kinds of MITM attacks. As discussed, malicious software is one of the attack methods employed to conduct OWB fraud and thus the usage of AV software should provide at least some level of protection against it. A bank could encourage the use of AV software through awareness campaigning and even subsidizing the purchase and requiring the usage of it. However, the experts are not in agreement. While one expert thinks it could add to the level of protection since some part of the customers will never act responsibly even with the awareness campaigns, one states that it could

hurt the bank's reputation even more. Also, it suffers from the creation of a monoculture. Hence, this is not a suggestion that could potentially increase control.

9. **Using facial recognition**

   Using facial recognition technology when doing online banking would manifest itself as requiring the user to have a webcam and activate it during online banking. A computer could check the identity of the user with the biometric data on file. Note that using static photos is not enough to fake this kind of authentication. According to two (out of four) experts, this could add to the external control on OWBF risk. However, (PS) states that malicious software could be used to capture webcam images for later use. Therefore, this control is rejected. Also, consumer privacy could prove to be an issue.

10. **Reversing the trust relationship**

    Another suggestion is a reversal of the customer-bank trust relationship. In essence, this would require the bank to identify itself to the customer instead of the other way around. This would have an advantage in combatting phishing attacks, as the customer would likely not enter his credentials on a faked Web site if he was absolutely assured that the site actually belongs to his bank. The value of this hypothetical control should not be underestimated, as phishing is perhaps the most popular one of the OWBF attack methods.

    The reversal of the trust relationship may be difficult to implement using current technology, since there is no known complete implementation. One example of a current method to prove the bank's identity to the user is the signed SSL certificate that banks use. However, as not all users are aware of this possibility, this issue could be solved using the awareness training 'on the job' discussed ahead.

    As reversing the trust relationship relies heavily on the use of technology, another critical major factor is trust, which is only perceived by humans. Therefore, reversing the trust relationship has no clear distinct technological or social nature, and should be placed around the center of the spectrum.

11. **Reducing the attractiveness of the OWBF business case**

    As criminals are after financial gain, the trade-off between effort and revenue is important to them. One way of decreasing OWBF occurrences is to make online banking customers a less attractive target by decreasing the potential revenue that can be acquired while keeping the effort at the same level. One interesting thing that

can be seen in micro transactions is that there is no fraud. One expert claims that using temporal limits on transaction amounts could very well decrease the attractiveness of OWBF. Since this suggestion cannot be verified by any expert, it is rejected.

8.10 Suggested social external control improvements

In this section, all suggested social external control improvements are discussed. For the sake of completeness, this list includes all suggestions that were discussed.

1. **Executing awareness campaigns:**

   Awareness campaigns are perhaps the most effective social external control as all experts agree that they are essential and effective as a method of educating and alerting banking customers to their online activities. As discussed, a significant part of the methods and tools used to commit OWBF are of a social nature, meaning they require the user to be deceived in order for the fraud to be committed. As discussed, awareness campaigns can be found in The Netherlands and all its peer countries.

   While all experts agree that the campaigns are effective, not all of them agree that intensifying them will increase control. One of the experts explicitly states that telling the customer more about OWBF could lead to distrust between the customer and the bank. This is not a step that any bank would want to take for commercial reasons, which was confirmed by (PS). Hence, the consensus between the experts is that current measures should be maintained but not increased.

2. **Shift communication to retail banks:**

   One of the experts (MS) proposes a change in the execution of the awareness campaigns. Most of the campaigning in The Netherlands is handled by the government and the NVB and not by the retail banks themselves. However, the level of trust and recognition between the customer and his bank is arguably much greater. If the campaigning were handled primarily by the retail banks, the campaign may be more effective. The banks, however, may not be willing to do this for commercial reasons according to (PS).

3. **Increase transparency:**

   One of the experts mentioned that more transparency could lead to lower OWBF activity. The idea being that if the banks would share more information with each other, the customers and other stakeholders; this may increase awareness at

customers and the readiness of other banks. However, another expert (PS) does not agree. Hence, the suggestion of increasing transparency has little support, while both support keeping current measures in place.

4. **Using password control:**

   Password strength controls such as minimum length, requiring integers, et cetera were also mentioned. Using password controls has a definite advantage as research has shown that the average user may not opt for a strong password if he's allowed to do so (Florencio & Herley, 2007). However, this suggestion is probably already widely implemented were applicable (note that the Rabobank and ABN AMRO do not use passwords). Hence, it should be maintained.

5. **Awareness training 'on the job':**

   Awareness training on the job involves redesigning online banking systems in such a way that customers are more aware of the security risks and how to recognize them. One example of awareness training on the job is the signing of tokens with transaction amounts, as it requires the user to see and check the amount once more. This suggestion is cited to increase the level of control over OWBF risk, if it is deployed along with the existing awareness media campaigns. Since this suggestion cannot be verified by any expert, it is rejected.

All suggestions and their proponents and opponents are listed in Table 9.

8.11 Suggestions matrix

#	Suggestion	MS	SS	TM	PS	Result2	Conclusion	Comments
Technological								
T01	Custom applications		–	–	–	Rejected	Do not implement	
T02	VPN and EDI	✓	✓	✓	✓	Rejected	Keep	Already implemented
T03	Two-factor, multi-factor authentication	✓	✓	✓	✓	Rejected	Keep	Already implemented
T04	Out of band authentication			✓✓	✓✓	Accepted	Implement	A.k.a. What You See Is What You Sign; already partially implemented
T05	Signing of token keys			✓✓	✓✓	Accepted	Implement	
T06	Dedicated machines	–	–	–	–	Rejected	Do not implement	No known implementations
T07	Risk-based analysis of transactions			✓✓	✓	Rejected	Keep	Already implemented
T08	Anti-virus software	✓✓		–	–	Rejected	Do not implement	
T09	Facial recognition		✓✓	✓✓	–	Rejected	Do not implement	
T10	Reverse the trust relationship			✓✓	✓✓	Accepted	Implement	Implementation needs further research
T11	Reducing attractiveness of business case				✓✓	Rejected	Potential improvement	Future research
Social								
S01	Awareness campaigns	✓✓	✓	✓	✓	Rejected	Keep	
S02	Communication by banks instead of NVB	✓✓		–	–	Rejected	Do not implement	
S03	Transparency			✓✓	✓	Rejected	Keep	
S04	Password control			✓✓	✓	Rejected	Keep	
S05	Awareness training ‘on the job’				✓✓	Rejected	Potential improvement	Future research

Table 9: Suggestions matrix. A double “V” indicates a potential for reducing risk, a single “V” indicates an effective control without a potential for reducing risk. Missing values are either because there was no answer, or the question was not asked because the suggestion was made by another expert after the interview.

[2] The hypothesis to be rejected or accepted is “does (suggested security control) significantly increase OWBF control compared to current control?”

8.12 Satisfaction of achieved level of control

Only one of the experts could provide an estimate of the Dutch retail bank's satisfaction with the achieved level of control. The Rabobank has moved beyond risk appetite for commercial reasons, hence the levels as described in COSO have been met. However, this statement was not verified hence it must be rejected.

None of the experts who did not work at a bank could answer this question with much certainty. As two of the experts are among the primary advisors for the banks, their work involves prioritizing and measuring of information system risk. In their position, they could perhaps benefit from having access this information. Furthermore, it was suggested that the banks may not have a clear picture of their risk appetite and current control. This, however, was strongly dismissed by a retail bank (PS). So, there is no support for the hypothesis that banks are not aware of their risk appetite and performance. There exists, however, a lack of this information at the hands of the advisory organizations.

9 Conclusions

9.1 Introduction

In this chapter, the final conclusions of the thesis are presented. First, the answers to the sub research questions and finally the main research question are given. Then, the research limitations and finally the suggestions for future research are presented.

9.2 Thesis findings

9.2.1 Sub questions

I. How effective are the technological external security controls for OWBF?

The experts agree that the Dutch banks at least close their risk appetite. Technological controls are considered to play a major role in reducing OWBF risk. The majority of the security controls are technological. For any threat, the technological controls are explored first, to be supplemented by social ones when the technological are insufficient. Additionally, the experts state the absolute necessity of technological controls. However, the experts also agree that no technological control has been perfect in the past, and they should not be expected to be perfect in the future.

If the total level of control is at or beyond the risk appetite, and the technological controls are considered more effective than the social ones, the technological controls must perform at least sufficiently, perhaps better. Thus, there is support for the conclusion that technological external security controls for OWBF are performing sufficiently, but not perfect.

II. How effective are the social external security controls for OWBF?

The social external security controls are cited to be a vital part of OWBF control, but come only after the technological ones are found to be insufficient. This is caused by a weakness in social controls that is caused by relying on humans rather than IT systems to execute the security controls.

Furthermore the most important social control, awareness campaigns, will not be intensified because of commercial reasons. Also, the number of social controls is much smaller than that of technological controls, increasing the importance of the few controls that are used. These two phenomena suggest a difficulty in increasing awareness campaigns for commercial reasons, while there are not many alternatives available.

III. **How can the effectiveness of the technological external security controls for OWBF be improved?**

As presented in Table 9, a number of proposed technological external security controls are supported by one or more experts and verified in interview D:

1. Out of band authentication
2. Signing of token keys
3. Reversing the trust relationship

IV. **How can the effectiveness of the social external security controls for OWBF be improved?**

As presented in Table 9, none of the suggested external social security controls that increase OWBF control have been accepted.

9.2.2 Main question

How can the Dutch banking organizations improve the effectiveness of both social and technological external OWBF security controls?

First of all, the current external security controls for online web-based banking fraud (OWBF) are quite effective in lowering OWBF risk towards the risk appetite of the Dutch retail banks. Technological controls are not 100% effective, and social controls suffer from the reliance on human beings. But while both types of security controls have their issues, there may be little room for improvement with respect to the security, ease-of-use, functionality (SFE) and security, costs (SC) trade-offs.

Before listing the security controls that have the potential of increasing OWBF control, it is important to mention the controls that need to be kept and maintained just to keep the status quo. These controls do not have the potential to significantly increase control. Hence, they already are at their full potential. These controls are: VPN, Two-factor or multi-factor authentication (excluding out of band authentication), risk-based analysis of transactions, awareness campaigns, transparency and password control.

The technological external security controls that have the potential to significantly decrease OWBF risk, while honoring the SFE and SC trade-offs, are: **out of band authentication**, **signing of token keys** (these two are also referred to as “What You See Is What You Sign” or WYSIWYS) and **reversing the trust relationship**. No social external security controls that meet the requirements were identified.

Additionally, there are two proposed controls (one technological, one social) that could not be verified within this research, they will be addressed in paragraph 9.4.

The Internet and online banking are the new way of doing financial transactions, and it suffers from its own weaknesses. It is important for any bank to secure their online banking applications in the interest of preventing crime, saving image and to increase the use of online banking even further. In the fight against OWBF, it is important to exploit all the security controls that are at your disposal. This research has identified a number of such proven security controls that have yet not been implemented in all Dutch retail banking applications.

9.3 Research limitations

As can be seen from Table 9, part of the suggestions that were made could not be verified by the other experts. This is due to the fact that interviews were only taken once and getting these answers would require a multi-round interview method, such as the Delphi method. However, the agendas of both this research project as well as the experts did not allow a multi-round interview method.

As this research is a qualitative exploration of the opinions and experiences of a few experts, the results are not generalizable to the compete population of OWBF experts. They can, however, provide an insight into the views of experts in the field from different angles.

9.4 Suggestions for future research

The various options for improvement that this research has stated have not always been fully conceptualized. Some of the suggestions need more thought and feasibility research before any definitive recommendation can be given.

As discussed, the single-round method that was used has limited the commentary of the experts on each other's suggestions as the experts were only presented with the suggestions of the others before them. A multi-round or panel type of discussion would increase the certainty of the results to the level of consensus among the experts.

Furthermore, as said none of the opinions expressed by the experts can be generalized to the complete population. However, a quantitative study could very well accomplish that. When designing a quantitative study, it helps to use closed-ended structured interviews such as is the case in surveys or questionnaires. The suggestions given in this research could add to the knowledge that is needed to design such a study.

Some of the suggestions expressed by the experts have not been verified by any peer, as is the achieved level of control versus risk appetite. This is also the result of the single-round

method. Still, the risk appetite and security controls suggestions may very well have merit, however they will have to be confirmed in future research. The rejected suggestions are “Reducing the attractiveness of the OWBF business case” and “Awareness training ‘on the job’”.

Some elements of the literature study discussed in Chapter2 have not been discussed with the experts. An attempt was made to list the specific security controls that are used in online banking. The comprehensive web of cooperating OWBF organizations around the world was also of interest. Also, the effectiveness of the internal security controls at retail banks has little scientific support.

Finally, the international situation on OWB crimes has found there to be significant differences in the definitions of OWBF and the statistical methods used to record its occurrences. Any measure of the effectiveness of a control would benefit from having international comparability in OWBF statistics. So, how would one compare the effectiveness of OWBF controls in a country relative to comparable countries? Research that focuses on the various legal definitions of OWBF and the various ways of recording and analyzing criminal statistics could help answer this question.

Bibliography

ABA, AHTCC & ASIC. (2011). *Protect Your Financial Identity*. Retrieved April 13, 2011, from Protect Your Financial Identity: http://www.protectfinancialid.org.au/

ABN AMRO. (2011). *ABN AMRO*. Retrieved May 23, 2011, from ABN AMRO: http://www.abnamro.nl/en/index.html

Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. (2006). A Multifaceted Approach to Understanding the Botnet. *IMC '06 Proceedings of the 6th ACM SIGCOMM conference on Internet measurement* (pp. 41-52). ACM New York, NY, USA.

ACCC. (2010). *Report of the ACCC on scam activity 2010.* Canberra, Australia: Australian Competition and Consumer Commission.

Australian Federal Police. (2011). *Internet fraud and scams*. Retrieved April 12, 2011, from Australian Federal Police: http://www.afp.gov.au/policing/e-crime/internet-fraud-and-scams.aspx

Australian Institute of Criminology. (2010). *Australian crime: facts and figures 2009.* Australian Institute of Criminology.

Australian Institute of Criminology. (2011, July 18). *Australian Institute of Criminology - Definitions and general information*. Retrieved May 23, 2011, from Australian Institute of Criminology: http://www.aic.gov.au/crime_types/cybercrime/definitions.aspx

Babbie, E. (2007). *The practice of Social Research.*

Birch, D. G. (2004). *Digital identity management: perspectives on the technological, business and social implications.* Hampshire: Gower Publishing Limited.

Blumberg, B., Cooper, D., & Schindler, P. (2005). *Business Research Methods.* New York, USA: McGraw-Hill Education.

BRA - National Council for Crime Prevention. (2011, 03 31). *Total number of reported offences*. Retrieved April 4, 2011, from BRA - National Council for Crime Prevention: http://www.bra.se/extra/pod/?action=pod_show&id=14&module_instance=11

Bundeskriminalamt. (2009). *IUK-KRIMINALITÄT.* Wiesbaden.

Canadian Centre for Justice Statistics. (2011). *Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics.*

Carter, D. (1995). Computer crime categories: how techno-criminals operate. *FBI Law Enforcement Bulletin, 64*(7), 7.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *COMMUNICATIONS OF THE ACM, 47*(7), 87-92.

CBS. (2010, July 07). *Gereg.criminaliteit; misdrijven naar soort misdrijf en politieregio*. Retrieved March 3, 2010, from CBS Statline: http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=80344NED&D1=0&D2=0-1,62,87,104-105,114,117,121-122&D3=0-1,19&D4=a&HDR=T,G3&STB=G1,G2&VW=T

Chaum, D., Fiat, A., & Naor, M. (n.d.). Untraceable Electronic Cash. *CRYPTO '88 Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology* (p. 1990). London, UK: Springer-Verlag.

Chua, W. F. (1986, October). Radical Developments in Accounting Thought. *The Accounting Review*, pp. 601-632.

Claessens, J., Dem, V., Cock, D. d., Preneel, B., & Vandewalle, J. (2002). On the Security of Today's Online Electronic Banking Systems. *Computers & Security*, 257-269.

comScore. (2010, 10 27). *The Netherlands Leads Europe in Online Visit Frequency.* Retrieved 02 23, 2011, from comScore: http://www.comscore.com/Press_Events/Press_Releases/2010/10/The_Netherlands_Leads_Europe_in_Online_Visit_Frequency/(language)/eng-US

comScore. (2010, 12 07). *Top 10 Countries by Online Banking Penetration*. Retrieved 02 23, 2011, from comScore Data Mine: http://www.comscoredatamine.com/2010/10/top-10-countries-by-online-banking-penetration/

COSO. (2004, September). *Enterprise Risk Management — Integrated Framework.* Retrieved March 11, 2011, from COSO: http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

Council of Europe. (2001, November 23). *Convention on Cybercrime.* Retrieved April 1, 2011, from Council of Europe: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Council of Europe. (2010, August 12). *Convention on Cybercrime.* Retrieved April 4, 2011, from Foreign & Commonwealth Office: http://www.fco.gov.uk/en/publications-and-documents/treaty-command-papers-ems/explanatory-memoranda/explanatory-memoranda-2010/050Cybercrime

Council of Europe. (2011, April 4). *Convention on Cybercrime Ratification.* Retrieved April 4, 2011, from Council of Europe: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

CyberSource. (2011). *2011 Online Fraud Report.* CyberSource.

Damiani, E., De Capitani di Vimercati, S., Paraboschi, S., & Samarati, S. (2004). An Open Digest-based Technique for Spam Detection. *Proceedings of the 2004 International Workshop on Security in Parallel and Distributed Systems*, (p. 6).

Davis, R., & Hutchison. (1997). *Computer Crime in Canada.* Toronto: Thomson Canada Limited.

Emigh, A. (2006). The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond. *Journal of Digital Forensic Practice*.

Ernst & Young. (2010). *Borderless security.* IT Risk and Assurance Services. Ernst & Young.

Ernst & Young. (2010, October 6). *Ernst & Young reports fiscal year 2010 global revenues of US$21.3 billion.* Retrieved August 15, 2011, from Ernst & Young: http://www.ey.com/GL/en/Newsroom/News-releases/Ernst-and-Young-reports-fiscal-year-2010-global-revenues-of-USD-21-3-billion

Europe's Information Society. (2009). *Safer Internet Centres*. Retrieved April 4, 2011, from Europe's Information Society: http://ec.europa.eu/information_society/activities/sip/projects/centres/index_en.htm

Federal Office for Information Security. (2009). *The IT Security Situation in Germany in 2009.* Federal Office for Information Security.

Federal Trade Commission. (2007). *Consumer Fraud and Identity Theft Complaint Data.* Washington, D.C.: Federal Trade Commission.

Federal Trade Commission. (2007). *Consumer Fraud and Identity Theft Complaint Data.*

Federal Trade Commission. (2008). *Consumer Fraud and Identity Theft Complaint Data.* Washington, D.C.: Federal Trade Commission.

Financial Fraud Action UK. (2010). *Fraud, The Facts 2010.* Financial Fraud Action UK.

Finanstilsynet. (2011). *Fact & Figures*. Retrieved April 15, 2011, from Finanstilsynet.net: http://www.finanstilsynet.dk/en/Tal-og-fakta.aspx

Florencio, D., & Herley, C. (2007). A Large Scale Study of Web Password Habits. *International World Wide Web Conference Committee* (pp. 657-665). Alberta, Canada: International World Wide Web Conference Committee.

FraudWatch International. (2011). *Phishing Email Methods* . Retrieved September 4, 2011, from FraudWatch International: http://fraudwatchinternational.com/phishing-fraud/phishing-email-methods/

Friesland Bank. (2011). *Friesland Bank*. Retrieved 07 09, 2011, from Friesland Bank: http://www.frieslandbank.nl

Goeijenbier, F. (2010, 02). Internet fraud: A study into Man-in-the-Middle attack at Dutch banks. Rotterdam, NL: Erasmus University.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*(2), 13-20.

GOVCERT.NL. (2010). *Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010.* The Hague, The Netherlands: GOVCERT.NL.

Government of Australia. (2001, October 1). Cybercrime Act 2001. Australia.

Guardia di Finanza. (2011). *Rapporto Annuale 2010.* Guardia di Finanza.

Hayward, C. (2004). *Identity theft.* Nova Science Pub Inc.

HEC. (2011). *The Centre of Expertise*. Retrieved August 15, 2011, from The Centre of Expertise: http://www.hec.nl/home/english/75

Honeynet Project and Research Alliance. (2005, March). *Know your enemy: Tracking Botnets*. Retrieved May 24, 2011, from The Honeynet Project: http://www.honeynet.org/node/52

Hutchinson, D., & Warren, M. (2003). Security for Internet banking: a framework. *Logistics Information Management*, 64-73.

ING Bank. (2011). Retrieved May 23, 2011, from ING Bank: http://www.ing.nl/particulier/

Innopay. (2010). *Online payments 2010 - Increasingly a global game.* Amsterdam: Innopay.

Internet Crime Complaint Center. (2009). *2009 IC3 Annual Report.* Internet Crime Complaint Center. Internet Crime Complaint Center.

Internet World Stats. (2009, December 31). *Countries with Highest Internet Penetration Rates*. Retrieved May 25, 2011, from Internet World Stats: http://www.internetworldstats.com/top25.htm

ISACA. (2007, May). *COBIT 4.1 Executive Summary.* Retrieved March 20, 2011, from ISACA: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

ISO 31000. (2009). *ISO 31000.* Geneva, Switzerland: International Organization for Standardization.

ISO/IEC 13335-1:2004. (2004). *ISO/IEC 13335-1:2004.* ISO/IEC.

ISO/IEC 27005:2008. (2008). *ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management.* ISO/IEC.

Jakobsson, M., & Myers, S. (2006). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft.* Wiley-Interscience.

Kabay, M. (2009). Understanding Studies and Surveys of Computer Crime. In S. Bosworth, M. Kabay, & E. Whyne, *Computer Security Handbook.*

Korps landelijke politiediensten. (2010). *Overall-beeld Aandachtsgebieden.* Driebergen: KLPD - Dienst Nationale Recherche.

Luca Becchetti, C. C.-Y. (2008, March). Web Spam Detection: link-based and content-based techniques. *ACM Transactions on the Web, 2*(1), 1-42.

MacDonald, Z. (2002). Official Crime Statistics: Their Use and Interpretation. *The Economic Journal*.

Maltz, M. (1977). Crime Statistics: A Hstorical Perspective. *Crime & Delingquency*, 23:32.

Ministry of Internal Affairs. (2010, 10 04). *Wetboek van Strafrecht Artikel 326*. Retrieved 10 04, 2010, from Wetten.nl:

http://wetten.overheid.nl/BWBR0001854/TweedeBoek/TitelXXV/Artikel326/geldigheidsdatum_04-10-2010

Moore T., Clayton R. & Anderson R. (2009). The Economics of Online Crime. Journal of Economic Perspectives, 3-20

Myers, M. D., & Avison, D. (2002). *Qualitative Research in Information Systems.* London, UK: Sage Publications Ltd.

National Council for Crime Prevention Brå. (2010, October 28). *Brå - Brottsförebyggande rådet - Statistical tables*. Retrieved March 03, 2011, from National Council for Crime Prevention Brå: http://www.bra.se/extra/pod/?action=pod_show&id=21&module_instance=11

NICC - ICTU. (2010). *United against cybercrime.* NICC - ICTU. The Hague: NICC - ICTU.

NICC - ICTU. (2011). *NICC - ICTU*. Retrieved August 24, 2011, from Samen tegen cybercrime: http://www.samentegencybercrime.nl/

NVB. (2010). *3x Kloppen*. Opgeroepen op 10 04, 2010, van 3x Kloppen: http://www.3xkloppen.nl/

NVB. (2011). *Vragen en antwoorden : Fraude met internetbankieren en oprichting ECTF.* Amsterdam: NVB.

Oppliger, R., Rytz, R., & Holderegger, T. (2009). Internet Banking: Client-Side Attacks and Protection Mechanisms. *Computer*.

Parker, D. (2002). *Fighting Computer Crime: A New Framework for Protecting Information.* Wiley.

PCAOB. (2007, November 15). *Auditing Standard No. 5 .* Retrieved March 22, 2011, from PCAOB: http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx

Provan, K., & Kenis, P. (2007). Modes of Network Governance: Structure, Management, and Effectiveness. *Journal of Public Administration Research and Theory*, 229-259.

Pudney, S., Deadman, D., & Pyle, D. (2000). The Relationship between Crime, Punishment and Economic Conditions: Is Reliable Inference. *Journal of the Royal Statistical Society. Series A (Statistics in Society)*, 81-97.

PwC. (2011). *PwC.com*. Retrieved 08 20, 2011, from PwC.com: http://pwc.com

Rabobank. (2011). Retrieved May 23, 2011, from Rabobank: http://www.rabobank.nl/

Raval, V., & Fichadia, A. (2007). *Risks, Controls, and Security.* Hoboken, New Jersey, USA: John Wiley & Sons.

Richardson, R. (2008). *CSI Computer Crime & Security.* Computer Security Institute.

Rijksoverheid. (n.d.). *Veilig internetten*. Retrieved 10 04, 2010, from Veilig internetten: http://www.nederlandveilig.nl/veiliginternetten/

Sécurité intérieure et des Libertés Locales. (2005). *Chantier sur la lutte contre la Cybercriminalite.*

Shaw, H. (2006, March 15). *The Trouble with COSO*. Retrieved March 10, 2011, from CFO.com: http://www.cfo.com/printable/article.cfm/5598405?f=options

Shirey, R. (2000, May). *RFC 2828: Internet Security Glossary.* Retrieved May 26, 2011, from The Internet Engineering Task Force (IETF): http://tools.ietf.org/html/rfc2828

SNS Bank. (2011). *SNS Bank*. Retrieved 07 09, 2011, from SNS Bank: http://www.snsbank.nl

Sonnenreich, W., Albanese, J., & Stout, B. (2005). Return On Security Investment (ROSI): A Practical Quantitative Model. *Journal of Research and Practice in Information Technology*, 239-252.

Soy, S. K. (2006, February 12). *The Case Study as a Research Method.* Retrieved April 25, 2011, from http://www.ischool.utexas.edu/~ssoy/usesusers/l391d1b.htm

StatBank Norway. (n.d.). Retrieved 03 05, 2011, from Statistics Norway: http://statbank.ssb.no/statistikkbanken/Default_FR.asp?PXSid=0&nvl=true&PLanguage=1&tilside=selecttable/hovedtabellHjem.asp&KortnavnWeb=lovbrudda

Statistics Denmark. (2011). *Danish Statistics*. Retrieved April 15, 2011, from Statistics Denmark: http://www.dst.dk/HomeUK/About/Library/danstat.aspx

Statistics Norway. (2011). *Table 4 Offences reported to the police, by type of offence. 1993-2010*. Retrieved April 15, 2011, from Statistics Norway: http://www.ssb.no/a_krim_tab_en/tab/tab-2011-03-21-04-en.html

Straub, D., & Welke, R. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 441-469.

The Hague University. (2011). *Quick facts*. Retrieved August 20, 2011, from The Hague University: http://www.thehagueuniversity.com/about-us/quick-facts

The SANS Institute. (n.d.). *Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines.* Retrieved March 9, 2011, from The SANS Institute: http://www.sans.org/critical-security-controls/

The Spamhouse Project. (2011). *The Spamhouse Project - The Definition of Spam*. Retrieved 07 09, 2011, from The Spamhouse Project: http://www.spamhaus.org/definition.html

Thornburgh , T. (2004). Social engineering: the "Dark Art". *1st annual conference on Information security curriculum development* (pp. 133-135). Kennesaw, Georgia: ACM.

U.S Department of Homeland Security. (2009, July 06). *UNITED STATES SECRET SERVICE SIGNS PARTNERSHIP AGREEMENT WITH ITALIAN OFFICIALS.* Retrieved April 15, 2011, from Secret Service: http://www.secretservice.gov/press/GPA05-09_EuropeanECTF.pdf

U.S Department of Homeland Security. (2010, August 09). *UNITED STATES SECRET SERVICE SIGNS PARTNERSHIP AGREEMENT WITH UNITED KINGDOM OFFICIALS.* Retrieved April 15, 2011, from US Secret Service: http://www.secretservice.gov/press/GPA06-10_LondonECTF.pdf

UK Payments Administration. (n.d.). *UK Payments Administration - Resources and Publications*. Retrieved 09 14, 2010, from UK Payments Administration: http://www.ukpayments.org.uk/resources_publications/

United States Department of Justice. (2004). *Reporting Computer, Internet-Related, or Intellectual Property Crime.* Retrieved April 4, 2011, from United States Department of Justice: http://www.justice.gov/criminal/cybercrime/reporting.htm

US General Accountability Office United States. (2002). *Identity Theft: Prevalence and Cost Appear to be Growing.*

Zeviar-Geese, G. (1997-1998). The State of the Law on Cyberjurisdiction and Cybercrime on the Internet. *Gonzaga Journal Of International Law, 1*.

Appendix A: OWBF statistics in peer countries

Country	Year	Citizens	Cases #	/100.000	Damage/incident	Total damage	Currency	Source	What is measured	Notes	Research method
USA	2010	317.641.000	(unknown)	(unknown)	(unknown)	(unknown)	USD	CyberSource	N/A	Commercial Anti-Crime Organization	Survey
Norway	2010	4.855.000	(unknown)	(unknown)	(unknown)	(unknown)	NOK	N/A	Police reports	Governmental body, non-specific fraud	Governmental crime database
Denmark	2010	5.481.000	(unknown)	(unknown)	(unknown)	(unknown)	DKK	N/A	Police reports	Governmental body, non-specific fraud	Governmental crime database
Sweden	2008	9.200.000	10.222	111,11	(unknown)	(unknown)	SEK	Brå	Police reports	Governmental body, definition issues	Governmental crime database
	2009	9.300.000	13.800	148,39	(unknown)	(unknown)	SEK	Brå	Police reports	Governmental body, definition issues	Governmental crime database
Germany	2008	82.100.000	37.900	46,16	982	37.200.000	EUR	Bundeslagebild IUK	Police reports	Governmental body	Governmental crime database
	2009	81.900.000	50.254	61,36	734	36.900.000	EUR	Bundeslagebild IUK	Police reports	Governmental body	Governmental crime database
UK	2004	59.900.000	(unknown)	(unknown)	(unknown)	12.200.000	GBP	FinancialFraudActionUK	Confirmed cases	Financial Industry report	Crime database
	2005	60.200.000	(unknown)	(unknown)	(unknown)	23.200.000	GBP	FinancialFraudActionUK	Confirmed cases	Financial Industry report	Crime database
	2006	60.600.000	(unknown)	(unknown)	(unknown)	33.500.000	GBP	FinancialFraudActionUK	Confirmed cases	Financial Industry report	Crime database
	2007	61.000.000	(unknown)	(unknown)	(unknown)	22.600.000	GBP	FinancialFraudActionUK	Confirmed cases	Financial Industry report	Crime database
	2008	61.400.000	(unknown)	(unknown)	(unknown)	52.500.000	GBP	FinancialFraudActionUK	Confirmed cases	Financial Industry report	Crime database
	2009	61.800.000	(unknown)	(unknown)	(unknown)	59.700.000	GBP	FinancialFraudActionUK	Confirmed cases	Financial Industry report	Crime database
France	2010	62.600.000	(unknown)	(unknown)	(unknown)	(unknown)	-	N/A	N/A	N/A	None
Spain	2010	46.000.000	(unknown)	(unknown)	(unknown)	(unknown)	-	N/A	N/A	N/A	None
Italy	2010	60.200.000	(unknown)	(unknown)	(unknown)	(unknown)	-	N/A	N/A	N/A	None
The Netherlands	2008	16.400.000	(unknown)	(unknown)	(unknown)	2.100.000	EUR	NVB	Confirmed cases	Banking organization report	Private banking org.
	2009	16.500.000	154	0,93	12.338	1.900.000	EUR	NVB	Confirmed cases	Banking organization report	Private banking org.
	2010	16.600.000	1.383	8,33	7.086	9.800.000	EUR	NVB	Confirmed	Banking organization	Private banking org.

									cases	report	
Australia	2010	21.551.000	(unknown)	(unknown)	(unknown)	(unknown)	AUD	N/A	N/A	N/A	None
	2009	21.293.000	(unknown)	(unknown)	(unknown)	(unknown)	AUD	N/A	N/A	N/A	None

Table 10: OWBF statistics in peer countries

Appendix B: Semi-structured interview questions

The interview questions have a semi-structured nature which means that at least the following questions must be discussed with each expert. At the interviewer's discretion, additional questions may be necessary to enhance the quality of the results.

The first two questions are meant to establish the context and credibility of the expert, while the remaining questions are used to answer the research questions.

1. What is your current position within your organization? How does that relate to Dutch retail banking?
2. What is the relevance of OWBF to:
    a. You
    b. Your banking clients, if you have them
    c. Your organization
3. There seem to be a lot of differences in the response to OWBF in Western countries. Could more international cooperation, either on the corporate, lobby, or governmental level benefit the fight against OWBF? How, exactly?
4. How effective are the technological external security controls for OWBF?
5. How effective are the social external security controls for OWBF?
6. How satisfied is your organization (or your clients) with the achieved level of external control?
7. Can the effectiveness of the technological external security controls for OWBF be improved? How?
8. Can the effectiveness of the social external security controls for OWBF be improved? How?

Appendix C: Interview invitations

Organization	Business unit or section	Response
ABN AMRO	-	Negative
Rabobank	Information Risk Management	Positive (D)
SNS REAAL	-	Negative
ING	-	Negative
Friesland Bank	-	Negative
Ernst & Young	IT Risk and Assurance	Positive (B)
KPMG	IT Risk and Compliance	Positive (reserve)
PWC	Systems & Process Assurance	Positive (C)
Het Expertise Centrum	Public-sector management and auditing advisor	Positive (A)

Table 11: Sent interview invitations with responses