MASTER THESIS

CYBERCRIME AND THE IMPACT ON BANKS' FRONTLINE SERVICE EMPLOYEES

A qualitative study towards the impact of cybercrime on the experiences, concerns and actions taken by Frontline Service Employees within the banking sector.

Fleur Staal
S0207233

EXAMINATION COMMITTEE
N. Baas, MSc.
Dr. J. Karreman

UNIVERSITY OF TWENTE.

Title:
Cybercrime and the impact on banks' Frontline Service Employees.
A qualitative study towards the impact of cybercrime on the experiences, concerns and actions taken by Frontline Service Employees within the banking sector.

Name student: Fleur Staal
Student number: S0207233

Faculty of Behavioral Sciences
Communication Studies
Master Corporate Communication

Hengelo, 1 May 2015

First supervisor: N.Baas, MSc.
Second assessor: Dr. J. Karreman.

Preface

Writing my preface, I realize that it's the last part I have to write for my thesis. The result of months of research, talking with participants and reading lots of articles about cybercrime. Of course, I couldn't do this all, without the help of some people.

First, I would like to thank my supervisors Niels Baas en Joyce Karreman for a number of helpful meetings. I learned a lot from your expertise and feedback that supported me to finish this thesis. It was a pleasure to have you both as my supervisor.

Second, my special thanks go to Lisa. I would like to thank Lisa for her support and her contribution to reading and revising my final report.

I would also like to thank my family for their endless support to finish my thesis. Rik, you always said that I could do this. Thank you for your support and for always believing in me.

Last, but definitely not least, thanks to those who participated. I really appreciate it.

Enjoy reading!

Fleur Staal
Hengelo, May 2015

UNIVERSITY OF TWENTE.

Abstract

An increasing number of banks rely on digital networks for their business operations. This increases the risks for banks and their customers of becoming a cybercrime victim. This study focuses specifically on Frontline Service Employees in the banking sector, because they have an important role in providing customers with information about cyber security. Therefore, they must be aware of cybercrime and its consequences. This awareness needs to be increased, so that all employees are able to take appropriate measures to reduce the risk of cyber threats. This study aims to understand more about the conception FSE's have towards cybercrime, by focusing on the relationship between experiences and concerns over cybercrime and the resulting actions. Using a sample of 25 FSE's from the banking sector in the Netherlands, the impact of cybercrime is examined by means of interviews. The results show that FSE's in general have little knowledge about the consequences of cybercrime. However, their experiences ensure that they can provide customers with basic information. To cope with, the threat of, cybercrime, FSE's use their experiences and problem-focused coping strategies. They try to find out more about the situation and concentrate on the next step in helping the customer as good as possible. Banks should consider special courses to establish more awareness among these employees about the consequences of cybercrime. FSE's could use this acquired knowledge to provide customers with more specifically information about cybercrime.

Keywords: Cybercrime, Banking sector, Frontline Service Employees, Coping, Coping strategies

Samenvatting

Net zoals in veel organisaties, neemt ook voor banken het gebruik en daarmee de afhankelijkheid van ICT nog altijd toe. Steeds meer processen en diensten, zoals internetbankieren, zijn hier volledig van afhankelijk. Tegelijkertijd nemen ook de risico's voor deze organisaties en hun klanten toe. Dit onderzoek richt zich op de service medewerkers in de banken sector, omdat zij een belangrijke schakel zijn in het informeren van klanten over cybercrime. Daarom is het belangrijk dat zij zich bewust zijn van cybercrime en de gevolgen daarvan. Deze bewustwording moet worden verhoogd, zodat alle medewerkers in staat zijn om passende maatregelen te nemen om het risico van cybercrime te verminderen. Dit onderzoek heeft als doel om meer inzicht te krijgen in het beeld dat service medewerkers hebben ten opzichte van cybercrime, door te focussen op de relatie tussen ervaringen, de zorgen die medewerkers kunnen hebben en de daaruit volgende acties. 25 service medewerkers uit de banken sector zijn voor dit onderzoek geïnterviewd. Uit de resultaten blijkt dat de medewerkers over het algemeen weinig kennis hebben over cybercrime en de gevolgen die het met zich mee kan brengen. Om met, de dreiging van, cybercrime om te gaan gebruiken service medewerkers voornamelijk hun ervaring en probleem gerichte coping strategieën. Ze proberen meer over de situatie te weten te komen en concentreren zich op de stappen die moeten worden ondernomen om de klant zo goed mogelijk te kunnen helpen. Banken zouden specifieke cursussen kunnen geven om meer bewustzijn onder de werknemers te creëren. Service medewerkers kunnen op hun beurt de opgedane kennis gebruiken, om klanten te voorzien van meer specifieke informatie over cybercrime.

TABLE OF CONTENTS

CYBERCRIME AND THE IMPACT ON BANKS' FRONTLINE SERVICE EMPLOYEES

A qualitative study towards the impact of cybercrime on the experiences, concerns and actions taken by Frontline Service Employees within the banking sector.

1. Introduction

Organizations have become increasingly virtual (Arachchilage and Love, 2014; National Cyber Security Centre [NCSC], 2014). As more daily activities migrated online and people's reliance on the Internet grows, the potential of hacking, attacks and other security breaches by cyber criminals increase rapidly (Böhme and Moore, 2012; Arachchilage et al., 2014). According to Wada and Odulaja (2012) it is an everyday reality and it is growing in an unprecedented dimension in line with the ICT development.

In the past few years, banks were often target of the so-called Distributed Denial-of-Service attack (DDoS attack). With a DDoS attack large amounts of data are send to the servers of banks so that they are inaccessible for users. There also has been more media coverage concerning cyber attacks. It is in the news everyday and reported on widely by both classical and new media (NCSC, 2013b). Cyber attacks, like DDos attacks, phishing, hacking incidents, and viruses targeting individuals, corporations and government sites, are all united under the word most frequently used by the media, '*cybercrime*' (Jang and Lim, 2012).

Not only the media adopted the term cybercrime, also academia, law enforcement and governments use it to refer to online criminal activities (Hunton, 2009). Cybercrime covers a wide range of activities that are related to the use of information communication technology [ICT] for criminal purposes (Hunton, 2009; Kraemer-Mbula, Tang and Rush, 2013; Leukfeldt, Veenstra and Stol, 2013; Jang et al., 2012), and poses a serious threat to public and private organizations (Stokkel and Smulders, 2013; NCSC, 2013a).

An increasing number of financial organizations are the target of cyber criminals (Manzoor, 2014). The growing threat of cybercrime globally requires all employees of an organization to be aware of cybercrime dangers. This awareness needs to be increased, so that all employees are able to take appropriate measures to reduce the risk of cyber threats. It is not a matter for the ICT department or the Chief Information Officer [CIO] alone to prevent the organization against cyber attacks (NCSC, 2013b; NCSC, 2014). Cybercrime can harm the continuity of business processes and organizations suffer financial and reputational harm (de Joode, 2011; Bhasin, 2007). In addition, it affects the core of the organization, including all employees. Employees must recognize and assess risks of the use of ICT, but also which measures should take to reduce risks (NCSC, 2014; de Joode, 2011; Arachchilage et al., 2014).

This study focuses on the Frontline Service Employees [FSE's]. These employees have an important role regarding the organization's reputation and play a salient role in customers' satisfaction and perceptions of service quality (Whiting, Donthu and Baker, 2011: Elmadag, Ellinger and Franke, 2008; Di Mascio, 2010; Jackson and Sirianni, 2009; Coelho, Augusto and Lages, 2010; Singh, 2010; Malhotra, Mavondo, Mukherjee and Hooley, 2013).

Delivering service quality to customers is important to succeed and survive in today's competitive banking environment (Samli and Frohlich, 1992, in: Yavas, Bilgin and Shemwell, 1997). Therefore, FSE's must be aware of cyber threats and measures to reduce the risks of cyber threats in their respective organizations (Finau, Samuwai and Prasad, 2013).

The extant literature, specific to the cybercrime discipline, has concentrated on how different forms of cybercrime impact customers (Böhme et al, 2012; Martin and Rice, 2011; Saini, Rao and Panda, 2012) and organizations (Bhasin, 2007; Lagazio, Sherif and Cushman, 2014). However, the impact on employees, especially FSE's, had not been studied before. Therefore, the aim of this study is to gain deeper insights into the impact of cybercrime in the banking sector, especially the impact of cybercrime on banks' FSE.

The emphasis of this study is on the relationship between cybercrime and the impact on bank FSE's, by focusing on the relationship between experiences and concerns over cybercrime and the resulting actions. These actions are the coping strategies FSE's use when they interact with customers. The central question in this paper is: *How do Frontline Service Employees react to, the threat of, cybercrime?* It is important for organizations to understand the factors, feelings and experiences that affect FSE's *perspectives* and *performances* to ensure that their attitude and behavior are conducive to delivering service quality (Whiting et al., 2011).

2. Theoretical framework

2.1. What is cybercrime?

The use and dependence of Information and Communications Technology [ICT] increase. It is a driving force in our society and a growing number of processes are completely dependent of ICT (Arachchilage and Love, 2013; Liang and Xue, 2009; NCSC, 2014). ICT can improve human and organizational performance, but when ICT is exploited for malicious purposes, it can pose huge threats to individuals, organizations and society (Liang et al., 2009).

Despite the fact that the term cybercrime has entered into common usage, many people find it hard to define cybercrime precisely. In addition there is no universally accepted definition of cybercrime (Hunton, 2009; Kraemer-Mbula et al., 2013; Kshetri, 2013; Leukfeldt et al., 2013). The definition of cybercrime depends on its final purpose, means and classifications (Leukfeldt et al., 2013). According to the NCSC (2013, p.106) cybercrime is defined as *"a form of criminality that targets an ICT system or the information it processes"*. In other words, cybercrime describes all kinds of crime and other illicit activities that involve the use of telecommunications networks, in which computers or computer networks are a tool, a target, or a locale of criminal activity (Hunton, 2009; Kraemer-Mbula et al., 2013).

Cybercriminals attack systems, or get access to confidential information and data from users. Therefore, they make use of a wide range of techniques (Hunton, 2009; Arachchilage et al., 2014). They use techniques such as ”a set of computer programs which can disturb the normal behavior of computer systems (viruses), malicious software (malware), unsolicited email (spam), monitoring software (spyware), attempting to make computer resources unavailable to its intended users (Distributed Denial-of-Service or DDos-attack), the art of human hacking (social engineering) and online identity theft (phishing)” (Arachchilage et al., 2014, p. 304). These types of attacks are frequently used and pose a serious threat to public and private organizations, including the banking sector (Stokkel et al., 2013; Bhasin, 2007). It also impacts the daily activities of businesses and government (Choo, 2011).

2.2. Cybercrime and the banking sector

(Financial) cybercrime increases by the ongoing digitalization. More and more organizations rely on digital networks for their business operations. This increases the risk for organizations and their customers of becoming victims of cybercrime. Over the past few years there were several cyber attacks in the banking sector and on various components of online banking. Those attacks varied from stealing money to disabling online payment systems such as online banking through websites, mobile apps and iDeal. Cyber attacks in the banking sector are mainly fraud related, because of the financial gain and have many forms (Arachchilage et al., 2014: NCSC, 2014; Lagazio et al., 2014; Bhasin, 2007). Table 1 (p.11) gives an overview of the main cyber attacks that banks consider as a risk.

Table 1: overview of the main cyber attacks which banks consider as a risk (NCSC, 2013b, p. 105-110).

Cybercrime	Definition
Phishing	An umbrella term for digital activities with the object of tricking people into giving up their personal data. This personal data can be used for criminal activities such as credit card fraud and identity theft.
Malware	A contraction of ‘malicious’ and ‘software’. As a generic term, malware currently includes infection of computers with viruses, worms and Trojans.
Skimming	The illegitimate copying of data from an electronic payment card such as a cashpoint card or a credit card. Skimming often involves the theft of pin codes with the final objective of making payments or to draw money from the victim’s account.
DDos-attacks	(Distributed) Denial of Service term for a type of attack in which a particular service (e.g. a website) becomes unavailable to the usual consumers of the service. DDoS attacks on websites are often performed by bombarding websites with huge amounts of network traffic, so that they become unavailable.

Phishing affects financial organizations, in particular banks, worldwide. An increasing number of banks become the target of phishing attack criminals (Manzoor, 2014). Phishing and malware are forms of online banking fraud, whereby criminals steal confidential information and online banking details from its victims (Arachchilage et al., 2014). Another form of cybercrime is skimming. Skimming refers to stealing customer card information and Personal Identification Numbers (PINs). Criminals installed skimming devices at Automatic Teller Machines (ATM's) to steal this kind of confidential information (Choo, 2011). Besides phishing, malware and skimming, a *Distributed Denial of Service attack* [DDoS attack] is also seen as a risk for banks (Bhasin, 2007). DDos attacks are attacks in which particular services (e.g. the website of the bank, iDeal or Digi-D) becomes unavailable to the usual consumers of the services (NCSC, 2014). Between January 1st and September 11th 2013, a total of 39 DDoS attacks disrupted the services of the bank of which one-third were subject to the banking sector (NCSC, 2013a).

The impact of cybercrime has generated a significant risk exposure for individuals (personal harm) and organizations (reputational harm). It includes exposure to financial losses, regulatory issues, data breach liabilities, damage to brand and reputation, and loss of client and public confidence (Verma, Hussain and Kushwah, 2012). Cybercriminals can significantly threaten the finances and reputations of banks and other (financial) organizations. Moreover, it affects the relationship between the image of the organization and the trust that customers and other stakeholders have in the organization. Consequent negative publicity can create some serious issues for organizations when they become victims of cybercrime (de Joode, 2011).

2.2.1. Organizational crises as a result of cybercrime

When banks are confronted with cybercrime, crises can occur. According to Coombs (1999, in: Miller, 2009, p.187) "Organizational crisis is an event that is an unpredictable, major threat that can have a negative effect on the organization, industry, or stakeholders if handled improperly". Crisis can disorganize an organization due to its unplanned character. Miller (2009) describes three stages in which organizational crisis can evolve: (1) pre crisis, (2) crisis, and (3) post crisis.

Pre crisis

In this stage, employees can work to prevent or prepare themselves, the organizations and their stakeholders for possible problems (Coombs, 2007; Miller, 2009). For example, banks implement cyber security measures to protect information and the functioning of ICT. According to the National Cyber Security Centre [NCSC] (2013b, p. 17-18), cyber security is '*being free of the danger of harm caused by the disruption, failure or inappropriate use of ICT'.* Cyber security can help in gaining a good reputation and restricts the actual occurrence of incidents and the damage they entail.

The study of Arachchilage and Love (2013) has indicated that technology alone is insufficient to solve critical ICT security problems. Cybercrime can occur due to computer-related threats and due to individuals' conventional behaviors. It is important, for organizations and individuals, to fight cybercrime using both technological and conventional behavioral countermeasures (Arachchilage et al, 2013; Arachchilage et al., 2014; Lai, Li and, Hsieh, 2012; Metalidou, Marinagi, Trivellas, Eberhagen, Skourlas and Giannakopoulos, 2014). Therefore, cyber security begins with awareness of the whole organization. It is not a matter for the ICT department or the CIO alone. Cybercrime influences the continuity of business processes, reputation, cost and liability of protecting customer or personal data and risk management (de Joode, 2011; NCSC, 2014).

In the first place, banks can use technological solutions such as basic protection- and preventive measures (Bhasin, 2007). According to the NCSC (2013a) Dutch banks have a very high standard of security measures. Within banks many ICT experts work day and night to keep the payment systems and transactions as safe as possible. They monitor possible DDos attacks and if necessary take additional (technological) measures. They can, for instance, temporarily restrict access to their website. Banks also implement mechanisms to restrict the effects of abuse. Geo-blocking, for example, ensures that a skimmed bankcard cannot be used outside the user's usual geographical area.

Secondly, employees must recognize and assess risks of the use of ICT and also know which measures should be taken to reduce risks and errors in the use of ICT. To create awareness regarding the types of cyber risks, banks could organize seminars, or trainings for their employees (NCSC, 2014; de Joode, 2011; Bhasin, 2007). In addition to create awareness among customers, banks provide extensive explanation on their websites about how criminals carry out attacks, what security measures the bank have implemented and how customers can secure their devices and confidential information as effectively as possible. The *Nederlandse Vereniging van Banken* [Dutch Association of Banks, NVB] has set up an awareness-raising website that makes active reference to the risks of cybercrime (NCSC, 2013a). According to Arachchilage and Love (2014), where it is impossible to entirely eliminate the end-user from the system, the best possible approach for computer security is to educate the end-user in prevention.

Crisis

During the crisis stage, there is a trigger (e.g. cyber attack) that threatens an organization's survival or reputation (Miller, 2009) and managers must actually respond to a crisis (Coombs, 2007). Besides security measures, banks need to be well prepared for cyber incidents. In case of emergency, banks should have a solid incident response plan as part of their policies and procedures. This plan can limit the damage to the banks' image and reputation (Coombs, 2006; Bhasin, 2007). During a crisis, there is a lot of uncertainty (Miller, 2009). Decisive actions (e.g. disabling all affected technology) and clear communication (e.g. what organizations say and do after crisis hits the organization) are important to preserve the trust of customers and to protect the organization's reputation (Coombs, 2006). Similar, banks should communicate toward their customers. However, research has shown that banks and financial organizations often do not communicate when they have had to deal with a cyber attack. They fear of revealing their weaknesses and a consequent loss of confidence amongst their clients and of reputational damage (Choo, 2011; Kraemer-Mbula et al., 2011).

Reputation is about how an organization is perceived by its public. To protect the organizational reputation it is important to select the appropriate crisis response strategies, which can be chosen by crisis managers. Coombs Situational Crisis Communication Theory [SCCT] provides a crisis manager with three basic options for using crisis response strategies. The three basic response options are deny, diminish, and deal (Coombs, 2006). Table 2 (p.14) provides an overview of the various crisis response strategies according to these three options.

Table 2: Crisis response strategies (Coombs, 2006)

Response option	Definition
Deny	Establish that no crisis exists
Diminish	Alter the attributions about the crisis even to make it appear less negative to stakeholders
Deal	Alter how stakeholders perceive the organization-work to protect/repair the reputation

Post crisis

In the post-crisis stage, organizations are returning to business as usual. There are some key activities that must transpire. Firstly, managers should deliver all information promised to the customers, and other stakeholders of the bank, as soon as that information is known. Secondly, keep stakeholders updated on the progression of recovery efforts and finally, evaluate and analyze the crisis. To understand why the crisis occurred, learn from the crisis and integrate those lessons into the organization's crisis management system (Coombs, 2007).

Communication should focus on determining responsibility, perhaps apologizing, and establishing systems for coping with similar crises in the future. In all three stages, organizations have to deal with 'unplanned' change processes. Therefore, communication processes play a key role in coping with a wide range of these unplanned change processes (Miller, 2009).

2.3. Frontline Service Employees

The growing threat of cybercrime globally requires crisis managers to be aware. However, all employees have to take appropriate measures to reduce the risk of cyber threats (Finau et al., 2013; NCSC, 2014). Within the banking sector, Frontline Service Employees [FSE's] have an important role in relation to the reputation of the bank and have an important role in customer's satisfaction and perception of service quality (Whiting et al., 2011: Elmadag et al., 2008; Di Mascio, 2010; Jackson et al., 2009; Coelho et al., 2010; Singh, 2010; Malhotra et al., 2013).

Banks' FSE's are the service employees and the advisors for private customers. These advisors are working in the banking hall as well as in the Customer Contact Centre. They are important for the first contact with private customers in the banking hall as well as, via telephone, email and the Internet. FSE's personal interactions are at the front of most services in firm activities (Jackson et al., 2009). They represent the organization, the brand, and the marketing to customers (Zeithaml & Bitner, 2003, in: Whiting et al., 2011). The service that FSE's provide is critical in developing customer relationships, gathering customer information, and in creating customer satisfaction, loyalty and brand commitment (Malhotra et al., 2013).

Most FSE's are simultaneously concerned with their own and their customers' well being (Paulin, Ferguson and Bergeron, 2006), exhibit high levels of emotional engagement during customer interactions and thus creating a chronically stressful environment for themselves (Whiting et al., 2011). In addition, all employees must be aware of cyber threats (NCSC, 2014; Finau et al., 2013). According to Finau et al. (2013) the responsibility of cyber security primarily rests with the ICT department of the organization. However, all employees have an important role in effectively implementing their organization's cyber security plan. To succeed and survive in today's competitive banking environment, it is important for organizations to deliver service quality towards customers (Samli and Frohlich, 1992, in: Yavas et al., 1997).

2.4. Coping

In this study cybercrime will be used as a stressor, to get more insight in the immediate FSE outcomes such as stress, problem- and emotion-focused coping strategies, and service quality. Under stressful conditions, FSE's evaluate, select, and employ coping mechanisms (Whiting et al., 2011). Depending on the person and stressor, a person can cope by trying to solve the problem, talking to colleagues, inviting distractions, venting, getting outside help, pretending that all is well or freaking out (Kassin, Fein and Markus, 2008). According to Folkman et al. (1986, in: Lai et al., 2012) coping is defined as *"a person's efforts to manage demands, whether or not the efforts are successful"*. When people cope, they try to manage with difficult circumstances when they are faced with fear, stress or a threat (Lai et al., 2012).

When a person is faced with a stressful situation, he or she goes through a cognitive appraisal. This is a process through which a person evaluates whether a particular encounter with the environment is relevant for his or her wellbeing. The person can have different emotional reactions to the same event. If the person appraises the environmental situation to be stressful or affecting the individual's wellbeing, he or she generates potential coping strategies that help manage the situation (Kassin et al., 2008; Whiting et al., 2011). Lazarus and Folkman distinguished two general types of coping strategies (Kassin et al., 2008; Whiting et al., 2011; Carver, Weintraub and Scheier, 1989).

Table 3 (p.16) gives an overview of the two coping strategies.

Table 3: Coping strategies and scales

Coping strategy		**Scales**
Problem-focused	Taking actions to alter the stressor	Active coping; suppression of competing activities; technological coping
Emotion-focused	Reducing emotional distress	Seeking social support; denial; focusing on and venting emotions; denial; acceptance

The first is problem-focused coping. Problem-focused coping strategies are the cognitive and behavioral efforts to reduce stress by overcoming the source of the problem. It is an attempt to obtain information or perform actions to change the problem, such as making a plan of action, trying to find out more about the situation, or concentrating on the next step (Whiting et al., 2011; Kassin et al., 2008; Yavas and Babakus, 2011).

A second strategy is emotion-focused coping. When people are focused to reduce their emotional distress, people will use the emotion-focused strategy. This approach deals with the strategies an individual undertakes, by distancing oneself, in order to change his feelings and emotions toward the threat and crisis. Then the individual becomes less sensitive to the threat (Lai et al., 2012; Kassin et al., 2008; Yavas et al., 2011). Emotion-focused coping involves regulating emotions to overcome or reduce the impact of the situation, and it can occur in several forms, such as seeking social support, denial, or escapism (Whiting et al., 2011).

Coping scales

The psychological and behavioral moves undertaken to manage the situation are known as coping strategies. An individual FSE may use multiple coping strategies in a stressful encounter. The coping strategies, which an FSE may use, can be a mix of problem- and emotion-focused coping strategies and may be influenced by one's interpretation and explanation of, the threat of, cybercrime (Whiting et al., 2011; Welbourne, Eggerth, Hartley, Andrew and Sanchez, 2007).

People tend to take an active, problem-focused approach when they think they can overcome a stressor, but fall back on an emotion-focused approach when they perceive the problem to be out of control (Kassin et al., 2008). The effectiveness of coping strategies, and how people cope with stress, may depend on the type of coping used. The literature on coping strategies (Whiting et al., 2011; Lai et al., 2012) has demonstrated that problem-focused coping is more effective than emotion-focused coping, because problem-focused coping involves directly addressing and resolving the stressor.

There are different coping strategies to help manage the situation in a problem-focused way. Taking active steps to try to remove the stressor is called *Active coping.* Active coping includes initiating direct action, increasing one's efforts and trying to execute coping attempts stepwise (Carver et al., 1989). An individual FSE could use active coping in order to help the customer as good as possible, by taking certain steps that are important to solve the problem.

FSE's can also *suppress their competing activities.* When FSE's suppress their competing activities, they can for example put other projects aside, trying to avoid becoming distracted by other events or letting other things slide in order to deal with the stressor (Carver et al., 1989). It is likely that FSE's, in case of crisis, put other work aside and focus on the customer, or at least do what is expected in case of crisis. *Seeking of social support* can also be considered as relevant coping response strategy. The workplace coping literature characterizes seeking social support as efforts to reach out to others who can provide guidance or resources to help resolve workplace issues (Whiting et al., 2011). A form of problem-focused coping is seeking social support for instrumental reasons. When FSE's seek social support for instrumental reasons, they seek advice, assistance or information by their colleagues (Carver et al., 1989).

However, FSE's can also seek social support for emotional reasons. In this case, they seek moral support, sympathy or understanding by their colleagues (Carver et al., 1989). Emotion-focused coping involves avoiding, distancing or escaping the stressor (Whiting et al., 2011). Another form of emotion-focused coping is focusing on and *venting of emotions,* by focusing on whatever distress or upset one is experiencing and to ventilate those feelings (Carver et al., 1989). FSE's may get stressed and express their emotions towards their customers or colleagues.

Following, *denial* is as a response that sometimes emerges in primary appraisal. Denial involves thoughts that resign oneself to the present situation as a means to blunt the stress that is experienced (Carver et al., 1989; Whiting et al., 2011). Instead of taking active steps to alter the stressor, the FSE could also deny the problem. The opposite of denial is *acceptance*. It is arguable that acceptance is a functional coping response, in that a person who accepts the reality of a stressful situation would seem to be a person who is engaged in the attempt to deal with the situation (Carver et al., 1989).

When people face the problem as a challenge, they seem to take a problem-oriented coping behavior and treat the problem as a thing that can be controlled. In contrast, emotion-focused coping, the problem identified as a threat and loss, people tend to perceive it as something that cannot be solved by them and hence, take an emotional coping behavior (Lai et al., 2012). If users perceive a malicious ICT threat, they are more likely to take problem-focused coping, or if they believe that the threat is not avoidable, they will inactively avoid the threat by performing emotion-focused coping (Beaudry and Pinsonneaut, 2001, in: Lai et al., 2012).

2.5. Conceptual scheme

Following from the concepts and dimensions discussed in the theoretical framework, the following conceptual scheme (p.18) is used for this study.

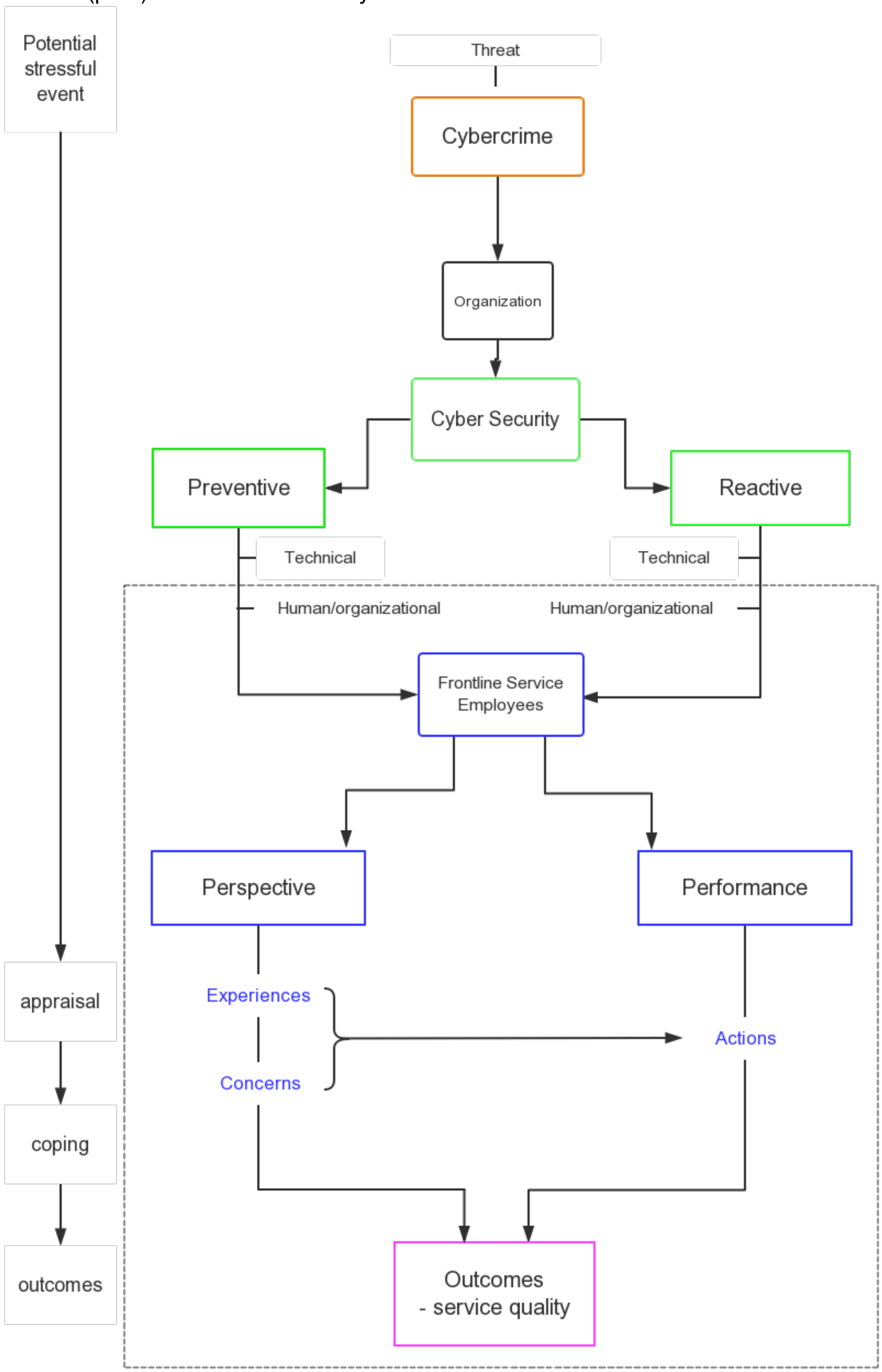

Figure 1: conceptual scheme

This study looks at the relationship between cybercrime and the impact on banks' Frontline Service Employees (FSE's). The focus is on the concepts *perspective* and *performance.* Within the concept of perspective, the focus is on the relationship between experiences and concerns over cybercrime. The concept of performance is focusing on the resulting actions taken by FSE's.

In appendix A, the operationalization of the concepts *perspective* and *performance* can be found. According to the conceptual scheme, banks are confronted with different forms of cyber attacks (potential stressful event). To defend themselves against cyber-attacks, most banks take preventive and reactive measures (cyber security). In addition, it is important for organizations to understand the factors, feelings and experiences that could affect FSE's perspectives and performance to ensure that their attitude and behavior are conducive to deliver service quality.

The first concept, *perspective,* is operationalized following concepts of the Special Euro barometer 390 (European Commission, 2012) survey and has combined three themes, namely experiences, concerns and cyber security. Regarding this survey, the focus is on the experiences that FSE's have at work or at home with cybercrime. Apart from experiences, concerns over cybercrime could drive people to take precautions online or react in a different way to their customers when they are at work. The focus of cyber security is on how FSE's are prepared or informed by their organization about cybercrime.

The second concept, *performance,* is based on the coping literature. Coping is how FSE's respond when they confront with difficult or stressful events (cybercrime) during their work. There are a lot of ways to cope with stressful events. Finally, cybercrime might have influences on the service quality FSE's deliver towards customers.

Based on this conceptual scheme, the factors, feelings, experiences and how FSE's react to cybercrime, will be examined in this study.

2.6. Research questions:

Following from the above stated, the main research question is formulated: *How do Frontline Service Employees in the banking sector react to, the threat of, cybercrime?*

The sub-questions formulated to answer the main research question are the following:

1. Which experiences do Frontline Service Employees in the banking sector have with cybercrime?
2. To what extent are Frontline Service Employees concerned about cybercrime in the banking sector?
3. Which coping strategies do Frontline Service Employees use to cope with cybercrime?

3. Research design

3.1. Research Method

To gain more insight in FSE's perspective towards cybercrime and their performance at work dealing with cybercrime, semi-structured interviews were used as research method for this study.

The interview has started with the Critical Incident Technique [CIT] to let the participants tell what their experiences with cybercrime are. CIT is usually built in as part of a questionnaire or interview. Chill (1998, in: Gremler, 2004) provided the following description of the CIT method: "The critical incident technique is a qualitative interview procedure which facilitates the investigation of significant occurrences (events, incidents, processes, or issues) identified by the participant, the way they are managed, and the outcomes in terms of perceived effects. The objective is to gain understanding of the incident from the perspective of the individual, taking into account cognitive, affective, and behavioral elements". Critical incidents can be gathered in various ways. Due to the sensitive topic, which is related to job-related information and personal situation, the CIT method will be a good method to start with (Downs and Adrian, 2004). The approach generally asks participants to tell a story about an experience they have had, and in this context, their experience with cybercrime.

By using semi-structured interviews, the participants could optimally tell their experiences and the interviewer could adapt to unexpected or unforeseen answers (Baarda, Goede & Teunissen, 2009). Interviews give high-quality information that can be probed in detail in a face-to-face relationship with the employee. Face-to-face interaction during an interview enhances the information flow. It allows the researcher to be persuasive and questions can be asked that probe for more information (Downs and Adrian, 2001). Due to the semi-structured nature of the interview, information can be added, changed or adapted (Baarda et al., 2009).

3.1.1. Design of the interview

Each interview started with an explanation of the purpose of the study, after which the interview questions were asked. The interview consists of two concepts, *perspective* and *performance*. The first concept, perspective, combined several categories to gain more insight in what FSE's know about cybercrime and what their experiences are with cybercrime. The CIT method was used to gain more insight in the participants' experiences. Participants were asked to tell something about their experiences with cybercrime to find out what they know about cybercrime, and which types of cybercrime are most common. In addition, participants were also asked to give an overall picture.

The second concept performance focused on the resulting actions taken by FSE's. The resulting actions are the coping strategies FSE's use to cope with, the threat of, cybercrime. Participants were asked how they assess the situation the situation in the first place and how they cope with the situation. This was asked to examine which coping strategies FSE's use when they have to deal with cybercrime, and how they react towards their customers.

The interview was constructed based on relevant research literature (Whiting et al., 2011; Böhme et al., 2012; Lai et al., 2012), and consist of a wide range of questions. The interview guide can be found in appendix B.

3.2. Participants and sampling method

The subjects of this study were Frontline Service Employees [FSE's] who are working for several Dutch banks (i.e. Rabobank (n = 13, 52%); ABN Amro (n = 5, 20%); Regiobank (n = 4, 16%) and SNS bank (n = 3, 12%)). A total of 25 people, working for four different banks, participated in this study. Of the participants, 72% were women (n=18) and 28% were men (n=7). The participants ranged in age from 26 to 59 (mean = 40) years.

Participants were contacted in several ways. Firstly, participants were contacted via personal contacts. Some connections were made with family members and acquaintances working for the bank. These first connections were very valuable, because of their connections with FSE's. Secondly, a message was posted on social media. This yielded some connections with bank employees, who finally had participated in this study. The participants who participated were asked if they knew other employees who could participate.

Besides that, snowball sampling was used to come into contact with more participants. This sampling method was used, because the sample for the study is limited to a very small subgroup of the population. The snowball sampling method uses existing participants to ask if they know more employees, with a similar trait of interest, that would like to take part in the research (Downs et al., 2004; Noy, 2008).

The list of participants, including information on their age, sex, function of the participant and status, can be found in appendix C. Moreover, the names of the participants have been replaced with numbers to respect their anonymity.

3.3. Data collection procedure

The empirical data of this study was conducted in 14 weeks and consists of 25 interviews with Frontline Service Employees. The specific requirement for selecting participants for this study was that they were working as a Frontline Service Employee for a bank in the Netherlands.

Data contains both responses to face-to-face interviews as well as telephone interviews. 18 interviews were face-to-face. The interviews mostly took place in the work place of the participants. This location was chosen to ensure their comfort, to assure privacy and to stimulate free communication. The other seven interviews were telephone interviews.

The intended number of interviews to conduct was 30. Therefore a total of 30 people have been approached, by sending e-mails or via the snowball sampling method. With a non-response of five people, a total of 25 interviews were conducted for this study. Due to the sampling method, most participants who reacted were working for banks in the province Overijssel. The list of participants can be found in appendix C.

During the study there were no real ethical issues that influenced the study. The main ethical consideration taken into account was the need to be aware of the anonymity of the banks and their employees. Therefore, before the interview started, participants were asked to read and sign the informed consent form. This informed consent form explained the anonymity of their participation and that recording material would be kept confidential. In case of telephone interviews the conditions were mentioned in advance and the participant was asked to give permission for recording the interview on tape. Ensuring every person's privacy their names were replaced with numbers, and contact information was only noted in case more information was needed for clarification of their responses.

3.4. Data analysis methods

Data analysis started after the interview with the participant. By recording the interviews via a mobile phone, the transcriptions were done shortly after the interview took place. The transcriptions were analyzed using ATLAS.ti software. A codebook, with a set of codes and definitions, was used as a guide to help analyze the data (see appendix D). The codebook, with 135 codes, was constructed by creating free codes selected from the data, combining concepts form the literature (e.g. Whiting et al., 2011, on FSE's and coping; Böhme et al., 2012, on cybercrime, experiences and concerns; and Carver et al., 1989, on coping strategies and scales) and questions from the interviews with the FSE's. The codes were assigned to raw data, for making new connections between concepts (DeCuir-Gunby, Marshall and McCulloch, 2011).

The method used to establish reliability was Cohen's Kappa, by examining the similarities and differences for each code. Therefore, a second coder used the codebook to analyze one of the 25 interviews. Both worked independently of each other and applied the coding instructions to the set of data. The second coder has a Bachelor in Communication Science, and has experiences with this method. After coding, the codes that differed significantly were discussed to create more consensus.

The coding round resulted in a Kappa of 0.70, which signifies overall substantial coder agreement. A Cohen's Kappa of 0 would mean that the observed agreements are all based on chance and a Cohen's Kappa of 1 would mean that there is a full agreement on the observed agreements between the researcher and coder.

4. Results

This paragraph describes the results of the interviews, based on the conceptual schema on page 18.

4.1. Perspective

To gain more insight in the perspective of FSE's about cybercrime, participants were asked to define cybercrime. The majority of participants referred in their answers to the banking sector. In other words, the perception of cybercrime is primarily based on their function as FSE. Due to their function, their focus is on financial cybercrime, like phishing, skimming, spam and online fraud. Those examples of cybercrime were mostly used in their definitions, whereby phishing is the most common form, followed by skimming and fraud. Besides the focus on different forms of financial cybercrime, participants also focused on the use of Internet. For example, arranging things on the Internet (with or without permission) or attacks on the Internet and related services like online banking.

Participants' definitions were not very specific and some participants doubted whether their perception of cybercrime was correct. Notably, a few participants related cybercrime not only to the Internet, online banking or the bank itself, they referred in their definition to the banks' customers. *"In fact, all forms of misuse towards our customers" [participant 21].* These participants saw cybercrime as a form of online criminality, whereby criminals misuse confidential information of customers and their trust in online services of the bank.

Two participants acknowledge that they do not know how to define cybercrime. Talking about cybercrime, they both said, *"I don't know, but I think hacking of online banking" [participant 3].* As they further explained, *"Look, there are days that online banking can pose problems for our customers and then they contact the bank. Besides that, we don't have to deal with incidents that much" [participant 13].*

4.1.1. Participants' experiences

With exception of one participant, all participants had experiences with cybercrime at work. Participants' experiences were mainly based on different forms of cybercrime at work. Analysis shows that participants primarily had to deal with identity fraud, such as phishing and skimming. FSE's have to deal with these forms of cybercrime more often, because customers are more aware. In case of phishing, customers contacted the bank when they had received a phishing mail. At that moment, it was unclear whether the customer had become a victim of phishing. Most customers contacted the bank by way of precaution, to (1) inform the bank that phishing mails are circulating on the Internet, or (2) to check how they have to deal with, for example, phishing mails, *"Fortunately, nine out of ten phone calls are customers calling the* *bank out of precaution" [participant 14].* The participant explained, *"They haven't responded, but wanted to know why they received that mail and what they have to do with it" [participant 25].*

Experiences with phishing were not only based on situations during customer-contact. Employees themselves were also confronted with phishing at work. According to the experiences of four participants, *"Recently, I had someone on the phone who requested a new bankcard. The card wasn't for her, but she knew everything of that person" [participant 21].*

Beside phishing incidents, employees also dealt with skimming incidents at work. In case of skimming, customers contacted the bank when they noticed something suspicious at, for example an ATM or found out that they were skimmed. Skimming affects a large amount of people at the same time. *"They skimmed in reasonably large numbers at the same time. So, our bank and the other bank in this town both had 20 customers who had lost 1500 euros" [participant 5].* Furthermore, FSE's also dealt with online shopping fraud, like 'marktplaats' fraud. Participants argued that the number of online shopping fraud victims has increased, and even more customers contacted the bank when they became victim of online shopping fraud. Notably, none of the participants had experience with DDos attacks at work. They only could remember the DDos attacks on banks in April 2013.

4.1.2. Frequency

There is a difference in the extent to which FSE's are confronted with cybercrime. This has to do with the difference between notification and incident. For example, (1) there might be many customers calling about phishing on a particular day, but when it is only a notification the impact of the incident is low. Second, (2) it is also possible that a notification about cybercrime has a larger impact. When a lot of customers became victim at the same time or when the bank's system is unavailable due to a cyber attack, the impact is substantial and may influence the concerns of FSE's.

A small minority of the participants said that they had to deal with cybercrime daily. Almost every day someone contacted the bank about phishing mails. *"The notifications about phishing increased. Customers contact the bank almost daily" [participant 9].* Fortunately, it is not an everyday reality that customers become victims of cybercrime. Participants, who had contact with customers about cybercrime daily, attributed this to the increasing attention in the media. Because of the increasing media attention, people are much more alert and aware of the consequences of cybercrime.

About half of the participants indicated that they did not have to deal with cybercrime often. According to one of the participants, *"Yes, of course it happens a lot in the banking sector. But I don't have to deal with* *it very often" [participant 1].* These participants did not experience situations where people reacted on phishing mails, or that customers were involved.

In addition, it appeared that all FSE's of relatively small banks compared their bank with other banks in the Netherlands. They argued that their bank is not an interesting target for cyber criminals compared to the 'larger' banks.

4.1.3. Concerns

19 of the 25 participants were not concerned about the organization being victimized by cybercrime. The main reason why the FSE's do not have concerns is because they see it as a task and responsibility of the bank, as a total organization, and the banks' security department. According to these participants, *"Well, I think it isn't my responsibility, but the responsibility of the security department of the bank. Therefore, I have no concerns of becoming a cybercrime victim" [participant 24].* It is seen as the responsibility of the bank to inform customers correctly and protect them and the bank against cyber attacks. Participants, who pointed this out, were mainly working for the 'larger' banks in contrast to participants who work for smaller banks. The participants who are working for smaller banks had less concerns, because they argued being a less interesting target for cybercriminals due to the size of the bank and its customers.

In addition, a number of participants stated that they do not experience the threat of cybercrime at work, *"I never think about the consequences of cybercrime. I'm more focused on the customer and the impact it might have on the customer" [participant 18].* They said that they were more concerned about their customers who can become victims of cybercrime and that it is influencing the service quality towards customers.

About half of the participants, who did not have concerns, explained that they see it as the responsibility of the customers to protect themselves and confidential information against cybercriminals. They said that customers often blame the bank, or subsequently had no longer confidence in online banking. According to these participants, *"When something went wrong, it is often the fault of the customers themselves" [participant 17].*

The minority of participants indicated having concerns about cybercrime. Those participants were concerned because of the possibility that the bank may become a cybercrime victim, *"I think that the possibility of becoming a cybercrime victim has increased. I mean, the security will be better, but so will criminals and their criminal activities" [participant 11]*. Moreover, most participants did not know how and when a cyber attack occurred, because other departments, like the security department, took appropriate measures before the news had reached the employees.

Notably, a comparison is made by a number of participants to the west (of the Netherlands). These participants mentioned that online shopping fraud and skimming are more common in the west of the Netherlands, like Amsterdam. *”If you work for a bank in a big city or if your work in Amsterdam, there are more criminals compared to where I live. So in that case, I it’s more likely to become a cybercrime victim over there. However, it may be an incredible prejudice of mine. I don’t know, because you do not see where it comes from” [participant 23].*

Participants were also asked whether they were concerned of becoming a cybercrime victim themselves. Here again, the majority of participants said having no concerns. They indicated having no concerns, because they are more alert and more aware of the risks of cybercrime due to their work. *”Well, you might have a little bit more knowledge about the risk of cybercrime than an average person. So maybe I’m more aware of it” [participant 6].*

There is one participant who said to have concerns of becoming a cybercrime victim. According to this participant: *”After that moment […] I realized that it can happen, and that makes me more aware of the possibility” [participant 7].*

Moreover, the majority of participants said that they were more aware of the consequences, due to their experiences at work. They used their experiences to reduce the risk of becoming victims of cybercrime themselves. *”I believe that I’m more aware of the consequences of cybercrime. I always check the website whether it’s locked or not, what website it is and if I know the website” [respondent 19]*. It is noteworthy that 5 participants indicated to avoid online banking. They preferred the ’old’ form of banking. The main reason why they preferred the old way of banking is that they do not trust the Internet or the application for online banking. One other participant only used the Internet at work for online banking and two other participants stated that they do not use the application for online banking. Furthermore, about half of the participants avoid the Internet for online purchases. They prefer to buy their clothes or other products in the store.

4.1.4. Preventive

An important aspect of fighting cybercrime is the resilience of the bank. As mentioned before, the majority of participants argued that they see it as a task and responsibility of the bank to protect all data against cyber attacks. There is also a special security department, or ICT department, that monitors all systems 24/7. Besides this, the bank is also responsible to ensure awareness among customers is raised. The bank shared information on their website about cybercrime, employees provided information about security measures towards customers, and campaigns were developed by the government in cooperation with banks how to overcome or prevent cybercrime.

To provide information or react in certain situations, it is important that FSE's are well prepared. Therefore, FSE's were asked to what extent they are prepared and whether they are informed about the consequences of cybercrime.

Of all participants, there were 7 participants who indicated to be prepared. *"As an employee you know that there is a chance that a cyber attack can hit the organization'" [participant 9].* Otherwise, participants said that they talked about cybercrime incidents with colleagues or during work meetings. It often remained to the basic information which FSE's usually had. This means that they were made aware of the phishing mails circulating on the Internet and knew how to react towards customers. As an employee, you are able to prepare yourself by reading information about cybercrime and know all the protocols and instructions, which are available on intranet. Most employees were aware of this, but there were also a few employees who indicated never read those protocols or instructions before. In addition, they explained that they could talk with colleagues about their experiences.

The participants, who indicated to be prepared, were sufficiently informed about the consequences of cybercrime, *"Anyway, we all know something about cybercrime. However, I must say that cybercrime isn't something you have to deal with and read about every day. We are all informed, but when you don't read about it every day, you have to read the information again when it happens" [participant 8].* They indicated that they had the basic knowledge to help customers, and in case of emergency, they could read information on intranet.

However, the majority of participants argued not being prepared. The main reason they gave, *"Cybercrime is changing constantly and I also think that it's a race between the criminal and the bank; who's first. We are also confronted with something new every time" [participant 7].* A number of participants explained that knowledge about cybercrime incidents ensured that you know how to react. The more experience you have, the better you know how to respond and know how to deal in certain situations. Besides that, it is also a matter of doing to help the customers as good as possible. Two other participants explained not to be prepared, because cybercrime always happens unexpectedly, and you do not take into account that it can happen.

Participants, who indicated not being prepared, stated being sufficiently informed about the consequences of cybercrime by the bank. Although, there is a difference in which banks communicate with employees and how they are made aware of important subjects. The participants indicated that they could find general information about cybercrime and actual events on intranet. Otherwise, they heard about cybercrime incidents during work meetings or conversations with colleagues.

According to the majority of the participants, the bank sufficiently informed both employees and customers. Employees were informed when there were circulating phishing mails on the Internet. Besides that, employees had the opportunity to read all information about cybercrime and cybercrime incidents on intranet. Customers were made aware of cybercrime via campaigns and information is given on the websites of the banks. However, a number of participants indicated that the bank should provide more information, so that they have more knowledge and are able to tell the customers what happened. There was one participant who indicated that the bank could solved this, by providing more examples or case studies about real cybercrime incidents, *"Give us an example about a specific situation and share it on the intranet; the situation, the consequences and how it can be solved. I think that we don't hear everything, about what is happening. So, I don't think that it is wrong to share some examples or cases. You can always learn from it" [participant 8]*

In addition, there were some participants who indicated that specific knowledge about cybercrime is not necessary. One participant noted that it is not good to warn both employees and customers about the consequences of cybercrime. This participant argued that people could become more anxious and that they might stay away of the bank.

However, there were also a number of participants who indicated not to be sufficiently informed about cybercrime. They had several reasons. There was one participant who said, *"Well, I think that we dissociate us from cybercrime and the consequences. You don't want to know what could happen. You don't think that it can happen, but when it does" [participant 12].* Another participant was shocked after she attended a meeting organized by the bank about safe banking; here she found out that she did not know that much about cybercrime as she thought before.

In addition, there were two participants who said they wanted to be more informed about the consequences of cybercrime, so they become more aware of incidents. They primarily wanted more additional information, because they indicated to know how they have to react when customers contacted the bank.

4.2. Performance

4.2.1. Coping strategies

When people are confronted with problematic circumstances, people make two types of evaluations. First, people appraise the situation, whereby the person is evaluating the significance of the threatening event. Based on their experiences, participants were asked how they appraise the situation in case of cybercrime.

In the first place, participants said that it was important to identify the person who contacted the bank, and why the person contacted the bank. Secondly, to find out more about the situation, FSE's had to take the problem seriously. *"I immediately ask the customer if they have clicked on something or gave their personal data" [participant 25].* From this information stem two things: (1) the customer contacted the bank by way of precaution, or (2) the customer became a cybercrime victim. The severity of the situation influences the coping behavior of the employees.

Subsequently, after collecting information about the customer, employees took several steps to control the stressor. The employee made an assessment of the best solution. Participants described the strategies they used to cope with the situation and how they reacted to their customers. In case of phishing, when people contacted the bank as a precaution measure, then all employees react *active*. They indicated what the customer should do. FSE's gave information about which preventive measures the customer should take. This information is primarily related towards the behavior and awareness of the customer. Participants stated, *"I think, everyone has their own responsibility in this. A lot of people don't realize that when they publish something in public or accidentally save it on their browser, criminals can misuse their confidential data. However, there are also people who lend their bank card with pin code and then they are surprised that somebody stole their money" [participant 16].* Most FSE's said that customers are often naive when it comes to cybercrime and most of the time not very smart. Afterwards, customers were told to send the phishing mail to the security department for further research.

On the other hand, FSE's reacted differently when they found out that the customer became victim of cybercrime. Beside their different reactions, they also used different coping strategies to cope with the situation. In the first place, about half of the participants used problem-focused strategies. Also here, they reacted *active.* According to these participants, *"take decisive actions, find out more about the situation, which cards were used, what do we have to block […]" [participant 7].* In addition, there were also some participants who sought *social support*. The participants were all looking for instrumental support, whereby they asked the security department or colleagues for assistance or help. In most cases, customers were forwarded to the security department where the incident was further investigated. At that moment, the FSE has completed the notification.

Moreover, the other half of the participants reacted in this case both problem- and emotion-focused. They also addressed the problem *actively* and sought instrumental *social support* by contacting the security department or colleagues for assistance. A few participants used *accepting* to cope with the situation. These participants indicated, *"At a certain point, we can't do anything else about the situation as a bank" [participant 17].* Beside using an active approach, seeking instrumental support and accepting the situation, there were also four participants whereby *emotion* plays a significant role in coping with the situation. The incident primarily leads to frustration by these participants.

Notably, these emotions were different than the emotions in the reactions towards customers. According to all participants, it was important to ensure that you could reassure customers during the contact. Most customers panicked due to the situation. When customers panicked, it was important for the FSE to remain calm and reassure the customer. So, that they were able to do what they had to do in that situation. FSE's did not deny the problem. They all see it as their job to help the customer as good as possible.

The majority of the participants indicated experiencing no stress when customers called and it appears that they became victim of cybercrime. This is due to several reasons. A number of participants indicated that they did not get stressed because they saw it primarily as their work. It is their task to help the customer. In addition, according to the majority of the participants, experience played an important role to deal with the situation. One participant noted, *"Due to the number of incidents, you know how to communicate with your customers. These are very unpleasant conversations. However, it remains the responsibility of the person himself" [participant 13].* As other participants further explained, *"Each situation is different. You use your experience to deal with the situation" [participant 17].*

Only three participants indicated experiencing stress, *"Obviously it is stress. At that moment, you have to take it over from the customer" [participant 2].* To solve the problem as soon as possible for the customers, these employees explained that they did not allow emotions and addressed the problem actively in accordance with protocols. The participants, who indicated that they were really stressed, also contacted the security department for instrumental social support. Furthermore, emotions played a significant role in addressing the stressor. According to this participant, *"My heart is beating faster and I am getting nervous […] I have to check everything. It is all right when nothing has happened, but when it does, then I get really sweaty" [participant 25].*

4.3. Outcomes

Lastly, employees were asked about the impact of, the threat of, cybercrime. About half of the participants indicated that cybercrime affected the workload. According to the participants, *"You have a really busy day, when you have to deal with phishing […] you have to do many action under time pressure. So in that case, I experience stress at work" [participant 17].* In case of emergency, a few participants experienced time pressure. At that moment, they need and have to react as fast as possible, which increases the workload.

Another outcome of, the threat of, cybercrime is that customers became anxious. Therefore, they were less confident or had a more negative feeling towards the bank. As a result, employees had to deal with angry customers and with customers who were in panic more often.

Employees tried to solve this as good as possible by ensuring that the service quality remained high. FSE's noticed that customers' expectations became higher. In addition, customers asked more question about the reliability of online banking. Customers called the bank more often to inform about cyber security or became suspicious when the banks' website or online banking was unavailable for several hours. Participants indicated that customers were helped as good as possible, because the service quality may not deteriorate despite the fact that there is always a possibility that the customer become a victim of cybercrime. *"When something happens, you have to provide assurance. We have to take care for that" [participant 15].*

5. Conclusions and discussion

This study explored the reactions of Frontline Service Employees [FSE's] towards the threat of cybercrime, by focusing on the relationship between experiences and concerns, and the resulting actions. The empirical findings of this study, which were presented in the previous section, were conducted through 25 interviews with Frontline Service Employees in the banking sector. The central question of this study was; *how do FSE's in the banking sector react to, the threat of, cybercrime?*

How FSE's react to the threat of cybercrime is affected by their experiences, factors and feelings they have towards cybercrime. This study shows that FSE's in general have little knowledge about, the consequences, of cybercrime. FSE's experiences with cybercrime ensure that they, in case of incidents or during customer contact, can provide customers with basic information. Besides their experiences, FSE's use problem-focused coping strategies to cope with, the threat of, cybercrime. They try to find out more about the situation and concentrate on the next step in helping the customer, as soon and as good as possible.

However, FSE's do not see it as their responsibility to solve cybercrime. They see it primarily as the task and the responsibility of the security department that data and systems are as secure as possible, and customers are informed correctly. In addition, FSE's believe customers have a great responsibility to protect themselves against cyber attacks.

The responsibility of cyber security to protect the organization and its customers primarily rests with the banks' security department. However, all employees have an important role in effectively implementing their organizations' cyber security plan. With their limited knowledge, FSE's react to, the threat of, cybercrime according to their function; they are able to help customers by providing basic information and therefore, help customers as good as possible. This is important to keep the customers satisfied and to ensure that the service quality remains high.

In the following section, the findings of the empirical chapters will be summarized in order to answer each sub-question and thereby explaining the above stated. The conclusions will be discussed in line with the theory and academic literature from the theoretical framework. In section 5.2 some theoretical and practical implications will be discussed and conclusively, in section 5.3 recommendations will be given.

5.1. Answering sub-questions

Regarding sub-question one, the experiences of FSE's with cybercrime indicates that they mainly have to deal with forms of financial cybercrime, such as phishing, skimming and online shopping fraud. Phishing generally focuses on the customers as well as skimming and online shopping fraud. FSE's have to deal with these forms of cybercrime more often, because customers are more aware and contact the bank when they noticed something suspicious. Once customers contact the bank, the FSE's have to provide the customer with information. FSE's are for the first contact with private customers, and their personal interactions are at the front of most services in firm activities (Jackson et al., 2009). The experiences of FSE's with cybercrime can be divided into two categories. In the first place, (1) experiences where the customer contacts the bank as way of precaution. They inform the bank about phishing mails circulating on the Internet, or (2) to check what they have to do (e.g. in case of phishing).

Banks consider, beside phishing and skimming, also malware and DDos attacks as forms of cybercrime in which banks are at high risk (Arachchilage et al., 2014; Stokkel et al., 2013; NCSC, 2013). Banks are often hit by DDos attacks, but firewalls of banking systems prevent these attacks most of the time. Due to taken measures by the banks, customers are unaffected and FSE's hardly have to deal with these forms of cybercrime. Probably, because of this, both forms of cybercrime were not described in the definitions or experiences of the FSE's.

Sub-question two focused on the concerns which FSE's possibly have with becoming a victim of cybercrime, or that the bank could become a victim. Paulin et al. (2006) showed that FSE's are simultaneously concerned with their own and their customers' well being. In this study, FSE's indicate to have more concerns about customers becoming a victim of cybercrime, than about the bank being hit by a cyber attack. Therefore, they have no concerns that the bank or themselves become victim of cybercrime. Furthermore, FSE's indicated that the bank provides both customers and employees with information about cybercrime.

FSE's have the knowledge to inform customers with basic information. They inform customers about steps the customer should take to delete phishing mails, or which preventive measures the customers should take. In case of cybercrime, the role of the FSE is mostly limited to provide the customer with basic information. They have no background knowledge about cybercrime and believe that it is, due to their function, unnecessary. They believe that it is the responsibility and task of the banks to secure all data against cyber attacks, as well as providing information to customers about cybercrime and its consequences.

In addition, most FSE's hold the customers responsible for becoming a victim of cybercrime. The customers have, although they give it under false pretenses, revealed their own bank details. According to the NCSC (2013) the end-user often lacks the technical knowledge required to apply the security measures. Moreover, the end-user is responsible for basic safety measures, such as updating their software, using safe passwords and anti-virus software on their computers.

An important fact is that all employees within the organization must be aware of cybercrime dangers and to take appropriate measures to reduce the risk of cybercrime (Finau et al., 2013). An organization's cyber security strategy requires all employees to be trained in cyber security measures and be able to identify cyber security threats as early as possible (Finau et al., 2013; NCSC, 2013). However, not all employees indicate to be prepared or informed about the consequences of cybercrime. The majority of FSE's indicate that it is not possible to prepare for cyber attacks. Cyber attacks are almost always unexpected and take on different forms rapidly. Due to this, most FSE's do not take account of that they can be confronted with a cyber attack at their work.

Looking at sub-question three, FSE's use primarily problem-focused coping strategies to cope with cybercrime incidents at work. This has to do with one's interpretations and explanation of that event (Kassin et al., 2008; Whiting et al., 2011). The coping strategy, that an individual FSE use, depends on the incident that occurs. Just as the experiences, the coping strategies can be divided into two categories. (1) When the employee has to deal with customers who called the bank out of precaution, they address the problem actively. This is a form of problem-focused coping whereby, in this case, the employee verifies all data of the customer, let the customer sent the mail to the security department and provide the customer with information about cyber security. The FSE's also often use problem-focused coping strategies, when (2) they found out that the customer has become a victim. In the first place, the employees address the problem actively. They try to find out more about the situation and are concentrating on the next step. Secondly, they seek social support with their colleagues or the security department to solve the problem together.

FSE's do not use emotion-focused coping strategies often. They try not to show their emotions and handle as quickly as possible, because they want to solve the problem as soon as possible for the customer. As noted earlier, FSE's are simultaneously concerned with their own and the customers' well being. This is reflected in their responses to the customers. While they do not allow showing their emotions while solving the problem, they do anticipate on the emotions of the customer. They feel sorry for the customer, and try to reassure them by showing their empathy. They let the customers tell what has happened and give the customer confidence that it will be solved.

FSE's primarily used a problem-focused strategy because people facing a problem as a challenge seem to take a problem-oriented coping behavior and treat the problem as a thing that can be controlled (Whiting et al., 2011; Kassin et al., 2008; Yavas et al., 2011). They are in control when they address the problem actively and, in most cases, solve it together with the security department.

5.2. Discussion

This study contributes to gain more insight into the impact of cybercrime in the banking sector. Combating cybercrime is a global priority, organizations and governments committed to prevent cybercrime. Where previous studies mainly focus on the consequences of cybercrime in the banking sector and how customers react to cybercrime, this study focuses on an important group of employees in the banking sector. Frontline Service Employees [FSE's] are important for the contact with customers, and have a major influence on how customers perceive of the bank. Both customers and the bank can become a cybercrime victim. The bank has several preventive measures, to minimize the risk of becoming a cybercrime victim and to create awareness among customers. When a customer has become a victim, or the bank is hit by a cyber attack, it is primarily the task of FSE's to reassure customers by providing service quality.

This study aims to understand more about the conception FSE's have towards cybercrime, how FSE's experience cybercrime at work and how they deal with it. Linking these topics has created a new study within the cybercrime discipline. It is important to understand the factors, feelings and experiences that affect FSE's perspectives and performance to ensure that their attitude and behavior are conductive to deliver service quality. This study enhances the understanding of employees' perspectives of delivering service quality, and where it can be improved in situations with cybercrime.

In addition, it is relatively new that coping is used as a method to examine how individuals respond to ICT threats. This study shows that it is possible to use coping deal with technology threats. Where coping is mainly supported from other academic disciplines like psychology, health care, organizational behavior and consumer research (Whithing et al., 2011), it is relatively new in the field of ICT, with the exception of some recent studies (e.g. Lai et al., 2012).

5.3. Limitations

The first point of limitation is the number of participants who participated in this study. Due to some participants who had canceled the appointment, there were fewer participants who had participated than the 30 that were initially expected. Due to the fact that it is a very specific group of people, there was ultimately decided to keep it with the 25 interviews.

A second limitation is due to the selection of the participants, which was done via snowball sampling. Therefore, the data of the participants does not necessarily reflect the larger population of Frontline Service Employees who are working for Dutch banks. Notably, most participants were working as FSE by banks in the province “Overijssel”.

Third, in this study the background variables of employees were omitted, because the focus was on how employees generally responded to cybercrime. It is important to understand why employees responded this way. Other employees, with less or more experiences, could use very different strategies to cope with cybercrime. In addition, men could respond different than women, or other (environmental) stressors could ensure that employees reacted differently.

5.4. Recommendations

Based on the conclusions that have been written in the previous section, and based on the needs of the participants who participated in this study, it is possible to formulate a number of recommendations.

A recurring subject during this study is awareness among employees. This study has shown that FSE’s underestimate, the threat of, cybercrime. Most employees did not experience cyber attacks or forms of cybercrime with a major impact at work or in their private life. Therefore, it is important to establish more awareness among these employees about the consequences of cybercrime. FSE’s are mainly informed via intranet, or hear during work meetings about phishing mails. In order to be aware of the possible consequences, banks should provide courses for these employees. According to this study, participants who had followed a course about online banking were startled about the consequences of cybercrime that may occur. However, they could use the acquired knowledge to inform customers about the most important consequences.

In addition, employees have more background knowledge and are more aware of their role within the organization to prevent the organization and its customers for possible cyber attacks. It increases the knowledge of employees. These courses could also be online. Employees indicated that they had no experiences with major cyber attacks or do not know what is happening on the background. Therefore the bank could choose to establish online cases to train the employees, with several examples.

References

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3), 706 - 714.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior,* 38, 304-312.

Baarda, D.B., Goede, M.P.M. de & Teunissen, J. (2009). *Basisboek Kwalitatief Onderzoek. Handleiding voor het opzetten en uitvoeren van kwalitatief onderzoek.* Nederland, Groningen/Houten: Noordhoff Uitgevers bv.

Bhasin, M. (2007). Mitigating cyber threats to banking industry. *The chartered accountant*, 55(10), 1618 - 1624

Böhme, R. & Moore, T. (2012). How do consumers react to cybercrime? *eCrime researchers summit (eCrime), IEEE,* 1 – 12

Carver, C.S. & Scheier, M.F. (1989). Assessing Coping Strategies: A Theoretically Based Approach. *Journal of Personality and Social Psychology,* 56(2), 267 – 283

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719-731.

Coelho, F., Augusto, M., & Lages, L.F. (2011). Contextual factor and the creativity of frontline service employees: The mediating effects of role stress and intrinsic motivation. *Journal of Retailing,* 87(1), 31 – 45.

Coombs, W. T. (2006). The protective powers of crisis response strategies: Managing reputational assets during a crisis. *Journal of Promotion Management*, 12(3-4), 241-260.

Coombs, W.T. (2007). *Crisis Management and Communications.* Retrieved 1 March 2015 from http://www.facoltaspes.unimi.it/files/_ITA_/COM/Crisis_Management_and_Communications.pdf

DeCuir-Gunby, J.T., Marshall, P.L. & McCulloch, A. (2011). Developing and using a codebook for the analysis of interview data: an example from a professional development research project. *Field Methods,* 23(2), 136 – 155.

Di Mascio, R. (2010). The service models of frontline employees. *Journal of Marketing*, 74(4), 63-80.

Downs, C.W. & Adrian, A.D. (2004). *Assessing organizational communication.* The Guildford press; New York

Elmadag, A.B., Ellinger, A.E. & Franke, G.R. (2008). Antecedents and consequences of frontline service employees commitment to service quality. *Journal of Marketing Theory and Practice,* 16(2), 95 – 110

European Commission (2012). *Special Eurobarometer 390 Cyber Security*. Retrieved 9 December 2013 from http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

Finau, G., Samuwai, J. & Prasad, A. (2013). Cybercrime and its implications to the pacific. *The Accountant: The journal of the Fiji Institute of Accountants,*

Gremler, D.D. (2004). The critical incident technique in service research. *Journal of Service Research*, 7(1), 65 – 89.

Hunton, P. (2009). The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model. *Computer Law & Security Review,* 25(6), 528 - 535.

Jackson, D.W. & Sirianni, N.J. (2009). Building the bottom line by developing the frontline: career development for service employees. *Business Horizons*, 52, 279 – 287

Jang, Y.J. & Lim, B.Y. (2012). Harmonization among National Cyber Security and Cybercrime Response Organizations: New Challenges of Cybercrime.

Joode, A. de. (2011). Effective corporate security and cybercrime. *Network Security*, 2011(9), 16 - 18.

Kassin. S., Fein, S. & Markus, H.Z. (2008). *Social psychology.* Boston, New York; Houghton Mifflin Company.

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80(3), 541 - 555.

Kshetri, N. (2013). Reliability, Validity, Comparability and Practical utility of cybercrime-related data, metrics and information. *Information*, 4, 117 – 123.

Lagazio, M., Sherif, N. & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security,* 1 - 32.

Lai, F., Li, D. & Hsieh, C. (2012), Fighting identity theft: The coping perspective. *Decision Support Systems*, 52, 353 – 363.

Leukfeldt, R., Veenstra, S. & Stol, W. (2013). High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, 7(1), 1 – 17.

Liang, H. & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly*, 33(1), 71 – 90.

Malhotra, N., Mavondono, F., Mukherjee, A. & Hooley, G. (2013). Service quality of frontline employees: a profile deviation analysis. *Journal of Business Research*, 66, 1338 – 1344.

Manzoor, A. (2014). Protecting Customers Online: Response from Pakistani Banks. *International Journal of Science and Applied Information Technology*, 3(1), 1 – 7

Martin, N. & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, 30, 803 – 814.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. & Giannakopoulos, G. (2014). The human factor of information security: unintentional damage perspective. *Procedia - Social and Behavioral Sciences,* 147, 424 – 428.

Miller, K. (2009). *Organizational Communication; Approaches and Processes.* Wadsworth Cengage Learning; Boston.

Nationaal Cyber Security Centrum [NCSC] (2013a). *Cybersecuritybeeld Nederland.* Nationaal Cyber Security Centrum: Den Haag.

Nationaal Cyber Security Centrum [NCSC] (2013b). Cyber Security Assessment Netherlands. National Cyber Security Centre: The Hague.

Nationaal Cyber Security Centrum [NCSC] (2014). *Cybersecuritybeeld Nederland.* Nationaal Cyber Security Centrum: Den Haag.

Noy, C. (2008). Sampling knowledge: The hermeneutics of snowball sampling in qualitative research.

International Journal of social research methodology, *11*(4), 327 – 344.

Paulin, M., Ferguson, R.J. & Bergeron, J. (2006). Service climate and organizational commitment: the importance of customer linkages. *Journal of Business Research*, 59, 906 – 915.

Saini, H., Rao, Y.S. & Panda, T.C. (2012). Cyber-Crimes and their impacts: a review. *International Journal of Engineering Research*, 2(2), 202 – 209.

Singh, J. (2010). Performance productivity and quality of frontline employees in service organizations. *Journal of Marketing*, 64, 15 – 34.

Stokkel, M. & Smulders, A. (2013). Cybersecurity: hoe wordt het behapbaar? *Keynotes,* 42 – 26.

Wada, F. & Odulaja, G.O. (2012). Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories. *African Journal of Computing & ICT*, 5(1), 69-82.

Welbourne, J.L., Eggerth, D., Hartley, T.A., Andrew, M.E. & Sanchez, F. (2007). Coping strategies in the workplace: relationships with attributional style and job satisfaction. *Journal of Vocational Behavior*, 70, 312 – 325.

Whiting, A., Donthu, N. & Baker, A.M. (2011). Investigating the immediate and long-term effects of job stressors on frontline service employees. *Journal of Research in Marketing*, 28, 319 – 331.

Yavas, U., Biglin, Z. & Shemwell, D.J. (1997). Service quality in the banking sector in an emerging economy: a consumer survey. *International Journal of Bank Marketing*, 15(6), 217 – 223.

Yavas. U. & Babakus, E. (2011). Job Demands, Resources, Burnout, and Coping Mechanism Relationships. *Services Marketing Quarterly*, 32(3), 199 – 209.

Verma, M., Hussain, S.A. & Kuswah, S.S. (2012). Cyber Law: Approach To Prevent Cyber Crime. *IJRREST: International Journal of Research Review in Engineering Science and Technology,* 1(3), 123 – 129.

Appendix A: operationalization

Table 4: categories, operationalization and indicators of the interview

Concept	Categories	Operationalization	Indicators
Perspective	Experiences with cybercrime	On the basis of the CIT method and a question of the Eurobarometer survey, participants were asked to give a definition of cybercrime. Secondly, they were asked if they could tell their experiences with cybercrime in their private life or at work.	- Wat verstaat u onder cybercrime? - Als we het hebben cybercrime, kunt u dan uw ervaring met cybercrime omschrijven?
	Concerns about cybercrime	Another part of the indicator perspective is if the respondents have concerns about cybercrime. Apart from experience, concern over cybercrime could drive people to take precautions online or react in a different way to their customers when they are at work.	- In hoeverre maakt u zich zorgen dat u zelf (opnieuw) slachtoffer wordt van cybercrime? - In hoeverre maakt u zich zorgen dat uw bank (opnieuw) slachtoffer wordt van cybercrime?
	Cyber Security	Cyber security is the first category of this indicator performance. This are the preventive measures banks take towards their organization and their customers.	- Vindt u dat u voldoende bent geïnformeerd over de gevolgen van cybercrime? - Wat zou u willen dat uw organisatie (extra) doet om cybercrime tegen te gaan? - In hoeverre bent u voorbereid op dit soort situaties?
Performance	Coping strategies	Following on the experiences with cybercrime, we are interested in how people respond when they confront with difficult or stressful events during their work. There are lots of ways to try to deal with stress. This interview asks the respondent what they generally do and feel, when they experience stressful events. Different events bring out somewhat different responses.	-Hoe beoordeelde u, in eerste instantie, de situatie? -Kunt u omschrijven welke acties u ondernam om met de situatie om te gaan? -Ervaart u stress op de werkvloer? -Heeft cybercrime, of de dreiging van, hier invloed op/zou kunnen hebben? -En als er een cyberaanval plaats zou vinden, zou u dan meer stress ervaren?
	Outcomes	Focusing on quality service. Changed any behaviors as a causal consequence from concern over cybercrime.	- Wat zijn de gevolgen voor privé / werk?

Appendix B: interview guideline

Interview: Cybercrime and the influence on bank FSE's

Dit interview wordt gehouden onder service medewerkers die werkzaam zijn bij verschillende banken in Nederland. In dit interview zal de (mogelijke) invloed van cybercrime op deze medewerkers worden onderzocht. Het interview bestaat uit 3 onderdelen; ervaringen, zorgen en acties.

Vraag 1: Wat verstaat u onder cybercrime?

Cybercrime spreekt vaak tot de verbeelding van personen, waardoor iedereen een eigen beeld heeft van cybercrime.

Definitie: Alle vormen van criminaliteit waarbij ICT een wezenlijke rol speelt / Vorm van criminaliteit waarbij een ICT-systeem of de informatie die daardoor wordt verwerkt, het doelwit is.
Voorbeelden van cybercrime: hacking, phishing, d-Dos aanval (platleggen van systemen etc).

Vraag 2: Als we het hebben over cybercrime, kunt u dan uw ervaring met cybercrime omschrijven?
Medewerker zijn of haar ervaring met cybercrime laten vertellen.
2a: Privé
2b: Werk

Heeft u in de afgelopen maanden iets gezien of gehoord over cybercrime in uw directe omgeving?
Heeft u in de afgelopen 12 maanden cybercrime ervaren of bent u slachtoffer geweest?

Vraag 3: Kunt u iets vertellen over de cyberaanval waar uw bank mee te maken heeft gehad?
Vraag 3b: Kunt u iets vertellen over de cyberaanval waar u te maken mee heeft gehad?

Vraag 4: Hoe beoordeelde u, in eerste instantie, de situatie?
Hoe kwam u erachter dat er sprake was van een cyberaanval?

Vraag 5: Kunt u omschrijven welke acties u ondernam om met de situatie om te gaan?
Hoe reageerde u in deze situatie naar uw klanten?
Hoe reageerde u in deze situatie?

Vraag 6: In hoeverre bent u voorbereid op dit soort situaties?
In hoeverre hebben jullie instructies gehad? Voorbereid: oefening gehad? Protocol?

Wat zijn de richtlijnen?

Vraag 7: Wat zijn de gevolgen voor privé / werk?

Heeft de manier waarop u omgaat met dit 'probleem' invloed op uw functioneren?

Uit onderzoek blijkt dat mensen met een zogenoemde frontline functie, meer stress ervaren op de werkvloer. Dit heeft met verschillende factoren te maken.

Vraag 8a: Ervaart u stress op de werkvloer?

Vraag 8b: Heeft cybercrime, of de dreiging van, hier invloed op/zou kunnen hebben? En als er een cyberaanval plaats zou vinden, zou u dan meer stress ervaren?

Vraag 9a: In hoeverre maakt u zich zorgen dat u zelf (opnieuw) slachtoffer wordt van cybercrime?

Waarom maakt u zich wel zorgen?

Waarom maakt u zich geen zorgen?

Meegemaakt: meer of minder zorgen?

Uit onderzoek blijkt dat het bankwezen steeds vaker getroffen wordt door cyberaanvallen. In de afgelopen jaren zijn er verschillende aanvallen geweest op diverse onderdelen van digitaal bankieren. Deze aanvallen betroffen zowel het stelen van geld als het uitschakelen van online betalingssystemen, zoals internetbankieren via websites, mobile apps en iDeal. Uit eerder onderzoek van MKB-Nederland blijkt dat 60 procent van de ondernemers zich zorgen maakt over de beveiliging van hun systemen tegen cybercrime.

Vraag 9b: In hoeverre maakt u zich zorgen dat uw bank (opnieuw) slachtoffer wordt van cybercrime?

Waarom maakt u zich wel zorgen?

Waarom maakt u zich geen zorgen?

Meegemaakt: meer of minder zorgen?

Vraag 10: Vindt u dat u voldoende bent geïnformeerd over de gevolgen van cybercrime?

Vraag 11: Wat zou u willen dat uw organisatie (extra) doet om cybercrime tegen te gaan?

Appendix C: list of participants

Table 6: List of participants

n	Function	Gender	Age	Status
1	Adviseur Particuliere Relaties	v	59	Conducted in person 28/03/2014
2	Adviseur Particuliere Relaties	v	36	Conducted in person 28/03/2014
3	Adviseur	v	48	Conducted in person 09/04/2014
4	Adviseur	m	52	Conducted in person 16/04/2014
5	Adviseur	m	55	Conducted in person 23/04/2014
6	Advies en Service Center	v	26	Conducted by phone 24/04/2014
7	Coördinator Verkoop & Service Adviseur	m	44	Conducted in person 24/04/2014
8	Bankhal	v	28	Conducted in person 24/04/2014
9	Bankhal	v	38	Conducted in person 24/04/2014
10	Klantenservice medewerker - VSA B	v	38	Conducted in person 24/04/2014
11	Klantenservice medewerker - VSA B	v	41	Conducted in person 24/04/2014
12	Verkoop en Service Adviseur Particulieren	v	51	Conducted in person 06/05/2014
13	Adviseur Particuliere Relaties	v	53	Conducted in person 07/05/2014
14	Advies en Service Center	m	28	Conducted by phone 08/05/2014
15	Adviseur	m	48	Conducted in person 16/05/2014
16	Medewerker Klantenservice	m	27	Conducted by phone 26/05/2014
17	Verkoop en Service Adviseur Particulieren	v	32	Conducted by phone 19/06/2014
18	Klant Contact Center	v	44	Conducted in person 23/06/2014
19	Klant Contact Center	v	42	Conducted in person 23/06/2014
20	Klant Contact Center	v	40	Conducted in person 23/06/2014
21	Klant Contact Center	v	45	Conducted in person 23/06/2014
22	Klant Contact Center	v	46	Conducted in person 23/06/2014
23	Verkoop en Service Adviseur Particulieren	v	30	Conducted by phone 25/06/2014
24	Medewerker Klantenservice	m	28	Conducted by phone 03/07/2014
25	Medewerker Klantenservice	v	27	Conducted by phone 04/07/2014
26	Klant Contact Center	v	32	No response
27	Klantenservice medewerker - VSA B	v	55	No response
28	Medewerker Klantenservice	m	28	No response
29	Medewerker Klantenservice	m	26	No response
30	Medewerker Klantenservice	v	26	No response

Appendix D: Codebook

1. Defintie cybercrime: Wat verstaat u onder cybercrime?

Code	Naam	Definitie
1.1.	CYBERCRIME_DEFINITIE	De persoon omschrijft in eigen woorden wat hij of zij onder cybercrime verstaat
1.1.1.	CYBERCRIME_INTERNET	De persoon geeft aan dat cybercrime te maken heeft met het internet. Bijvoorbeeld een aanval of strafbare dingen doen
1.1.2.	CYBERCRIME_SOORTEN	De persoon legt aan de hand van voorbeelden uit wat cybercrime is
1.1.3	CYBERCRIME_GEGEVENS	De persoon geeft aan dat cybercrime voornamelijk gaat om het stelen van gegevens/geld
1.1.4.	CYBERCRIME_PERSOON	De persoon legt voornamelijk de nadruk op de crimineel om cybercrime te verwoorden
1.1.5.	CYBERCRIME_INTERNETBANKIEREN	De persoon geeft aan dat cybercrime te maken heeft met internetbankieren
1.1.6.	CYBERCRIME_BANK	De persoon geeft aan dat cybercrime te maken heeft met het inbreken bij een bank
1.1.7.	CYBERCRIME_PC	De persoon geeft aan dat cybercrime te maken heeft met verschillende aanvallen op computers
1.1.8.	CYBERCRIME_KLANT	De persoon legt de nadruk op de klanten die slachtoffer worden als het gaat om cybercrime.
1.2.	CYBERCRIME_GEEN_IDEE	De persoon geeft aan dat hij of zij niet weet wat onder cybercrime wordt verstaan

2. Ervaring met cybercrime: Kunt u uw ervaring met cybercrime omschrijven

Code	Naam	Definitie
2.1.	ERVARING_PRIVE	Persoon omschrijft een privé ervaring die hij of zij heeft gehad met cybercrime
2.1.1.	ERVARING_PRIVE_PHISHING	Persoon geeft aan privé wel eens phishing mails te hebben ontvangen, of via de telefoon te zijn benaderd/(poging tot)opgelicht
2.1.2.	ERVARING_PRIVE_SKIMMING	Persoon geeft aan privé wel eens geskimmt te zijn
2.1.3.	ERVARING_PRIVE_DDOS	Persoon geeft aan wel eens te maken heeft gehad met een dDos-aanval op een website, waardoor het niet mogelijk was in te loggen
2.1.4.	ERVARING_PRIVE_HACKING	Persoon geeft aan wel eens te zijn gehackt
2.2.	ERVARING_WERK	Persoon omschrijft een ervaring met cybercrime die hij of zij op het werk heeft gehad
2.2.1.	ERVARING_WERK_PHISHING	Persoon geeft aan dat hij of zij op het werk te maken heeft gehad met phishing
2.2.2.	ERVARING_WERK_SKIMMING	Persoon geeft aan dat hij of zij op het werk te maken heeft gehad met skimming

2.2.3.	ERVARING_WERK_FRAUDE	Persoon geeft aan dat hij of zij op het werk te maken heeft gehad met fraude (overboekingen en marktplaatsfraude)
2.2.4.	ERVARING_WERK_DDOS	Persoon geeft aan dat hij of zij op het werk te maken heeft gehad met een dDos-aanval, waardoor het systeem van de bank eruit lag
2.2.5.	ERVARING_WERK_OVERIG	Persoon geeft aan dat hij of zij op het werk te maken heeft gehad met een vorm van cybercrime (die nog niet eerder genoemd is)
2.3.	ERVARING_PRIVE_GEEN	Persoon heeft geen privé ervaring met cybercrime
2.4.	ERVARING_WERK_GEEN	Persoon heeft op het werk nog nooit met cybercrime te maken gehad

3. Hoe vaak heeft de persoon te maken met cybercrime (werk/privé)?

Code	Naam	Definitie
3.1.	CYBERCRIME_FREQUENTIE_WERK	De persoon geeft aan hoe vaak hij of zij op het werk te maken heeft met cybercrime
3.1.1.	CYBERCRIME_DAGELIJKS_WERK	De persoon geeft aan dat hij of zij op het werk dagelijks te maken heeft met cybercrime
3.1.2.	CYBERCRIME_PERIODIEK_WERK	De persoon geeft aan dat hij of zij op het werk periodiek te maken heeft met cybercrime
3.1.3.	CYBERCRIME_REGELMATIG_WERK	De persoon geeft aan dat hij of zij op het werk regelmatig te maken heeft met cybercrime
3.1.4.	CYBERCRIME_NIET_VAAK_WERK	De persoon geeft aan dat hij of zij op het werk bijna nooit tot nooit te maken heeft met cybercrime
3.2.	CYBERCRIME_FREQUENTIE_PRIVE	De persoon geeft aan hoe vaak hij of zij thuis te maken heeft met cybercrime
3.2.1.	CYBERCRIME_DAGELIJKS_PRIVE	De persoon geeft aan dat hij of zij thuis dagelijks te maken heeft met cybercrime
3.2.2.	CYBERCRIME_PERIODIEK_PRIVE	De persoon geeft aan dat hij of zij thuis periodiek te maken heeft met cybercrime
3.2.3.	CYBERCRIME_REGELMATIG_PRIVE	De persoon geeft aan dat hij of zij thuis regelmatig te maken heeft met cybercrime
3.2.4.	CYBERCRIME_NIET_VAAK_PRIVE	De persoon geeft aan dat hij of zij thuis bijna nooit tot nooit te maken heeft met cybercrime

4. Beoordeling van de situatie: Hoe beoordeelde u de situatie?
- Hoe wordt de situatie ingeschat door de persoon (wat is er aan de hand?)

Code	Naam	Definitie
4.1.	BEOORDELING_PRIVE	Het inschatten van de situatie bij een privé ervaring van de persoon
4.1.1.	BEOORDELING_PRIVE_FOUT	Phishing: De persoon ziet in het geval van phishing door uiterlijke kenmerken dat de mail niet echt is, of

		in het geval van een telefoontje weet de persoon dat het niet echt is en gaat er niet op in.
4.1.2.	BEOORDELING_PRIVE_TWIJFEL	Phishing: De persoon heeft na enige twijfel door dat de mail of telefoontje dat hij of zij heeft gekregen niet echt is.
4.2.	BEOORDELING_WERK	Het inschatten van de situatie bij een ervaring op het werk
4.2.1	BEOORDELING_WERK_SERIEUS	De persoon geeft aan dat hij of zij het probleem meteen serieus neemt.
4.2.2.	BEOORDELING_WERK_INVENTARISATIE	De persoon geeft aan dat hij of zij meteen gaat inventariseren wat er aan de hand is/de persoon verifiëren of het daadwerkelijk om de persoon gaat
4.2.3	BEOORDELING_WERK_STRESS	De persoon geeft aan dat hij of zij in de stress schiet/ervan schrikt als er sprake is van cybercrime
4.3.	BEOORDELING_CYBERCRIME	Hoe kwam de persoon erachter dat er sprake was van een cyber aanval
4.3.1.	BEOORDELING_CYBERCRIME_KLANT	De persoon kwam er door het contact met de klant achter dat er sprake was van een cyber aanval
4.3.2.	BEOORDELING_CYBERCRIME_INTERN	De persoon kwam er door interne berichten/info van tevoren achter dat er sprake was van een cyber aanval
4.3.3.	BEOORDELING_CYBERCRIME_MEDIA	De persoon kwam er door berichten in de media achter dat er sprake was van een cyber aanval

5. Acties: Kunt u omschrijven welke acties u ondernam om met de situatie om te gaan? (inschatting beste oplossing - hoe reageerde u in deze situatie?)

Code	Naam	Definitie
5.1.	ACTIES_PRIVE	Hoe handelt de persoon bij een privé ervaring met cybercrime
5.1.1.	ACTIES_PRIVE_ACTIEF	Actief aanpakken: het probleem wordt geanalyseerd en opgelost (active coping)
5.1.2.	ACTIES_PRIVE_SAMEN	Sociale steun zoeken: troost en begrip zoeken bij anderen, samen met een ander het probleem oplossen. Zowel instrumenteel als emotioneel. (seeking social support)
5.1.3.	ACTIES_PRIVE_VERMIJDEN	Vermijden: het probleem wordt ontkend en vermeden (denial)
5.1.4.	ACTIES_PRIVE_EMOTIES	Expressie van emoties: het probleem leidt tot frustratie, spanning en agressie (venting emotions)
5.1.5.	ACTIES_PRIVE_GERUST	Geruststellende gedachten: men houdt zich voor dat het probleem vanzelf wel goed komt of dat anderen het nog veel zwaarder hebben

5.1.6.	ACTIES_PRIVE_ ONDERDRUKKING	Onderdrukking van concurrerende activiteiten: men laat het werk liggen en gaat eerst doen wat belangrijk is (suppression of competing activities)
5.1.7.	ACTIES_PRIVE_IT	ICT: de persoon lost het probleem op door gebruik te make van firewalls, anti-virus software en houdt de computer up-to-date (Technological coping)
5.1.8.	ACTIES_PRIVE_ACCEPTEREN	Accepteren dat het is gebeurd, maar er zelf verder niks aan kunnen doen (Acceptance)
5.2.	ACTIES_WERK	Hoe handelt de persoon bij een ervaring met cybercrime op het werk
5.2.1.	ACTIES_WERK_ACTIEF	Actief aanpakken: het probleem wordt geanalyseerd en opgelost (active coping)
5.2.2.	ACTIES_WERK_SAMEN	Sociale steun zoeken: troost en begrip zoeken bij anderen, samen met een ander het probleem oplossen. Zowel instrumenteel als emotioneel (seeking social support)
5.2.3.	ACTIES_WERK_VERMIJDEN	Vermijden: het probleem wordt ontkend en vermeden (denial)
5.2.4.	ACTIES_WERK_EMOTIES	Expressie van emoties: het probleem leidt bij de medewerker zelf tot frustratie, spanning en agressie (venting emotions)
5.2.5.	ACTIES_WERK_GERUST	Geruststellende gedachten: men houdt zich voor dat het probleem vanzelf wel goed komt of dat anderen het nog veel zwaarder hebben
5.2.6.	ACTIES_WERK_ ONDERDRUKKING	Onderdrukking van concurrerende activiteiten: men laat het werk liggen en gaat eerst doen wat belangrijk is (suppression of competing activities)
5.2.7.	ACTIES_WERK_IT	ICT: de persoon lost het probleem op door gebruik te make van firewalls, anti-virus software en houdt de computer up-to-date (Technological coping)
5.2.8.	ACTIES_WERK_ACCEPTEREN	Accepteren dat het is gebeurd, maar er zelf verder niks aan kunnen doen (Acceptance)

6. Hoe zijn de reactie van klanten en de reacties van medewerkers naar de klanten?

Code	Naam	Definitie
6.1.	REACTIES_KLANTEN	Hoe reageren klanten in het geval dat zij te maken hebben gehad met een vorm van cybercrime en contact opnemen met de bank
6.1.1.	REACTIES_KLANTEN_PANIEK	De persoon geeft aan klanten vaak geschrokken of in paniek zijn als ze te maken hebben gehad met cybercrime
6.1.2.	REACTIES_KLANTEN_CHECK	De persoon geeft aan dat klanten vaak heel goed weten wat ze moeten doen, en de bank bellen als dubbel check/of om door te geven dat er bijvoorbeeld phishingmails rondgaan.

6.1.3.	REACTIES_KLANT_BANK	De persoon geeft aan dat de klanten vaak de schuld bij de bank neerleggen
6.2.	REACTIES_MEDEWERKERS	Hoe de persoon reageert als hij een klant spreekt die net te maken heeft gehad met een vorm van cybercrime
6.2.1.	REACTIES_MEDEWERKERS_ EMPATHIE	De persoon geeft aan met de persoon mee te leven/empathie te tonen naar de klant (emotie tonen naar klant)
6.2.2.	REACTIES_MEDEWERKERS_ GERUSTSTELLEND	De persoon geeft aan dat tijdens het contact met de klant het heel belangrijk is om de klant gerust te stellen
6.2.4.	REACTIES_MEDEWERKERS_TIPS	De persoon geeft aan dat tijdens het contact met de klanten het geven van tips centraal staat
6.2.5.	REACTIES_MEDEWERKERS_VERTROUWEN	De persoon geeft aan dat tijdens het contact met de klant het vertrouwen in de bank moet worden overgebracht
6.2.6.	REACTIES_MEDEWERKERS_KLANT	De persoon geeft aan dat de klant vaak zelf de fout in is gegaan/dat het van twee kanten komt als je slachtoffer wordt van cybercrime

7. Voorbereid: In hoeverre bent u voorbereid op dit soort situaties? En: Vindt u dat u voldoende bent geïnformeerd over de gevolgen van cybercrime?

Code	Naam	Definitie
7.1.	VOORBEREID_WEL	De persoon geeft aan voorbereid te zijn
7.1.1.	VOORBEREID_HANDLEIDING	De persoon geeft aan door middel van handleidingen voorbereid te zijn op dit soort situaties
7.1.2.	VOORBEREID_PROTOCOL	De persoon geeft aan door middel van protocollen die gevolgd moeten worden voorbereid te zijn op dit soort situaties
7.1.2.	VOORBEREID_ERVARING	De persoon geeft aan dat door de ervaring voorbereid is op dit soort situaties
7.1.3.	VOORBEREID_GOED_GEINFORMEERD	Persoon geeft aan dat hij of zij goed geïnformeerd is over de gevolgen van cybercrime
7.2.	VOORBEREID_NIET	De persoon geeft aan niet voorbereid te zijn
7.2.1	VOORBEREID_NIET_SITUATIE	De persoon geeft aan niet voorbereid te zijn op dit soort situaties, doordat elke situatie anders is
7.2.2.	VOORBEREID_NIET_ONVERWACHT	De persoon geeft aan niet voorbereid te zijn op dit soort situaties, omdat cybercrime vaak heel onverwacht is
7.2.3.	VOORBEREID_NIET_GEINFORMEERD	Persoon geeft aan niet voldoende of niet goed is geïnformeerd over de gevolgen van cybercrime
7.2.4.	VOORBEREID_NIET_DOEN	Persoon geeft aan dat je niet voorbereid kan zijn in het geval van cybercrime, maar dat hij of zij wel weet hoe er moet worden gehandeld

8. In hoeverre heeft de persoon het vertrouwen in zijn of haar eigen vermogen/coping gedrag om zichzelf te beschermen tegen dergelijke bedreigingen?

Code	Naam	Definitie
8.1	VERTROUWEN	De persoon geeft aan dat hij of zij vertrouwen heeft in het eigen vermogen om het probleem zelf op te lossen
8.1.1.	VERTROUWEN_MAATREGELEN	De persoon geeft aan dat hij of zij dit vertrouwen heeft, doordat alle maatregelen zijn genomen om het probleem te voorkomen
8.1.2.	VERTROUWEN_BEWUST	De persoon geeft aan dat hij of zij dit vertrouwen heeft, omdat hij of zij heel bewust omgaat met het internet/persoonlijke gegevens.
8.2.	GEEN_VERTROUWEN	De persoon geeft aan dat hij of zij niet het vertrouwen heeft in het eigen vermogen om het probleem zelf op te lossen
8.2.	GEEN_VERTROUWEN_KENNIS	De persoon geeft aan dat hij of zij niet dit vertrouwen heeft omdat de persoon er te weinig kennis van heeft

9. Stress: Ervaart de persoon stress op de werkvloer, of door cybercrime?

Code	Naam	Definitie
9.1.	STRESS_WERKVLOER	Persoon geeft aan dat hij of zij stress ervaart op de werkvloer
9.1.1.	STRESS_CYBERCRIME	De persoon geeft aan dat hij of stress ervaart op de werkvloer door, de dreiging van, cybercrime
9.1.2.	STRESS_WERKDRUK	De persoon geeft aan dat hij of zij stress ervaart door de werkdruk die wordt verhoogt als er verschillende incidenten zijn
9.2.	STRESS_CYBERCRIME_GEEN	Persoon geeft aan dat cybercrime geen stress veroorzaakt
9.2.1.	STRESS_CYBERCRIME_ PERSOONLIJKHEID	Persoon geeft aan dat hij of zij geen stress ervaart door cybercrime door zijn of haar persoonlijke eigenschappen (bijvoorbeeld: nuchter, geduldig, niet snel gestresst).

10. Zorgen: In hoeverre maakt u zich zorgen dat hij, zij of de organisatie slachtoffer wordt van cybercrime.

Code	Naam	Definitie
10.1.	ZORGEN_PRIVE	Persoon geeft aan zich zorgen te maken dat hij of zij privé slachtoffer wordt van cybercrime
10.1.1.	ZORGEN_PRIVE_KANS	Persoon geeft aan zich wel een zorgen te maken, omdat het steeds vaker voorkomt
10.2.	ZORGEN_PRIVE_NIET	Persoon geeft aan dat hij of zij zich geen zorgen maakt om privé slachtoffer te worden van cybercrime
10.2.1.	ZORGEN_PRIVE_NIET_VEILIG	Persoon maakt zicht geen zorgen dat hij of zij prive slachtoffer wordt, omdat diegene er alles aan doet om de kans zo klein mogelijk te maken

10.2.2.	ZORGEN_PRIVE_NIET_KANS	Persoon geeft aan dat hij of zij zich geen zorgen maakt om prive slachtoffer te worden van cybercrime, omdat iedereen slachtoffer kan worden, maar de kans heel klein is
10.2.3.	ZORGEN_PRIVE_NIET_INTERNET	Persoon geeft aan dat hij of zij zich geen zorgen maakt om privé slachtoffer te worden van cybercrime, omdat er heel bewust met internet om wordt gegaan
10.2.4.	ZORGEN_PRIVE_NIET_ALERTER	Persoon geeft aan dat hij of zij zich geen zorgen maakt, maar wel alerter/bewuster is. Persoon weet dat het kan gebeuren.
10.2.5.	ZORGEN_PRIVE_NIET_SLACHTOFFER	Persoon geeft aan zich geen zorgen te maken omdat hij of zij nog geen slachtoffer is geweest.
10.3.	ZORGEN_WERK	Persoon geeft aan zich zorgen te maken dat de bank slachtoffer wordt van cybercrime
10.3.1.	ZORGEN_WERK_FOCUS	Persoon geeft aan zich zorgen te maken dat de bank slachtoffer wordt doordat de focus nu voornamelijk lijkt te liggen op andere belangrijke zaken (bijvoorbeeld; overgang naar IBAN)
10.3.2.	ZORGEN_WERK_TOENAME	Persoon geeft aan zich zorgen te maken dat de bank slachtoffer wordt, omdat het steeds vaker voorkomt
10.3.3.	ZORGEN_WERK_NIEUW	Persoon geeft aan zich zorgen te maken dat de bank slachtoffer wordt omdat er steeds iets anders wordt verzonnen door de criminelen
10.3.4	ZORGEN_WERK_KANS	Persoon geeft aan zich zorgen te maken dat de bank slachtoffer wordt, maar dat hij of zij ook wel het vertrouwen heeft dat de bank er alles aan doet.
10.4	ZORGEN_WERK_NIET	Persoon maakt zich geen zorgen dat de bank slachtoffer wordt van cybercrime
10.4.1.	ZORGEN_WERK_NIET_KANS	Persoon maakt zich geen zorgen dat de bank slachtoffer wordt, omdat de bank er alles aan doet om de kans zo klein mogelijk te maken
10.4.2.	ZORGEN_WERK_NIET_TAAK	Persoon maakt zich geen zorgen dat de bank slachtoffer wordt, omdat dat min of meer de taak van de bank is om ervoor te zorgen dat de bank geen slachtoffer wordt.
10.4.3.	ZORGEN_WERK_NIET_ANGST	Persoon maakt zich geen zorgen dat de bank slachtoffer wordt en geeft aan dat je het er ook niet teveel over moet hebben. Dit zorgt voor meer angst

11. Wat zijn de gevolgen van cybercrime op het werk (job outcomes) en op het privé gebruik als het gaat om cybercrime?

Code	**Naam**	**Definitie**
11.1.	GEVOLGEN_WERK	De persoon geeft aan of, de dreiging van, cybercrime van invloed is op de job outcomes, zoals: werkdruk, service quality, tevredenheid van de klant, het functioneren etc
11.1.1.	GEVOLGEN_WERKDRUK	Persoon geeft aan dat als gevolg van cybercrime de werkdruk wordt verhoogd.

11.1.2.	GEVOLGEN_SERVICE_QUALITY	Persoon geeft aan dat cybercrime invloed heeft op de kwaliteit van de service
11.1.3.	GEVOLGEN_KLANT	Persoon geeft aan dat cybercrime invloed heeft op de tevredenheid van de klanten
11.1.4.	GEVOLGEN_FUNCTIONEREN	Persoon geeft aan dat cybercrime invloed heet op het functioneren op het werk
11.2.	GEVOLGEN_PRIVE	Persoon geeft aan dat er gevolgen zijn voor het gebruiken van internet e.d. thuis
11.2.1.	GEVOLGEN_PRIVE_INTERNET	Persoon geeft aan wat de gevolgen zijn voor het gebruik van bijvoorbeeld internet (online winkelen, websites bezoeken)
11.2.2.	GEVOLGEN_PRIVE_BANKIEREN	Persoon geeft aan wat de gevolgen zijn voor het bankieren/internetbankieren (via de app of juist op de ouderwetse manier)
11.2.3.	GEVOLGEN_PRIVE_BEWUST	Persoon geeft aan dat hij of zij thuis bewuster omgaat met het internet door de ervaringen op het werk.
11.3.	GEVOLGEN_WERK_NIET	Persoon geeft aan dat, de dreiging van, cybercrime niet van invloed is op een van de job outcomes.
11.4.	GEVOLGEN_PRIVE_NIET	Persoon geeft aan dat er geen gevolgen zijn

12. Organisatie: Wat doet de organisatie aan cyber security, en doet de organisatie er in de ogen van de medewerker genoeg aan?

Code	Naam	Definitie
12.1.	ORGANISATIE_CYBERSECURITY	Persoon geeft aan wat de organisatie er aan doet om cybercrime tegen te gaan
12.1.1.	CYBERSECURITY_MAIL	Persoon geeft aan dat klanten hun phishing mail door kunnen sturen naar een speciaal mail adres
12.1.2.	CYBERSECURITY_INFORMATIE	Persoon geeft aan dat de organisatie voldoende informatie verstrekt (bijvoorbeeld op websites) om cybercrime tegen te gaan/mensen te informeren
12.1.3	CYBERSECURITY_AFDELING	Persoon geeft aan dat de organisatie een speciale afdeling heeft die dagelijks met cybercrime bezig is
12.1.4.	CYBERSECURITY_CAMPAGNE	Persoon geeft aan dat de organisatie mee werkt aan verschillende campagnes over cybercrime
12.1.5.	CYBERSECURITY_BLOKKEREN	Persoon geeft aan dat de organisatie tegenwoordig aan geo-blocking doet, waardoor klanten eerst hun pasje moeten deblokkeren als ze er buiten europa gebruik van willen maken
12.1.6	CYBER_SECURITY_GEEN	Persoon geeft aan geen idee te hebben wat de organisatie aan cyber security doet of nog zou moeten doen om cyber crime tegen te gaan
12.1.7	CYBER_SECURITY_OVERIG	Persoon geeft aan wat de organisatie er aan doet om cybercrime tegen te gaan
12.1.	ORGANISATIE_MEER	Persoon geeft aan dat de organisatie er meer aan zou kunnen doen om cybercrime tegen te gaan.
12.1.1.	ORGANISATIE_MEER_INFO	De persoon geeft aan dat de organisatie meer informatie zou kunnen verstrekken over cybercrime

12.1.2.	ORGANISATIE_MEER_CASUS	De persoon geeft aan dat de organisatie door middel van casussen de medewerkers beter kan voorbereiden op mogelijke cyberaanvallen
12.1.3.	ORGANISATIE_MEER_SAMENWERKEN	De persoon geeft aan dat de organisatie meer met andere instanties zou kunnen samenwerken om cybercrime tegen te gaan
12.2	ORGANISATIE_VOLDOENDE	Persoon geeft aan dat hij of zij het niet nodig vindt dat de organisatie er meer aan doet. Voldoende op dit moment.
12.3	ORGANISATIE_TE_VEEL	Persoon geeft aan dat de organisatie te veel doet om cybercrime tegen te gaan.
12.3.1.	ORGANISATIE_TE_VEEL_ANGST	De persoon geeft aan dat de organisatie er veel aan doet, maar dat te veel informatie verspreiden voor onrust kan zorgen bij de klanten