Leiden University – Faculty of Governance and Global Affairs

Master Thesis

Cyber Risk as a Reputational Risk: a Research into the Financial Sector of the Netherlands

Student: Nynke Broos

Student number: S2055619

Program: MSc Crisis and Security Management

Supervisor: Dr.ir. Vlad Niculescu-Dinca

Second reader: Mr. Sergei Boeke

Date: January 13, 2019

Word Count: 18.556

Acknowledgements

To begin with, I would like to express special gratitude to my thesis supervisor Vlad Niculescu-Dinca for his support and constructive feedback. His confidence in me finishing this thesis along a somewhat non-standard path, with two full-time internships along the way is highly appreciated.

I also gratefully thank PwC Amsterdam for giving me the opportunity to make use of its resources. Thanks to my former five colleagues who, as anonymous referees, shared their extensive knowledge for this research. A special thanks goes to Sanne Amber Maas, my internship supervisor at PwC, for her help and encouragement.

I would like to thank all my friends and family for their continues mental support. Thank you JJ, Charlot, Ruben and Emma for reviewing this research when time was of essence.

Last but not least, I would like to thank my parents for their belief in me and the positivity they have given me in the past year, and all the years before. Soon I will be able to close the book “My Life as a Student”, and they were the greatest motivation I could wish for to successfully finish the final chapter called “Master Thesis”.

Abstract

In times of technological developments, the digitalization of financial transactions and social media, cyber security incidents are seen as one of the main threats to the reputation of a financial institution. In recent years, especially the financial sector faced an increased amount of cyber risks. Even though it is widely acknowledged that cyber incidents pose a significant risk to the reputation of financial institutions, not a lot is known about *how* these institutions deal with cyber risks as a reputational risk. This qualitative and exploratory research therefore tried to understand the relation between cyber risks and reputational risk, while its inquiry focussed on financial institutions in the Netherlands. Understanding this relation was started by studying the perception and management of both reputational risk and cyber risks separately. The research demonstrated that compliance to different regulatory requirements are influential in the perception and management of reputational risk. It appeared that financial institutions do attach great value to their reputation and perceive the trust of its stakeholders an important asset, but in turn do not have a structured and comprehensive reputational risk management framework in place. This can be due to the fact that in most of the cases, financial institutions deal with reputational risk in an indirect way, or as the result of other developments, decisions and risks. The finding that financial institutions often deal with reputational risk as more of a 'risk-of-risks' instead of a specific, self-standing risk has influence on how is dealt with cyber risks as well. For example, with regard to their reputation, financial institutions often perceive cyber as a liability, something they have to comply with in order to make use of their reputation as an asset. Financial institutions recognize the importance of their cyber risks, but a gap exists between the management of the business aspects of cyber risk activities on the one hand, and the technical aspects of it on the other hand. The research findings demonstrated that the two risks are only integrated to a certain extent; the larger the potential financial consequences seem, the more the cyber risks are dealt with as reputational risk. Only when large consequences or financial losses are potentially involved, financial institutions play significant attention to the other aspects (tech-socio) as well, next to the technical aspects they normally focus on. The focus on the technical security side of cyber risks can be an explanation of making it more difficult to link cyber risks to the management of reputational risk. In the absence of a structured, comprehensive reputational risk framework, the findings of this research urge the need for further research into more structured ways to deal with reputational risk, before cyber risks can be more effectively incorporated. The study results serve as a starting point for better understandings that in turn can help to further build upon a comprehensive and integrated cyber-reputational risk framework for financial institutions in the Netherlands.

Table of Contents

1 Introduction

1.1 Background

1.1.1 The financial sector's reputation

In recent decades, the role of the financial sector within society has changed. While financial services and products became more important to citizens, governments and companies, the influence of financial institutions on the economy and society has increased strongly as well (Wetenschappelijke Raad voor het Regeringsbeleid, 2016, p. 7). More than ten years after the crisis hit the financial sector and following several scandals involving numerous different banks, the entire financial sector however lost a lot of society's trust (Wetenschappelijke Raad voor het Regeringsbeleid, 2016, p. 25). This can be illustrated by the fact that financial institutions, such as banks, insurers and pension funds, routinely rank the last place in 'trust'-surveys conducted in different industries (Bonime-Blanc, 2017). The 21st century's 'information society' in general, and specifically social media have a strong influence on a financial institution's reputation. A trustable reputation can be destroyed in only a few minutes (Gaultier-Gaillard, Louisot, & Rayner, 2009, p. 1). A loss of confidence by the public, or to say a "damaged reputation", can bring risks to financial institutions themselves. This can have mayor consequences, as a single firm's entire position depends on its reputation (Heidinger & Gatzert, 2018, p. 106). Therefore, business professionals and academics agree on the fact that 'reputational risk' is one of the major strategic risks for companies (Deloitte, 2014; Gaultier-Gaillard, Louisot, & Rayner, 2009). Society requires financial institutions to be more socially responsible, and public debate is focused on, for instance, privacy and security concerns or sustainability (PwC, 2014, p. 15).

1.1.2 Cyber threats and the reputation of financial institutions

In times of technological developments, the digitalization of financial transactions and social media, cyber security incidents are seen as one of the main threats to a company's reputation. This is especially the case for companies in the financial sector, as the amount of cyber-attacks in this sector rose by 80% in 2017 compared to the year before (Financial Conduct Authority, 2018). Even more, a report published by Accenture and the Ponemon Institute (2017) demonstrates that cyber-attacks have proven to be way more costly to firms in the financial sector than in any other sector. It thus comes with no surprise that both cyber and reputation are strategically important risks for the majority of companies.

Furthermore, the combination of reputational and cyber risk, is perceived as a relatively new, yet very powerful strategic matter for especially financial institutions. In order to meet the challenges that the relatively new 'combined' risk of cyber-reputational risks brings, financial institutions feel the need to transform themselves (PwC, 2014, p. 1). In the post-financial crisis era discussed in the first two sections of this chapter, factors such as increased regulatory requirements, changed expectations of customers and technological innovation, urged financial institutions to change their overall and reputational strategies (PwC, 2014, p. 1). Within these strategies, the role and responsibility financial institutions have with regard to society as a whole has become a more central aspect (Nederlandse Vereniging van Banken, 2014). In addition, in reaction to the increased amount of cyber-attacks as discussed previously, financial institutions also rapidly increased their expenditure on, and investment in, cyber risk management (Financial Conduct Authority, 2018).

1.1.3 The financial sector in the Netherlands

The Dutch financial sector also faces the challenges discussed in the previous sections. Compared to other European countries, the financial sector in the Netherlands is relatively large in size. The Netherlands Authority for the Financial Markets (2018) expects "the Netherlands to become the centre of European financial trading post-Brexit". Within the Netherlands, banks are the most dominant players, as their share of the whole financial market is more than 52% in terms of capital (Wetenschappelijke Raad voor het Regeringsbeleid, 2016, p. 78). Also, the concentration-ratio of the Dutch financial sector is among the highest in Europe. In essence, this means that there is a strong dependence in the Netherlands on the three biggest banks – ING, Rabobank and ABN AMRO. Next to these elements of uniqueness of the Dutch financial market, this market is comparable to those of other European countries, as all have to comply with the same regulations of the European Central Bank (ECB). Within European perspective, the biggest Dutch financial institutions are among the 39 most important ones. Worldwide, they are on the list of the 29 systemically relevant banks (Wetenschappelijke Raad voor het Regeringsbeleid, 2016, pp. 92-94). The discussion above gives a clear overview of the relevance of the Dutch financial sector, and explains why the Netherlands has been chosen as the focus country in this research.

1.2 Problem statement

Business professionals in the financial sector and academics clearly recognize the effects cyber security can have on a company's reputation. Most of them also agree on the fact that cyber-attacks are not entirely preventable, and thus a firm's reputation might always be at risk (Rance, 2014, pp. 4-5; PwC, 2018). Based on that assumption, the question is not if an organization will face a cyber-attack, but when. Accordingly, it can also be argued that cyber risks might always pose risks to the reputation of financial institutions. For that reason, it is important how risks are managed before, during and after a cyber-incident (Bonime-Blanc, Mitigating cyber-reputation risk, 2016). This has all to do with the decisions leaders of financial institutions make. This raises questions on what constitutes strategic leadership in the case of a cyber-attack, while simultaneously the reputation of a financial services company is taken into account. Especially, as is argued by Jan van den Berg et al. (2014, p. 7) "breaches occur in the technical layer while the true impacts (risks) of these breaches work out into the socio-technical layer of cyber activities". According to Bonime-Blanc (2016), the management of cyber-reputation risk is a team sport. In order to effectively govern cyber-reputation risks, approaches that are both cross-disciplinary and cross-segmental, are required. Therefore, all departments, experts and business units within a firm should cooperate before, during and after a cyber-reputation risk incident to be able to create an effective defence strategy for the long-term resilience that is needed to manage these strategic risks. Within most companies, reputational risk is however traditionally dealt with at the communications or public relations departments, while cyber issues are managed by IT-departments (Bonime-Blanc, 2017). In practice, cyber risks and reputational risks are thus often being linked, but 'treated' or managed separately. For example, in many policy documents, reports or surveys they are discussed in different sections and within different contexts. This is also the case for academic literature, as only few scholars integrate both concepts and mostly apply different frameworks and strategies to both risks, on which will be elaborated in Chapter 2 of this research. Furthermore, the fact that both 'cyber' and 'reputation' are broad concepts in both business and literature, but are interchangeably used, asks for further research into how they relate in practice. How do they interact, and what parallels and differences can be identified? Due to this knowledge gap, an exploratory research into the approaches policy practices, measures and strategies regarding cyber-reputational risks of financial sector firms is a good starting point for the revision of existing policies in the financial sector.

1.3 Objective of the research and research question

The objective of this research is to provide insights and better understandings into the current approaches on the management of cyber- and reputational risks by financial institutions, for which the Netherlands has been chosen as the focus country. The main research question of this thesis is: *"How do financial institutions in the Netherlands deal with cyber risk as reputational risk?"*

By answering this question links and patterns between cyber risks and reputational risk will be identified that might serve as a starting point for future research into cyber-reputational risk approaches that are more integrated and comprehensive. Such approaches can contribute to financial institutions attempts to reduce risks. It thus does not aim to explain the complex field of the Dutch financial sector as a whole, nor does it endeavor to create a complete new operational risk management model for the financial sector.

1.4 Sub-questions

In order to answer the main research question that is guiding this research, two sub-questions will be explored. The first sub question aims to get a clear view on how financial institutions perceive reputational risk and how their attempts in managing this risk look like. The second sub-question focuses on the perception of cyber threats and how cyber risk management of financial institutions in the Netherlands can be understood. The sub-questions are formulated as follows:

1. *"How do financial institutions in the Netherlands perceive and deal with reputational risk?"*
2. *"How do financial institutions in the Netherlands perceive and deal with cyber risk?"*

1.5 Societal Relevance

The Dutch National Coordinator for Security and Counterterrorism (2018) perceives certain processes within the financial sector as part of the critical infrastructure of the Netherlands. Failure or disruption of, for example, the cyber security of financial institutions may cause severe social disruption and pose a threat to national security. Even more, malicious use of IT and cyber-attacks can put financial stability in jeopardy. Next to that, the storage of a high amount of (sensitive) client-data makes financial institution's cyber security policy subject to privacy and personal data protection concerns, currently hot-topics in politics, the media and academics (Carr, 2016, p. 50). Therefore, it is important to manage cyber risks in an effective way.

Furthermore, the financial sector's reputation is dependent on the perceptions and expectations of its stakeholders (Rayner, 2004, p. 1). Research on reputational risk is thus relevant for society as the members of the previously mentioned society are those respective stakeholders. More knowledge on and the subsequent improvement of the management of instabilities and uncertainties that pose risks to financial institutions, is thus in the interest of the Dutch society, and also for the rest of the world. It is therefore highly relevant to further research how cyber risk is used as a reputational risk, and thus is managed as a comprehensive part of financial institutions. The primary societal value of this research resides in resolving more clearance on, and the relation between cyber risk and reputational risk issues. The secondary societal value is therefore providing policy-makers and business professionals with a stronger "toolbox" for developing and improving their risk-management strategies. The latter counts even more now the Netherlands Authority for the Financial Markets (2015) emphasizes that in order to restore society's trust in financial institutions, changes have to be initiated more from the sector itself. This might eventually also provide valuable insights for the government, which might help to improve public-private partnerships (Carr, 2016).

1.6 Academic Relevance

The emerge of new technologies and substantial changes that the financial sector itself underwent, made the academic body of knowledge on corporate reputation change a lot in the past decades. Literature that focuses on reputational risk in this new digital era is therefore not very developed yet, especially as most studies focus on the financial sector in the United States or were conducted before the 2008 financial crisis (Fiordelisi, Soana, & Schwizer, 2012, p. 107). As discussed before, amongst others due to EU regulations, European banks differentiate themselves to a certain extent from US banks, and the financial sector landscape has changed in the past decennia. Therefore, scholars stress the necessity for further research into the management of reputational risk (Heidinger & Gatzert, 2018, pp. 106-107). Due to the relative newness of the subject of cyber in the financial sector, scholars Lagazio, Sherif and Cushman (2014, p. 59) stress that theories and frameworks on cyber risk are also still premature. This is confirmed by Van den Berg et al. (2014, p. 1), who stress that "science has difficulties in speeding up with the recent fast digitalization developments in society and its related cyber security challenges", including cyber-risk challenges. Also, within the academic literature on cyber risks, a division can be observed between the studies focussing on the governance and business and those focussing on the technical aspects of cyber risks.

The primary academic value of this research is providing more much-needed clearance on reputational as well as cyber risk. It hereby contributes to the ongoing academic discussions within the context of the financial sector.

Furthermore, a clear knowledge gap exists in the research on "cyber-reputational risk" within the financial sector as an integrated risk, as only very few researches on this issue can be found. This is especially the case for the Dutch and European context, as most researches focus on the US (Fiordelisi, Soana, & Schwizer, 2012, p. 107), or the financial market as a whole. The findings of these researches are only to a limited extend applicable to the Netherlands, as the Dutch financial market has to adhere to other EU regulations. As this research will provide a more holistic approach, it also aims to contribute to this discussion and help to bridge gaps between the two risks, while in the meantime it contributes to studies focussed on the Dutch financial sector. The secondary academic value therefore resides in investigating the position and underdeveloped framework on the integration of cyber- and reputational risk. The clarification this research provides will open up avenues for integrated theories and frameworks for these two risks.

1.7 Organization of the thesis

This thesis is structured as follows. The first chapter of this thesis presented an overview of the problem and stressed the relevance of conducting research into the integration of cyber and reputational risk within the financial sector. In the following chapter, the theoretical framework on cyber risks and reputational risk will be presented. The third chapter demonstrates the methodology of this research that provides a framework for adequately formulating answers to the main research question in the subsequent analysis. From here, this thesis will proceed by answering the two sub-questions in chapter five. This chapter will present the research results and will provide an analysis on how financial institutions manage reputational- and cyber risks. Following this analytical chapter, chapter six will answer the main research question by presenting a conclusion and reflection, will feature the limitations of the research and will make recommendations for further inquiry.

2 Theoretical Framework

2.1 Introduction

This chapter reviews the current body of knowledge surrounding and reputational risk and cyber risks. Cyber and reputational risk contain different individual concepts, which are all subject to interpretation. By addressing the literature on these concepts, this framework provides the theoretical foundation of this research that will help to contextualize the research findings. To begin with, a brief overview of risk studies literature will be presented to problematize risk. Next, it is important to have a basic understanding on the concept of corporate reputation to be able to contextualize reputational risk. Therefore, academic perspectives on corporate reputation will be discussed first, followed by the literature on reputational risk. Thereafter, the literature on cyber and cyber risk will be reviewed. As many 'cyber' concepts are interchangeably used, both in practice as well in academics, a clarification to the concept of cyber security will be given first. This will be followed by a review of the literature on cyber risk and cyber risk management. Lastly, the existing literature that links both risks and studies cyber-reputational risk as an integrated risk will be discussed.

2.2 Problematizing 'risk'

As a large part of this research focuses on risks, it is necessary to put a 'brief dive' into the extensive risk studies literature. It should be stated that no single generally accepted definition for risk exists, as it is used in different academic disciplines, such as accounting and economics. Within the social sciences, three approaches with regard to risk are most commonly acknowledged. The first one is the 'governmentality' perspective of scholars stemming from Michael Foucault's practices and the second, developed by Mary Douglas, is more a 'cultural approach' towards risk (Burgess, Wardman, & Mythen, 2018, p. 2). The third approach, the understanding of the concept of a 'risk society', was put forward by the German sociologist Ulrich Beck. He defines risk as "a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself" (1992, p. 21). According to Beck, risks are produced by the industry and are dependent on decisions that are made (1992, p. 183). This is confirmed by Giddens, as he stresses that a risk only occurs in case a decision needs to be taken (Giddens, 1999, p. 8). He also states that the risks we currently face in our modern society are 'manufactured' by human development (Giddens, 1999, p. 4).

Giddens points out an important take away: these manufactured risks cause a so-called responsibility crisis, as “the connections between risk, responsibility and decisions alter (Giddens, 1999, p. 8). Contrastingly, Beck’s work is also criticized, for example by Mythen (2004, pp. 181-182), who argues that it is not engaging sufficiently with the possibilities of empirical validation of risk. Apart from the notion that the *nature* of risk has changed in the past modern era according to Beck and Giddens, positions – not necessarily contrasting - of other scholars on the concept of risk will be presented. A prominent scholar in risk studies, Ortwin Renn, understands risk as "an uncertain consequence of an event or an activity with respect to something that humans value” (Renn, 2005, p. 19). He argues that a consequence can either be negative of positive, and that a risk indicates a mixture of two elements. First, how likely potential consequences are, and second, the degree of the consequences of activities by nature, humans or both. Related to specifically organisations, Paul Collier cites the 1999 definition of International Federation of Accountants, who defines risks as the “uncertain future events which could influence the achievement of the organization’s strategic, operational and financial objectives” (2003, p. 28). Furthermore, Collier stresses that taking risks is unavoidable when doing business and that returns are the business’ compensation for those risks. (2003, p. 28).

The concept of risk is often seen as something subjective that is difficult to measure. Many current approaches to risk management therefore see it as an objective function of probability and undesirable consequences, dependent on the risk perception of the respective stakeholder (Cook, Phillips, & Holden, 2006, p. 418). Renn presents a very comprehensive and integrated framework for the empirical validation and analysis of risk governance. However, as this thesis does not dive into the (broad concept of) governance of risk, the part on risk management is of particular interest to this research (Renn, 2005, pp. 11-15). Referring to the central position of decision-making as put forward by Beck and Giddens in the previous section, according to Renn the phase of risk management “designs and implements the actions and remedies required to tackle risks with an aim to avoid, reduce, transfer or retain them” (Renn, 2005, p. 14). However, the steps that preclude the management sphere of risk, namely the assessment sphere, are of importance to understand the management. Therefore, the overall framework presents interesting insights that might be useful in the analysis and conclusion of this research.

What is interesting about this framework is the inclusion of the societal context and the fact that risk communication is seen as a key element within the overall risk management of an organization. In addition, scholars Van Asselt and Renn (2011, p. 431) provide a conceptualization of the management of risks that includes "the various ways in which many actors, individuals, and institutions, public and private, deal with risks surrounded by uncertainty, complexity, and/or ambiguity".

2.3 Literature review 'reputational risk'

2.3.1 Corporate reputation

Within the academic literature, corporate reputation can be explained from different perspectives. Larking (2002, p. 42) brought together several perspectives as can be seen in figure 2. For example, from a sociological perspective, reputation can be seen as the social construction of interactions between different actors.

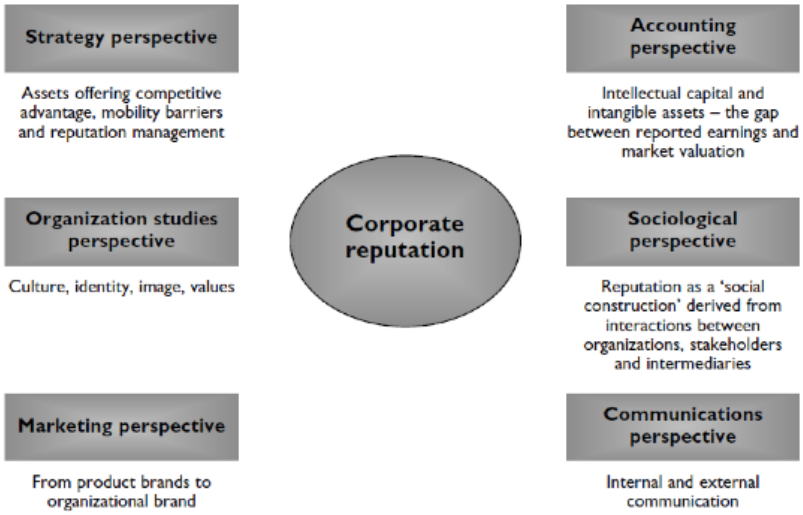

Figure 1: Corporate reputation: converging ideas (Larkin, 2002, p.42)

Even though the word 'reputation' has a different meaning in different perspectives and study disciplines, within all of the disciplines it implicates to be a relatively complicated and intangible asset. Rayner therefore argues that it is more important to focus on what constitutes a good reputation, namely "an organization enjoys a good reputation when it consistently meets or exceeds the expectations of its stakeholders" (Rayner, 2004, p. 2). According to Rayner (2004, p. 3), the most important advantage for a company to have a 'good' reputation is that it can create a certain amount of goodwill, or so-called reputational capital, amongst its stakeholders. This reputational capital can help the company by serving as a buffer during crises and attributing to crisis resilience.

Bonime-Blanc (2016, p. 6) further emphasizes the importance of stakeholders with regard to reputational risk: “knowing who your stakeholders are, understanding their expectations of your organization and how to prioritize them has everything to do with effective reputation risk management”. In addition to this, the Oxford Handbook of Corporate Reputation defines corporate reputation as ‘‘a collective assessment of a company’s attractiveness to a specific group of stakeholders relative to a reference group of companies with which the company competes for resources’’ (Fobrun, 2012, p. 100). Stakeholders are thus key towards corporate reputation, and in the financial sector the shareholders of an institution are seen as the main determinants. However, the classic (broad) definition by Edward Freeman of stakeholders is “any group or individual who can affect or is affected by the achievement of the organisation’s objectives” (Baumfield, 2016, p. 4) and can thus be customers, employees, the public, suppliers, the media, competitors, the government and even criminals.

2.3.2 Reputational risk

Because reputational risk strongly relies on the perceptions of external stakeholders, difficulties exist within the academic literature in defining and managing it (Miklaszewska & Kil, 2016, pp. 96-97). It is important to note that within the existing literature, discussion exists on the nature of reputational risk. One group of scholars define reputational risk as a specific, self-standing risk that has apparent drivers and brings real consequences for business, even if those drivers and consequences are difficult to measure (Economist Intelligence Unit, 2005). Amongst those scholars are Miklaszwska and Kil (2016, p. 97), who propose a new way of analyzing reputational risk as a self-standing risk. They examine the impact of reputational risk on bank performance by making use of a stakeholder reputation score-indicator. A second group of scholars do recognize the reputational aspects a specific risk might have, but do not consider reputational issues as a *risk* themselves. They perceive an issue such as reputational damage only as the result or consequence of other developments (Economist Intelligence Unit, 2005, p. 6). The third group of scholars state that reputational risk should not be seen as a risk in its own right, but more as a “risk of a risk”. They argue that reputational risk is dependent on other sources that influence or impact reputation. A cyber security attack is an example of such a source (Gaultier-Gaillard, Louisot, & Rayner, 2009, p. 9). Heidinger and Gatzert also underscore this form of interpretation to reputational risk, as they underpin the different determents of defining certain developments or practices as a reputational risk (Heidinger & Gatzert, 2018, pp. 1-2).

Bonime-Blanc seems to fit within this last group of scholars, as she defines reputational risk as "an amplifier risk that layers on or attaches to other risks (…) adding negative or positive implications to the materiality, duration or expansion of the other risks on the affected organisation, person, product or service" (Bonime-Blanc, 2017, p. 42). She further argues that reputational risk is strategic; see figure 2 for a visual presentation on how, according to her, reputational risk is best placed within 'all' risks an organisation faces (Bonime-Blanc, 2017, p. 49).

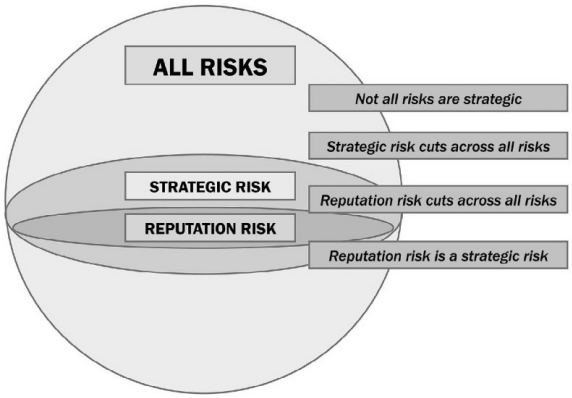

Figure 2: Reputational risk is a strategic risk (Bonime-Blanc, 2017, p. 49).

This figure points out an essential aspect of reputational risks; they interconnect with almost all aspects or risks within an organization. Not all scholars express clearly which of the three above-presented approaches they endeavour; Mukherjee, Zambon and Lucius (2008, p. 3) see reputational risk as anything that reduces the value of a reputation. They consequently measure reputational risk in two different ways. The first "gives a monetary valuation using market capitalization or return on assets". The second way applies the " valuation as intellectual capital using internal performance scorecard and other indices" (Mukherjee, Zambon, & Lucius, 2008, p. 3). Within the academic literature, there however exists a lack of uniformity with expressing reputational risk financially (Fiordelisi, Soana, & Schwizer, 2012, p. 107). Miklaszwska and Kil (2016, p. 113) argue that academic research on reputational risk in the financial sector is mostly focussed on the interests of all the different stakeholders, and to a lesser extent on regulatory requirements. As a result, Bonime-Blanc (2017) argues that many frameworks on reputational risk therefore focus on measuring perceptions among the stakeholders, such as customers, employees, shareholders, the government, the media etc., of the organization. She further states that reputational risk is seen by specifically the financial sector as 'compliance' and 'ethics'.

Bonime-Blanc (2017) also mentions that this sector thus often sees reputational risk as 'a cost of doing business', which can be linked to the first section of this chapter, where Collier stressed that taking risks in general is unavoidable when doing business.

2.3.3 Reputational-risk management

The development of a comprehensive infrastructure for reputational risk management is currently only it its early stages (Miklaszewska & Kil, 2016, p. 97). For example, Scandazzo (2011, p. 41) offers a framework that includes "the identification, assessment, monitoring and reporting", but does not offer further clarification on the management of reputational risk. Nadine Gatzert (2015, p. 488) is taking a more holistic approach to reputational risk, as she embedded it within the wider risk management model of an organization, by studying two relations. First, the impact of reputation on stakeholder behaviour and financial performance, such as revenue and shareholder value. Second, the impact of negative reputational occurrences on financial performance and the reputation of an organization. Her research however demonstrates the difficulty of measuring and identifying the "causal chain of events" (Gatzert, 2015, p. 495). Another scholar who studied reputational risk management in a more holistic manner is Bonime-Blanc (2016), as according to her it is a "risk management that requires the participation of public relations and a number of other key players and experts", and thus is not the same as public relations. She argues that it is also not similar to crisis management, as an organization is already too late managing their reputation if it waits until a crisis happens. She however stresses that organizations should take a proactive approach to reputational risk, and should incorporate this risk within the crisis management plan (Bonime-Blanc, 2014, p. 3). Additionally, she states that institutions need to have a proactive and holistic strategic approach towards reputational risks, which for example could be achieved by adding a Chief Integrity and Reputation Officer to their boards (Bonime-Blanc, 2017).

2.4 Literature review 'cyber risk'

2.4.1 Cyber security

The term cyber security is used to refer to a wide range of areas, such as "the integrity of our personal privacy online, to the security of our critical infrastructure, to electronic commerce, to military threats and to the protection of intellectual property" (Carr, 2016, p. 45). Academic literature on cyber security is broad and multidisciplinary, and includes, among many other things, national cyber security strategies, software- and firewall developments, public-private partnerships (PPP's), and discussions on privacy and data protection (Carr, 2016, pp. 45-46).

According to Lagazio, Sherif and Cushman, there exists a lack of consensus with regard to the "definitions, classifications, economic implications, security standards and solutions" of cybersecurity (Lagazio, Sherif, & Cushman, 2014, p. 59). Therefore, different approaches will be discussed. First a pragmatic approach is used by presenting the definition from the Dutch national perspective. The Dutch National Coordinator for Security and Counterterrorism defines cyber security in 2017 as "the entirety of measures to prevent damage caused by disruption, outage or misuse of IT and repair it should it occur. This damage could comprise impairing the availability, confidentiality or integrity of information systems and information services and information stored on them" (National Coordinator for Security and Counterterrorism, 2018, p. 51).

Furthermore, according Adams et al. cyber security includes different forms of security, such as information, computer, network, infrastructure protection and IT security. Consequently, their definition of cyber security is "the proactive and reactive processes working toward the ideal of being free from threats to the confidentiality, integrity, or availability of the computers, networks, and information that form part of, and together constitute, cyberspace – the conceptual space that affords digitized and networked human and organizational activities" (Adams, et al., 2015, p. 26). The perspective of Adams et al. is for a large part based on and in line with the perspectives of Van den Berg et al. (Berg, van den , et al., 2014), who argue that the term cyber security is a successor of the term information security, while it includes more business-oriented topics now, where information security focused on a more technical approach to cyber.

2.4.2 Cyber risk and cyber risk management

In order to build towards a working conceptualization of cyber risk, the definitions and approaches of various scholars are presented. The common and interchangeably used concepts such as 'cyber crime', 'cyber incident' and 'cyber attack' make defining cyber risk challenging. Conceptualization is difficult, as academics experience problems with defining what acts can be seen as 'cyber threats', and thus what exactly poses a risk (Johnson, 2015, pp. 132-135). In order to stress the complexity of interactions that happen in cyberspace, Jan van den Berg et al. added a socio-technical level above the technology level of cyberspace. According to this group of scholars, "cyber risks concern the IT-dependent risks all cyberspace actors in the various cyber dub-domains are exposed to when performing their (…) cyber activities." (Berg, van den , et al., 2014, p. 3).

According to Jan van den Berg et al., the incorporation of business-oriented issues in the standards of security has increased. They stress that topics as 'business continuity management' and 'compliance' are components of cyber risk management. Consequently, they define cyber-risk management as "a type of risk management that – complementary to the technical focus of information security risk management in the technical layer – focuses on the risks the [sic] have emerged in the socio-technical layer of cyberspace" (Berg, van den , et al., 2014, p. 3). Based on this definition, Adams et al. (2015, p. 22) argue that the concepts of cyber-risk management and cyber security can be used as synonyms. Elaborating on the definition of cyber risk put forward by Jan van den Berg et al. as presented in the previous section, it is argued that cyber incidents take place in the technical layer of cyber activities, although the actual impacts and risks of those are felt in socio-technical layer (Berg, van den , et al., 2014, p. 7). With specific regard to cyber risk management, the same scholars argued that "the cyber context in which the IT is used, is the starting point" (Berg, van den , et al., 2014, p. 3). With respect to this interpretation, Van den Berg et al. presented a model, seen in Figure 3, that demonstrates how different cyber threats can have impacts at different levels and amongst different parts of society: they do not just have technical impacts. Building on this way of reasoning, Van den Berg et al. separated cyber risk management also into different layers: a business, application and technology layer. They stress that the challenge lies in aligning the different actions and developments, as within these multiple layers "different groups of people are responsible for design and implementation" (Berg, van den , et al., 2014, p. 7).

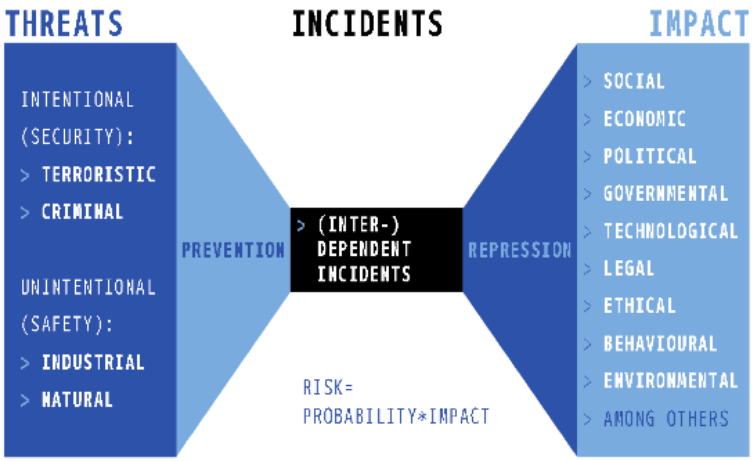

Figure 3: Cyberriskmanagement (Berg, van den, et al., 2014, p.3.)

Next to the perspectives of Van den Berg et al., according to Bonime-Blanc (Bonime-Blanc, Mitigating cyber-reputation risk, 2016) managing cyber risk is "a framework adopted within an organization to deal with the new and evolving risks relating to cyber space both within the organization and as the organization interfaces with the outside world. In this framework, the critical actors are the board, the C-suite or executive team, and frontline top management in charge of executing cyber-risk management." Key actors here are risks within the organization, as well as society and the outside world. This definition is visualized in figure 4.

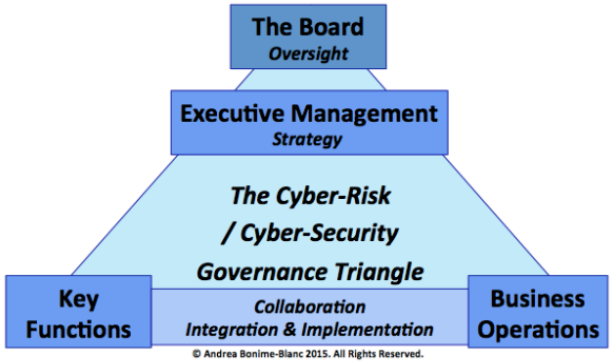

Figure 4 Cyber risk management framework(Bonime-Blanc, 2016)

Elaborating on this, Bonime-Blanc (2016) identifies five cyber risk management approaches: the Complacent Model, Irresponsible or Nonexistent Model, Vigilant Model, Integrated Model and the Command and Control Model, as presented in figure 5. The depended variables are the degree of cyber risk exposure, and the awareness and reactiveness of organizations' leaders.

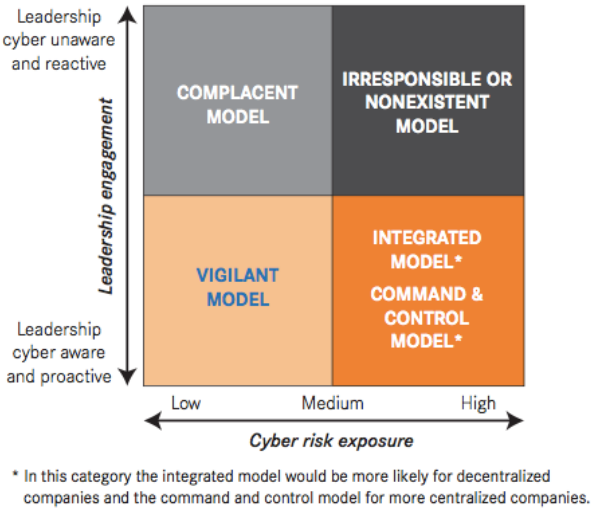

Figure 5 Cyber risk management models(Bonime-Blanc, 2016)

2.5 Cyber-reputational risk

Both the literature on cyber risk and reputational risk management do mention and identify 'each other' in their policies, models or frameworks as important examples, effects or drivers. Literature specifically focussing on linking the management and strategies of cyber and reputational risks seems absent, the theories and frameworks on cyber-reputational risk being underdeveloped (Lagazio, Sherif, & Cushman, 2014, p. 59). In the absence of such a comprehensive theory or framework, first a brief overview will be given on scholars who integrate both risks to only a certain extent.

Examples are the Situational Crisis Communication Theory (SCCT) by Coombs (2007) and a multi-level model, focused on understanding the impact of cyber crime in the financial sector, by Lagazio, Sherif and Cushman (2014). The former is an example out of several researches that discuss how cyber security attacks can influence the reputation of a company. Most of these researches have a marketing or communications approach towards reputation. The SCCT provides organizations a framework on how different factors in the aftermath of a crisis can influence their reputational risk (Coombs, 2007). Within this framework, a cyber security attack, as a result of a dysfunctional cyber security system, functions as an example or a driver for a reputational crisis. Contrastingly, the latter model, researching the impact of cyber crime in the financial sector, mentions that cyber crimes can have 'implicit costs', such as reputational damage. Subsequently, this (damaged) reputation can cause financial losses (Lagazio, Sherif, & Cushman, 2014, p. 60). Another example is the framework created by Fiordelisi, Soana & Schwizer on the reputational losses and operational risk in banking. In their article they created a model for estimating the reputational impact of operational losses of firms in the financial sector. Here, cyber security is identified only as one of many causes for these operational losses. For example, failures in technology could result in disturbed balance sheets (Fiordelisi, Soana, & Schwizer, 2012, p. 106).

An important scholar who does explain the relation between cyber and reputational risk more clearly and who treats cyber-reputational risk management as a 'single' concept is Bonime-Blanc (2016). According to her, managing cyber-reputation risk is a team effort. In order to effectively govern cyber-reputation risks, cross-disciplinary and cross-segmental input is desired. Therefore, all departments, experts and business units within a firm should cooperate before, during and after a cyber-reputation risk incident in order to be able to create an effective defence strategy for the long-term resilience that is needed to manage these strategic risks.

In other articles (Bonime-Blanc, 2014), she also clearly puts ‘cyber risk’ as part of ‘reputational risk’, but unfortunately does not offer a concise explanation, concrete components or a framework on how these two risks relate. Moreover, since reputational risk and cyber risks are both strategic risks, they are ideally the responsibility of the highest executive levels of an organization (Bonime-Blanc, 2016).

2.6 Summary and conceptual framework

The theoretical framework demonstrated that ‘cyber’, ‘reputation’ and ‘risk’ are so-called ‘blurred’ concepts that can be interpreted in different ways. Combining and integrating those blurred concepts – cyber-reputational risk - potentially yields a concept that is even more blurred. Therefore, this section will conceptualise and set out the most important takeaways of cyber risk and reputational risk. In this way a background will be provided against which the overview of cyber and reputational risk management techniques in the financial sector in the following chapters can be analysed and understood. First, the literature on risk demonstrated that risk (management) itself is complex. Second, an important discussion was presented on the very nature of reputational risk, whether it is no risk itself, a self-standing or a “risk of a risk”. For this research the position lays between the latter two positions as reputational risk is treated as a self-standing risk, but it is clearly recognized that it is also a risk of other risks. Furthermore, the literature on the management of reputational risk management stressed that next to the public relations departments, also the participation of other key players and experts is desired. Fourth, Adams argued that cyber security and cyber risks could be used as synonyms in certain circumstances. Also, it was presented by Van den Berg et al. that apart from the technical side, cyber activities have a socio-technical layer. Even more, Bonime-Blanc demonstrated different models of cyber risk(management). Finally, with regard to cyber-reputation risk it is important to note that all departments, experts and business units within a firm should cooperate before, during and after a cyber-reputation risk incident. Against this background, the data analysis framework, to be presented in the following chapter, will be derived.

3 Methodology

3.1 Introduction

This chapter sets out the methodology that is used in this research. To begin with, the research design will be presented. Identifying the selected data collection methods and data analysis will follow this. Subsequently, the internal and external validation and reliability will be elaborated. Finally, the organization of the thesis will be discussed.

3.2 Research design

According to the research strategy selection criteria of Yin (2009, p. 1) a case study design is recommended when "when "how" or "why" questions are being posed, when the investigator has little control over events, and when the focus is on a contemporary phenomenon within some real-life context." For this research the main research question is a "how" question, there is little control over the events being studied, and the contemporary situation of cyber and reputational risk in the financial sector is evaluated. Therefore, based on the research strategy selection criteria put forward by Yin, a case study is chosen as the appropriate strategy for this research. Even more, especially as the boundaries between the phenomenon of study - management strategies concerning cyber and reputation - and the context - a post-financial crisis sector environment with technological developments – are not precisely clear, it is in line with Yin's line of arguing for choosing a case study (Yin, 2009, p. 13). Furthermore, "illuminate a *decision* or set of decisions and how they were implemented" (Yin, Case Study Research: Design and Methods, 2009, p. 14) is consistent with the objectives of this study: as addressed in the previous chapter: risks are dependent on decisions being made. He further argues that a case study can have complementary purposes, so that they can be both explanatory and exploratory (Yin, 2009, p. 1). This is the case for this research as on the one hand, it aims to explore new conceptualisations and develop relevant suggestions for further research (Yin, 2009, p. 10). Next to that, however, the research intents to provide explanations between the phenomenon, different risk concepts in this case, and their context (Yin, 2009, p. 6).

The theoretical framework in the previous chapter demonstrated that no set-(qualitative) framework exists to study the relation between two relatively complex, new and broad risks. This research consequently also does not entail a standard and simple methodological framework.

The case study of this research is therefore based on the broader definition of a "case" by Merriam (2009, pp. 40-41), who emphasized that to make a study a case study, the phenomenon to be studied should have a bounded context. For this, one specific part of the worldwide financial sector is studied, with two specific risks– cyber and reputational risks – which makes it a bounded context. For this research, two different subjects – cyber and reputation - are studied to investigate the relation between cyber- and reputational risk, but within the same real life context of the financial sector. For this, the focus the case of the financial sector is studied, is zoomed in on the case of the Netherlands. The examination of global nature of this, makes this research suitable for a holistic design, which enables to derive multiple conclusions. As was discussed in the introductory chapter, the time frame is the post-crisis era. However, due to feasibility and time constraints and in order to make the study as contemporary as possible, the focus is on 2017 and 2018, as not all data from 2018 is available at this point in time.

3.3 Methods of data collection

This research aims to study the integration of two different risk strategies, whereby the collected data needs to be interpreted and contextualised within the real-world setting of the financial sector in the Netherlands. Therefore, a qualitative research methodology is chosen for this research, which is in line with the argumentation Yin (2011, pp. 8-9) describes in his book "Qualitative Research from Start to Finish". Yin also recommends the use of qualitative research methods when the subject of study is complex, and the collection and integration of multiple sources of data are needed for the research. These requirements are met in this research, due to the complexity of the Dutch financial-sector field in general, and even more that of cyber- and reputational risk as was put forward in the previous chapter. Even more, qualitative research methodology can provide a holistic interpretation of how is dealt with cyber risk as reputational risk by Dutch financial institutions Merriam (2009, p. 244). The unit of analysis of this research is the financial sector as a whole, with a focus on financial institutions in the Netherlands. For this, the financial institutions are being observed in different ways: policy and strategy documents, surveys that have been conducted. Interviewing professionals who are specialists on cyber and/or reputational risk topics, and who are able to present a comprehensive and as objective as possible view on the Dutch financial sector, seemed most suitable for this research.

Different methods, using both primary and secondary data, will be used for the data gathering in order to create data triangulation. The first method is the desk research of relevant policy documents and reports. This method is twofold: primary data from financial institutions themselves, and second, secondary data stemming from researches and surveys that have been conducted. Second, semi-structured interviews will be conducted with professionals who worked. This data can crosscheck each other.

3.3.1 Desk research

The first research technique is desk research, which enables a researcher to collect existing data without conducting fieldwork (Johnston, 2014, p. 619). For this desk research, the content of two different types of data will be analysed. The first method is the content analysis of primary, open source documents from financial institutions. These documents stem from the most important Dutch financial institutions themselves such as ING, ABN AMRO and Rabobank, and oversight bodies such as the Dutch Central Bank (De Nederlandsche Bank (DNB), the European Central Bank (ECB) and the Dutch Authority for the Financial Markets (Autoriteit Financiële Markten (AFM). Examples are policy statements and (annual) reports on overall risk strategies. The goal is to give a reliable first-hand insight of the strategies and risk management frameworks are used, according to the financial institutions themselves. The findings of this research technique can be used to confirm or further explain statements made by interviewees, or the other way around. It helps to explain cyber threats and cyber risks in the financial sector, and the functioning and perception of reputation and reputational risk management.

The second technique is the content analysis of publicly accessible secondary data. This data includes existing studies, reports and the results of surveys. For this method of desk research publicly accessible academic articles, reports and surveys conducted by governments and consultancy/advisory firms and the press will be analysed. The goal of applying this technique is to supplement or support the findings extracted from the primary data and interviews. Additionally, surveys or reports are able to provide quantitative support will be provided as well in order to underscore statements.

3.3.1 Interviews

The second method is conducting semi-structured interviews. Semi-structured interviews enable a researcher to get a rich and in-depth understanding of a certain topic, as a result of reciprocity with the interviewee and the possibility to ask follow-up questions.

The open questions that are asked during the semi-structured interviews are however more difficult to analyse compared to strictly structured interviews (Kallio, Pietilä, Johnson, & Kangasniemi, 2016, p. 2955). The objective of conducting interviews is to present an on comprehensive, objective view on how financial institutions deal with cyber and reputational risk and support the findings made by the desk research, or propose new findings. Therefore, it is important to conduct the interviews with professionals who do have considerable knowledge on the Dutch financial sector as a whole, and have access to relevant internal information of financial institutions. As most financial institutions lack the resources to tackle cyber and reputational issues on their own, they have outsourced a lot of work to third parties such as PwC (PwC, 2014, p. 16). The advantage of specifically this target group and relying on the experience and perceptions of specialists/consultants is that these persons are working for multiple Dutch financial institutions. Moreover, within this context they are expected to be more objective than professionals who are employed directly by the financial institutions themselves. The target group for the interviews was consequently based on the selection criteria of contemporary knowledge based on long-time experience and current experience in the Dutch financial sector. In total five interviewees were selected. An overview of the planning of the interviewees can be found in Annex 1. Given the nature of the main research question, the selected interviewees were two specialists in cyber security, two in risk management, and ultimately one who is specialised in both cyber security and risk management.

During the semi-structured interviews, the initial focus will be on factual questions, addressing and combining their detailed knowledge the specialists experienced with current and former clients they have worked for. Attention will be paid to the personal perceptions of the interviewees on, for example, what incidents the institutions they worked for experienced and how they managed a cyber-attack or reputational crisis. Eight pre-set questions will be prepared in advance of each interview, and will be asked to all five respondents. An overview of the interview questions can be found in Annex 2. However, specific follow-up questions either depend on the previous answers given by the interviewee, or be adjusted to the expertise and position of the respective interviewees. The interviews will be transcribed, however due to confidentiality reasons and in order to guarantee the anonymity of the interviewees, the interviewees will be referred to as “Specialist 1”, Specialist 2” etc.

3.4 Data analysis

The collected data will be analysed through the method of content analysis. Content analysis is the form that is most often used in qualitative research as it allows researchers to "analyse relatively unstructured data in view of the meanings, symbolic qualities, and expressive contents they have" (Krippendorff, 2004, p. 144). This will be done by creating indicators based on the conceptual framework presented in section 2.6 of the previous chapter. The theoretical framework in the previous chapter demonstrated that the concepts were broad, blurred that are difficult to define. Moreover, it showed that no set way to evaluate and explore or comprehensive integrated framework on cyber-reputational risk management was found in the existing literature. The literature review however emphasizes the importance of certain conceptualizations. Accordingly, these conceptualizations will form the basis for that analysis of the research findings. By making this selection of conceptualizations it is not argued that other literature is irrelevant, however focus on these concepts were found most suitable and fit this research the most.

Given the nature of the main research question, this research endeavours to find out how cyber risks are used as reputational risk. In order to answer the "how", means that in the analysis, the nature, perception and implementation of both risks have to be studied again. Therefore, the findings in the theoretical framework serve as a background, but are not a set-guide. This research is mainly inductive, for which the exploratory mode of data analysis is used. This mode of analysis focuses on exploring and recognizing phenomena and patterns in data (Jebb, Parrigon, & Eun Whoo, 2017, p. 267). Here is also where the more explanatory part of the research starts. For both cyber risks and reputational risk there is a focus on analysing the perception of the concept, the functioning and relevance of it within the financial sector, examples of incidents or crises, and the management and the incorporation of it within the whole operational risk strategy of financial institutions. In the absence of an existing theoretical framework that is found suited for this research, the data will be analysed through the following concepts.

- Reputational risk: Perception and nature: what encompasses a risk? Indicators are no risk at all, a 'risk of risk' or a specific, self-standing risk, a strategic risk, awareness and resources within the organisation;
- Cyber risk: Perception: what encompasses a risk: socio-technical and technical layer. Nature: no risk at all, a 'risk of risk' or a specific, self-standing risk, a strategic risk, awareness and resources within the organisation;

- Cyber-reputational risk: incorporation of departments, all layers.

The complete analysis scheme can be found in Annex 3.

Next to the previously presented themes and indicators, the analysis of the data will also rely on research on so-called 'emergent' indicators. The "how" part of the main research question asks for concrete answers, explanations, examples and parallels. Therefore, it would be premature and subjective to entirely rely on the-pre-set concepts. Emergent indicators and the utilization of "quotes" for analyzing the interview data are therefore also utilized in this research when unexpected variables are identified who clearly specify the perception of cyber- or reputational risks, or the relation between them.

3.4.1 Internal validity

Using "multiple sources of data means comparing and crosschecking data collected through observations at different times or in different places, or interview data collected from people with different perspectives" is a powerful strategy for increasing the credibility or internal validity of your research" (Merriam, 2009, p. 245). In order to increase the internal validity of this research by means of data triangulation and get more comprehensive views and insights on cyber- and reputation strategies, two methods of data collection will be conducted. As previously discussed, these two methods are desk research and document analysis, and in-depth interviews. In this way, the situation of the financial sector will be viewed from different standpoints, linking context and phenomenon as discussed in section 1.1 of this chapter. By using different methods as well as different sources, it is aimed to get a reliable broad and general view as the empirical results as they can assist, confirm, possibly contest, and supplement each other. For example, the data gathered from desk research can further explain certain concepts as mentioned by the interviewees, while interviewees can give specific examples or provide a more realistic view on the issues at hand based on their own professional work experience. For example, the internal validity increases when the perceptions of an interviewed specialist can be crosschecked by primary sources of banks or reports. Furthermore, internal validity is increased by consistently conducting the analysis.

3.4.2 External validity

Case study researches raise questions with as to what extent its findings are generalizable (Platt, 1992, p. 23). As this research focuses on the Dutch financial sector, the external validity of it is compromised, as certain characteristics such as national regulations and supervision or political developments, are only applicable to financial institutions based in the Netherlands. However, the external validity is still relatively high due to several reasons.

Even though the case of the Netherlands has its uniqueness, many financial institutions in other parts of the world do not only face similar challenges, they also have comparable organizational structures that operate within similar societal contexts. This is especially the case in the EU, where member states have comparable financial markets because of EU regulations (Wetenschappelijke Raad voor het Regeringsbeleid, 2016, p. 184). Additionally, according to the Dutch central bank, “many risks have a cross-border character” (De Nederlandsche Bank, sd). This is even more the case as Dutch financial institutions also operate across borders; as was explained in the introductory chapter, they have a considerable share of the EU financial market.

4 Analysis

4.1 Introduction

Elaborating on the conceptualization as discussed in the theoretical and further elaborated in the methodological framework, this chapter aims to find an answer to the main research question. This will be done by the analysis of the research findings and subsequently formulating answers to the two sub-questions that were posed in the first chapter of this research. By means of the data collection and analysis techniques as discussed in the previous chapter. First, the context of the Dutch financial sector will be elaborated. Further understanding of the bigger context in which financial institutions deal with reputational and cyber risks will help to understand the relationship between both risks. The third part of this chapter focuses on how financial institutions deal with reputational risk. Subsequently, the fourth part of this chapter studies how cyber risks are dealt with. The final part of this chapter consists of a discussion on the findings of this chapter.

4.2 The Dutch financial sector

The financial sector in the Netherlands experienced a rapid growth since the 1980's and its influence on the economy and Dutch society as a whole has strongly increased. (Wetenschappelijke Raad voor het Regeringsbeleid, 2016, p. 7). Financial institutions are a core part of Dutch society for the governments, companies and citizens. This can be illustrated by the fact that citizens are dependent on financial products for many important aspects of their daily lives; in order to receive salary, to buy food, to get a mortgage or to have an insurance (Specialist 5, 2018). From being a facilitator, the sector acquired a leading position within Dutch society. This makes the economy and society very vulnerable to any financial disruptions or instability, and consequently makes the financial sector part of socioeconomic policy. Even more, the failure of certain processes within the financial sector may cause social disruption and pose a threat to national security (Dutch National Coordinator for Security and Counterterrorism, 2018). Many actors, including the financial institutions themselves, are making strong efforts to create more stability and reduce the risks of the financial sector. Particularly since the financial crisis in 2008, the Dutch government expressed its concerns and critiques on the policies and behavior of financial institutions, and stressed the need for reforms in the financial sector.

The strengthening of interests and negotiating position of customers have to become a central part within this reforms, while improving the supervision of financial institutions. By imposing more regulatory requirements and legislation for, and supervision of financial institutions in the past decade, they are attempting to improve society's resilience to financial disruptions (Wetenschappelijke Raad voor het Regeringsbeleid, 2016, pp. 7-11).

According to the AFM (2019, pp. 4-5), current trends within the Dutch financial sector are the central role it has in the sustainability-transition of the economy and society, and the geopolitical risks the approaching Brexit brings along. Third, and most relevant for this research, are the risks that arise as a result of the financial sector's persistent digitalisation and innovation, such as the growth of so-called 'fintech' applications.

The Dutch financial sector consists of many different financial institutions that provide a varied range of financial services, and are supervised by the Dutch Central Bank (De Nederlandsche Bank (DNB), the European Central Bank (ECB) and the Dutch Authority for the Financial Markets (Autoriteit Financiële Markten (AFM). The financial regulatory framework of the Netherlands is for a considerable part derived from EU legislation. The most important institutions that provide financial services in the Netherlands are banks, insurers, investments- and pension funds (The Dutch Authority for the Financial Markets, 2017). As was already discussed in the introductory chapter, the Dutch financial market is highly concentrated. Banks, and especially the 'big three' Rabobank, ING and ABN AMRO take a dominant place within the sector. The combined share of the three big banks – ING, Rabobank and ABN AMRO - is very large: in 2017 they accounted for 84% of the balance sheet total (Banken.nl, 2018). Even though no "one size fits all" for all banks or financial institutions exists, within this analysis emphasizing is put on these three banks, as they represent and account for a relatively large part of the entire Dutch financial sector.

4.3 Reputational risk in the financial sector

4.3.1 Introduction

This section of the analysis chapter aims to understand how reputational risk is integrated within the financial-services sector. It will answer the sub-question *"How do financial institutions in the Netherlands perceive and deal with reputational risk?"* by means of different sections. After discussing different perspectives in the academic literature on reputation and reputational risk, the next section will demonstrate how Dutch financial institutions *perceive* reputation and reputational risk. Understanding this perception will help to further contextualize the results presented in the sections that follow.

Following this, examples of reputational incidents will be presented in order to illustrate and further understand the functioning of reputational risk. Hereafter, the management of reputational risk will be discussed. Finally, a sub-conclusion will be drawn, will serve as the main foundation for the discussion at the end of this chapter.

4.3.2 Perceptions of reputation and reputational risk

Elaborating on the discussion within the previous section, a trustworthy and reliable financial system is of key importance. Therefore, also the government requires the careful management of any reputational risk, because it can harm the stability of the financial system (Specialist 4, 2018). According to the Dutch government, "financial institutions must have an immaculate reputation. Otherwise, consumers and entrepreneurs lose confidence in the financial sector" (Rijksoverheid, n.d.). It however are not just governmental bodies who stress the importance and relevance of reputation; all specialists that were interviewed for this research confirmed that financial institutions are very much aware of their reputation and potential reputational damage. Within the financial-services sector, firms' perception of reputation is best to be defined as 'trust' (Specialist 3, 2018). This focus on trust is confirmed by studies conducted in the financial sector (Fiordelisi, Soana, & Schwizer, 2012, p. 105). One the one hand, this trust or reputation is for a large part based on the healthiness, solvency and liquidity of the firm. This can for example be seen at ABN AMRO, who states that its liquidity risk management "safeguards ABN AMRO's reputation" (2017, p. 66). Solvency of financial institutions raises questions such as whether a firm can meet its financial obligations and stay in business. Healthy financial institutions are eventually in the interest of society as a whole. On the other hand, the reputation of a firm is also strongly related to its mission statement and identity (Specialist 4, 2018). Consequently, the more a certain incident or problem is related to the core identity of a firm, the higher the reputational risk. For example, huge reputational damage that affects investors' trust most, is when core values are being attacked; the reputation of a bank focusing on environmental sustainability will suffer from a scandal with investments in environment-harming processes (Specialist 4, 2018). What can be seen in the mission statements of different Dutch financial institutions is mayor attention to society and centralization of people: **"**Growing a better world together*"* (Rabobank, 2017, p. 2), "Empowering people to stay a step ahead in life and in business" (ING, 2017, p. 3) and "Banking for better, for generations to come" (ABN AMRO, 2017).

Building on this, it can be stated that reputation is part of the entire strategy of financial institutions because in essence, every department's work is aimed at the realisation of the mission of the entire organisation (Specialist 5, 2018). The importance of reputation within their entire strategy can be confirmed by the amount of times the word 'reputation' is mentioned in the annual reports of 2017 of the three biggest financial institutions in the Netherlands. ING (2017) mentioned it 42 times, ABN AMRO (2017) 12 times and Rabobank (2017). However, it is important to note here that most times the word 'reputation' was not specifically linked to 'risk'. For example, as can be seen in figure 6, reputational risk is not seen as a 'major risk type' by ABN AMRO, but as one of several 'other risks'

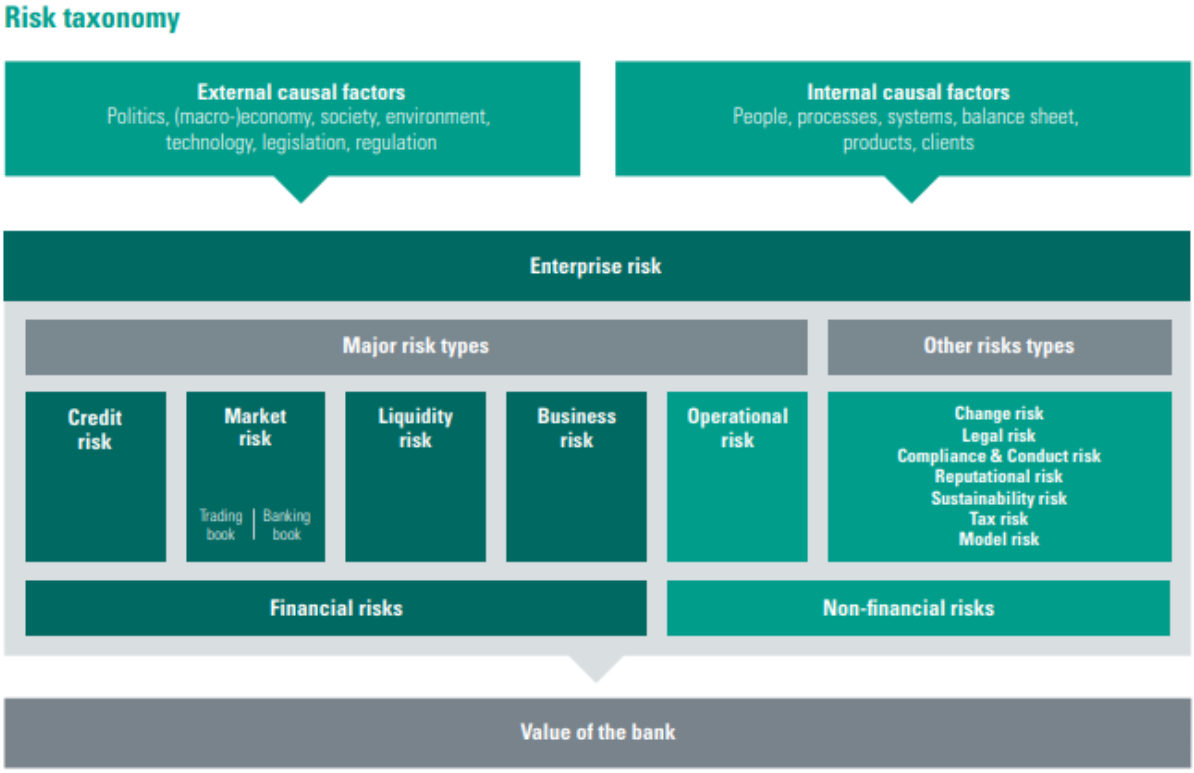

Figure 6 ABN AMRO Risk taxamony (ABN AMRO, 2017, p. 48)

A similar thing can be seen at ING, as it places reputational risk under its non-financial, operational risk category. Interestingly, it also explicitly states that strategic risks are not included within this operational risk category (ING, 2017, p. 193), from which could be concluded that it does not perceive reputational risk as a strategic risk. This is in contrast with the statement by Bonime-Blanc (2017, p. 49) that reputational risk is a strategic risk, as was presented in the theoretical framework of this research.

ING however does specifically define reputational risk in its annual report*:* "Reputational risk is defined as the possibility that adverse publicity regarding ING's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of ING. Reputational risk is multidimensional and reflects the perception of other market participants, like customers, counterparties, shareholders, investors or regulators that can adversely affect ING's ability to maintain existing, or establish new, business relationships and continued access to sources of funding*"* (ING, 2017, p. 193). Interesting here is the focus on negative consequences reputational risk potentially has, contrasting to the definitions presented by Renn (2005, p. 19) on risk in general, and Bonime-Blanc (2017, p. 42) on reputational risk specifically, who argue that consequences can be both positive and negative. Similar to ING, Rabobank, as it includes reputational risk, along other risks such as legal risks, under its overall operational risk. It does not present a definition of reputational risk (Rabobank, 2017, p. 199). This can be explained by the fact that within the Dutch financial sector reputational risk is perceived as "the consequence of other risks materialising" (Specialist 4, 2018).

Within the financial sector, apart from the influence of social media and technological developments on reputational risk, many things have changed. In the 'Trust Barometer of Edelman' the public opinion on bankers is extremely low (Specialist 4, 2018). Even though reports from the past years, such as the "Vision on the structure of the Dutch banking sector" (De Nederlandsche Bank, 2015) demonstrate that society in general does not have a lot of trust in the financial sector, it is also valuable to present contrasting data. This public opinion on banks in general has changed over the years through a series of events. Some of these events or will be discussed in the next section of this chapter.

4.3.3 Reputational crises

In fact, no better example of a reputational crisis in the financial sector in the Netherlands is the so-called financial crisis that started around 2007, and particularly affected the financial sector. The crisis had, and still has, mayor impacts on the entire sector. (Specialist 3, 2018). As was discussed in the first section of this chapter, it led to more regulations and society's distrust towards the sector (Wetenschappelijke Raad voor het Regeringsbeleid, 2016). By means of illustration and further understanding the functioning of reputational risk in the Dutch financial sector, three specific examples of reputational incidents will be discussed.

To begin with, the above-discussed financial crisis will be made bit more concrete by giving an example with direct consequences for the respective financial firm.

The Dutch DSB Bank went bankrupt in 2009 because, rather simply put, all its clients simultaneously withdrew their money. This client-behavior was based on 'rumors' about the solvency of DSB Bank. In other words, the reputation of DSB Bank as a healthy, solvent firm was damaged (Specialist 1, 2018).

Another example is the public announcement made by ING Bank in 2014, when it announced that it would make its client-data available for commercial purposes (Specialist 3, 2018). What followed was a lot of negative media attention, including newspaper headlines saying 'ING is selling client data', critique from the director of the Dutch Central Bank of the Netherlands, national politics, and the Dutch Authority for the Financial Markets (Spelier, 2014). According to a survey filled out by 27.500 persons, almost 80% of ING customers indicated their trust in ING heavily decreased following the announcement. Even more, 30% of them said they were actually considering leaving ING (Radar, 2014). On the one hand, with regard to direct consequences concerning its customers, even many people indicated switching banks, only a few of them actually did. So in that sense there were not a lot of consequences. On the other hand, it had considerable impact within ING in other terms and they also withdrew the initiative (Specialist 4, 2018). Next to the impact within ING, it also had its fallout in the whole sector and you still see that today. This event changed the attitude of many people towards the financial sector as a whole and it heavily affected the way that banks deal with client-data; they are more careful and reluctant sharing data (Specialist 3, 2018).

Another example of a reputational 'crisis' that coincidently concerns the same bank happened in the beginning of 2018, when ING Bank proposed the salary raise of its CEO. As a reaction, it received a lot of critique and negative media attention. As a result, ING withdraw (NOS, 2018). What the additional, indirect and long-term effects with regard to the reputation of this so-called 'salary scandal' will be is hard to tell at this point, however it is expected not to cause ING enormous financial losses (Specialist 4, 2018). This can be explained by the fact that, according to ING's own 'Investors Barometer', even though trust was damaged in the months of March and April, this trust was regained in May (ING, 2018). The media were talking about a 'gate' and 'scandal' and ING's reputation was damaged, nevertheless, the direct short-term effect is that it barely lost any clients due to this event. Moreover, it was reported that its net profit increased in May 2018 (IEX, 2018). Moreover, ING was put amongst the top 12 out of 500 companies with the best reputation in the Netherlands based on the criteria product leadership, customer orientation, employer and execution excellency (Management Team, 2018).

This is an interesting finding, as it contrasts findings of earlier conducted studies. For example, Fiordelisi, Soana and Schwizer (2012, p. 107) argue that large operational losses in the financial sector are also followed by increased reputational losses.

4.3.4 Reputational risk management

Even though reputation is related to the entire strategies and thus indirectly with all departments of financial institutions, reputational risk management is not an explicit part of these strategies (Specialist 4, 2018). The findings presented in section 4.3.2 demonstrate that reputation is incorporated within the overall (operational) risk management of Dutch financial institutions, but financial institutions however do not deal with reputational risk itself in an overarching, comprehensive structured manner (Specialist 5, 2018). Indeed, reputational risk is a tiny portion of the bigger picture of risk management (Specialist 5, 2018) Apart from being part of other risk frameworks, they do not have a specific reputation-risk management framework (Specialist 2, 2018). Obviously, institutions do have certain procedures in place. For example, employees are not allowed to talk with the press in case of an incident of the financial institution they work for (Specialist 2, 2018).

Given the missing specific reputation-risk management framework, it consequently is also difficult to identify and formulate a concise answer on who structurally deals with reputational risk issues within the financial institutions. Next to that, the different respondents posed contrasting answers to this question, and the reports of the three biggest financial institutions in the Netherlands presented contrasting issues as well. Normally, it are the public relations and marketing departments that deal with reputational issues in a pro-active way (Specialist 3). However, for example, ABN AMRO on the one hand treats reputational risk at the compliance and audit department, as it afraid to lose money and the accompanied reputational damage resulting from non-compliance, for example fines from regulators (ABN AMRO, 2017). On the other hand, within ABN AMRO (2017, p. 40) reputational risk management is most likely the responsibility of the "Transformation & HR" department, since this department "aims to prevent reputational damage and services to manage and improve the Group's reputation, brand name and brand value (…) as a trustworthy and sustainable organisation". With regard to the organizational context of ABN AMRO, it is thus not precisely clear where reputational risk is exactly put.

Also, elaborating on the second example of the previous section on the reputational incident at ING concerning client data, this issue was initially dealt with at the highest levels of the marketing department, which can be seen in the fact that ING's Marketing Director of the time made the announcement that it would use client data for commercial purposes (Specialist 4, 2018). At that point, and based on the obvious miscalculations ING made on the potential reputational damage of this announcement, it was probably not dealt with at the operational risk department, under which reputational risk is placed (ING, 2017, p. 194). Ultimately, this reputational incident was dealt with by the Board, the highest level of ING. The higher the potential financial loss or the bigger the calculated reputational damage, the higher the organizational level the issue is dealt with (Specialist 5, 2018).

This has also to do with the different nature different reputational threats can have. So when a certain error or incident occurs, obviously the responsible business line will deal with the issue. For instance, a legal breach that might harm the reputation of a financial institution, will be first and foremost dealt with by the legal department. This is a relevant example of how reputational risks specifically are often only used during or afterwards a scandal or crisis. This has to do with the nature of the threat and the size of the financial loss (Specialist 4, 2018). Ultimately, reputational risk is managed by the compliance department, as it is largely focussed on preventing misbehaviour. For example, before a financial institution sends out letters to their clients the message is being checked by the compliance department (Specialist 4, 2018).

4.3.5 Sub- discussion

It can be concluded that the most significant takeaway from this sub-chapter on the integration of reputational risk, when looking at the nature of risk as discussed in the theoretical framework of this thesis, reputational risk is to a large extent perceived as a 'risk of a risk' within the Dutch financial sector. This also explains why no comprehensive reputational risk management framework is used, and it consequently explains why the part reputational risk is found at different organizational parts within the institutions. An important explanation for this 'risk of a risk' can be more of textual nature, as inconsistencies seem present with regard to terminology on reputational risk, which for example make it difficult to decide, for example, which part of resources is allocated to reputational risk specifically. In that line of reasoning, if could even be argued that albeit the institutions mention reputational risk as a specific risk within their reports, they do not even recognize it as a risk itself, but a result of other developments coming together.

Altogether, this is in line with the statements made by Bonime-Blanc in the theoretical framework, as Bonime-Blanc states that in many organizations, the very existence of reputational risk is not doubted, however "the lack of a way to think about it in a structured manner: in other words, how to accurately identify and quantify reputation risk" (Bonime-Blanc, 2017).

An emergent factor or variable as a result of the findings of this analysis could be the involvement of 'publicity': the example of ING demonstrates that the issue of commercializing client data was not seen as a reputational risk yet before ING received negative publicity. Only when negative publicity emerged, it became a reputational risk. Moreover, the key role of publicity is also reflected in ING's definition of reputational risk. As a result, publicity can be seen as a key variable and decrement to whether something is dealt with as a reputational risk. This is not a strange conclusion, given the central role financial institutions give to the perception of their stakeholders. This central position of stakeholders is in accordance with the different definitions on reputational risk presented in the theoretical framework. This perception is influenced by the things they hear and read in the media; or 'publicity'.

The fact that the costs or expenses on reputational risk are not explicitly found within the financial statements of the annual reports (ABN AMRO, 2017; ING, 2017; Rabobank, 2017) of the three biggest banks confirms that reputational risk is seen as a 'non financial' risk. This confirms that financial institutions seem to face difficulties with measuring and quantifying their reputational damage and risks. This can be linked to the difficulties with the causal chain of events Gatzert (2015, p. 495) encountered in her research on the impact of reputational risk on financial performance, as well.

The above presents two examples of crises that caused the respective financial firm a lot of attention from the stakeholders. According to the statements made in the theoretical framework, an organization's reputation is dependent on the perception of its stakeholders. The remarkable element when looking at the cases of ING, is that regardless its perceived reputational damage, it is still perceived as a trustworthy bank and above all, even increased its market share following several crises. This raises question on whether reputational risk is actually even relevant or important for financial institutions in the Netherlands. Even though it would be premature to draw any conclusions, it would be interesting to further investigate whether the former has something to do with the high concentration ratio of financial institutions of the Netherlands, or whether reputational risk is only really relevant when the stakeholders and investors, instead of citizens, are involved?

4.4 Cyber Risk in the Financial Sector

4.4.1 Introduction

This part of the analysis chapter aims to provide a clear overview on how cyber risks are perceived and integrated within the financial-services sector. To be able to formulate an answer to the sub-question *"How do financial institutions in the Netherlands perceive and deal with cyber risks?",* this part of the analysis is divided into five sections. First, the cyber landscape for Dutch financial institutions will be elaborated. This will be followed by the discussion of examples of cyber threats and incidents in the Netherlands. Third, it will be analysed how cyber risks are perceived by financial institutions in the Netherlands. Understanding this perception is necessary to further contextualize the findings of the other sections. Fourth, the financial sector's management structure of cyber risks will be analysed. Lastly, a sub-discussion will be presented against the concepts and indicators presented in the methodology chapter of this research.

4.4.2 Cyber landscape

Financial institutions in the Netherlands are currently in the process of what can be called a digital transformation journey. Within their reports the largest banks in the Netherlands explicitly state they are in a "digital transition" (Rabobank, 2017, p. 3), a digital transformation (ING, 2017, p. 64) and ABN AMRO (2017, p. 9) focus on "digitalisation and financial innovation" which in all cases includes the introduction of new, innovative services. This means that institutions are aiming for "less office, and more apps and digital services" (Specialist 5, 2018). According to Sergio Hernando, responsible for cyber within the Financial Services Group of PwC Amsterdam, such a digital transformation means that "engagement models between financial organisations and clients are changing rapidly. For clients, trust provided by cyber security and privacy measures is instrumental in choosing their providers" (PwC, n.d.). Next to opportunities, all previously discussed institutions however agree within their reports that the digitalisation of financial services also brings risks. The sector is consequently also forced to transform its information security management to the new trends and build new cyber security strategies (Specialist 5, 2018). Especially since the financial sector in the Netherlands is experiencing high exposure to cyber risks. The current threats to the cyber security of the Dutch financial sector are next to cybercriminals, state actors who are attempting to infiltrate in or disrupt the critical infrastructure of the financial sector (National Coordinator for Security and Counterterrorism, 2018).

The Bureau for Economic Policy Analysis however emphasizes that compared to other countries, Dutch financial institutions have undertaken extensive cyber security measures in order to mitigate cyber risks (CPB, 2018).

4.4.3 Perceptions of cyber risks

To begin with, and following on the digital transformation that was discussed in the previous section, it can be observed that many financial institutions use the possibilities cyberspace offers as an asset, for example to expand markets. Examples are ING's numerous investments in the past years in so-called fintech partnerships (ING, 2017) and new innovations, such as the popular payment application 'Tikkie' introduced by ABN AMRO (ABN AMRO, 2017, p. 26). Referring to the fact that digitalization or cyber is used as an asset, the accompanied cyber risks are nevertheless perceived differently. According to the definition of Renn (2005, p. 19) as presented in the theoretical framework, risk can either have positive or negative consequences. The former examples can be seen here as the 'positive consequences' of cyber risks. Nonetheless, the focus within the cyber risks management frameworks of the financial institutions is on the prevention of cyber-attacks, and thus on the negative consequences of cyber risks.

In light of the cyber threats by criminals and state actors, and the influential role financial institutions within society, as was discussed previously in this chapter, financial institutions are seriously aware of current cyber risks (Specialist 5, 2018). This can also be seen in the annual reports of the three biggest Dutch banks; many times these institutions link words such as 'digitalization', 'data' and 'online services' to words such as 'protection' and 'security 'and 'compliance' (ABN AMRO, 2017; ING, 2017; Rabobank, 2017). Financial institutions are thus well aware of the importance of their cyber security (Specialist 3, 2018), especially because the firms in the financial sector have more regulatory controls than companies in other sectors. Through non-compliance with regulatory controls, such as the recent General Data Protection Regulation (GDPR), firms could be subject to enormous fines and thus lose large amounts of money (Fiordelisi, Soana, & Schwizer, 2012, p. 114). Research by financial firms themselves also show that due to these laws, stakeholders such as investors are more hesitant when large amounts of data are involved (ING, 2018).

As determined in the theoretical framework of this thesis, 'cyber' has many components, variations and can be defined in very broad ways. This section will cover how financial institutions in *practice perceive* cyber. Most of them make use of the National Institute of Standards and Technology (NIST) definition and framework. (Specialist 1, 2018).

The NIST-definition is formulated as “The process of protecting information by preventing, detecting, and responding to attacks” (National Institute of Standards and Technology, 2018, p. 45).

Within the annual reports of the largest Dutch financial institutions “cyber” is mentioned 45 times by ING (2017), only 5 times by Rabobank (2017) and 15 times by ABN AMRO (2017). Nevertheless, by none of them “cyber risk” is mentioned a single time as a specific risk. Referring back to the ‘nature’ of risk through which this is analysed, it could be said that cyber risk is not a self-standing risk with regard to that. However, this can also be due to different conceptualization, or incoherent language use. Especially as banks do emphasize “information security” as a specific operational risk. ABN AMRO, for instance, has a structured approach to information security, but not specifically to cyber security (ABN AMRO, 2017, p. 19). As Van den Berg et. al. discussed in the theoretical framework of this research; information security management is a precursor of cyber risk management.

4.4.4 Cyber incidents

In 2017 almost 2.000 data leaks were reported to the Dutch Data Protection Authority by the financial sector. According to the National Coordinator for Security and Counterterrorism, this was the result of the lack of security measures (National Coordinator for Security and Counterterrorism, 2018, p. 30). Institutions recognize various motivations for the different cyber-attacks, such as theft of intellectual property, data theft and money. Not all attacks have the intent of stealing data, as some hackers try to abuse the processing power of banks in order to mind crypto-currencies (Specialist 2, 2018). Next to theft, attackers might want to make a statement or hack an institution “for fun”. Even more, in many cases, cyber-attacks also involve some form of social engineering, such as phone phishing or physical visits (Specialist 1, 2018; Specialist 2, 2018). Well known examples of cyber threats in the financial sector are distributed-denial of service(DDoS) attacks and banking-Trojans (Specialist 2, 2018). In January 2018, many Dutch financial institutions, including ING, Rabobank and ABN AMRO, experienced such DDoS attacks (National Coordinator for Security and Counterterrorism, 2018, p. 17). These attacks gained a lot of media attention as the services of financial institutions were unavailable for several hours, which for example made it impossible for people to transfer money.

Next to banks, also iDeal, a Dutch online-banking payment system, experienced system failures as a result of DDoS attacks. According to Specialist 2 (2018), given the fact that nobody stopped using iDeal as a result of temporary system failures, the reputational impact of these attacks is insignificant. Even more, ING's example in the first part of this analysis could be perceived as a cyber-risk as well, next to a reputational risk. This however depends on the perspective. On the one hand, as financial institutions generally seem to include data protection under the 'cyber umbrella' it therefore could be considered a cyber-risk. On the other hand, given the involvement of the marketing department, it could also mean that in this case, cyber and reputational risks were indeed integrated, but miscalculated given the negative consequences for ING's reputation.

Finally, it is important to state that a lot more is happening at the cyber departments of financial institutions and their partners, however, not all of it is known by the public. Although certain risks are not public knowledge, it does not mean that there are indeed no cyber risks (Specialist 5, 2018).

4.4.5 Cyber risk management

Next to the emphasis on innovation with regard to applications and financial services, important Dutch financial institutions also invest in the innovation of cyber security. ING, Achmea, Rabobank, Volksbank and ABN AMRO are collaborating in a shared research program with the Netherlands Organisation for Applied Scientific Research aimed at improving their cyber security, in order to mitigate cyber risks (TNO, 2017, p. 3).

In the aftermath of a cyberattack, most financial firms in their post-crisis response initially and mainly focus on solving the technical issue at hand, and is therefore dealt with at the IT or cyber department (Specialist 2, 2018). Within the financial institutions, cyber issues are mainly dealt with at the cyber departments and IT-departments, as "a lot of cyber risks are IT-risks, and many of the IT-risks are linked to cyber" (Specialist 5, 2018). Cyber risks are thus not directly linked to the bigger operational risk management practice (Specialist 5, 2018). This given can also be seen within the organizational charts and the risk management strategies of ABN AMRO (ABN AMRO, 2017), ING (ING, 2017) and Rabobank (Rabobank, 2017), as they do not include cyber risk as a self-standing risk. Moreover, according to Specialist 5 (2018), the problem with the management and incorporation of cyber risk within the bigger picture of an institution is the fact that cyber risk is hardly quantifiable and the cyber and IT-departments are not able to translate it into 'euros'.

This also means that the management of cyber risks is not well integrated within the whole organizational structure of financial institutions. Linking this to the models proposed by Bonime-Blanc (2016), this means that no structural cooperation and involvement with the Board and the technical departments exists. According to Specialist 5 (2018), it depends on the respective department how cyber risks are treated as a reputational risk. The bigger the potential effects on its stakeholders, the greater involvement of other departments, the overall risk management, and the more is dealt with the cyber risk as a reputational risk.

Furthermore, a lot of the work regarding cyber risks of financial institutions is outsourced to external parties such as cybersecurity companies or consultancy firms with cyber security specialists like PwC (PwC, n.d.). Even more, according to the Bureau for Economic Policy Analysis ("Centraal Plabureau", CPB), the mitigation against DDoS-attacks of the largest financial institutions within the Netherlands – ING, Rabobank and ABN AMRO – is for a significant part outsourced to a firm in the United States (Bureau for Economic Policy Analysis, 2018, p. 37).

4.4.6 Sub-discussion

With regard to leadership awareness of cyber risks, it can be stated that financial institutions in the Netherlands are very much aware of cyber risks. This can be confirmed by statements made by the government. However, with regard to the organizational context, the problem lies with the integration of the technical divisions and other parts of the institution. Therefore, financial institutions would be positioned between the Integrated Model and the Command and Control Model proposed by Bonime-Blanc (2016) in the theoretical framework chapter. Another so-called emergent indicator that has been identified in this analysis, is 'measurement'. Similar to reputational risks, financial institutions face difficulties with quantifying and measuring cyber risks. For instance, ABN AMRO (2017, p. 17) states that "cybercrime can cause significant financial losses and reputational damage". This is interesting, as it deliberately separates reputational damage from financial losses.

Even though the digitalization and innovation of financial services is to a great extent used as an asset and opportunity, based on the findings of the previous sections, the cyber risks that are accompanied with it are more seen as a liability, as immense and something financial institutions have to comply with. Here, the cost or liability of cyber risk can be linked to theoretical framework on reputational risk, as Bonime-Blanc (2017) argues that reputational risk is linked to the 'cost of doing business'.

With regard to the proposed integrated model by Bonime-Blanc for cyber risk management and the involvement of the Board, it can be argued that the highest levels within the financial institutions are only involved when external factors, bigger parts of society might be impacted by the cyber issue. Or in other words, when the reputation of the firm could potentially become damaged. In that sense, the mitigation of cyber risks could be more seen as 'supportive' of keeping the institution's reputation intact, and in that sense could be seen as 'a risk of reputational risk'. Also, concepts such as 'digital innovation' are often used in the context and interest of 'improving customer experience' (ABN AMRO, 2017; ING, 2017; Rabobank, 2017), a factor that potentially influences the reputation of the institution. Given the assumption that the digital innovation is accompanied by cyber risks, underscores this 'cost of doing business'.

5 Conclusion

5.1 Answering the research question

The analysis presented in this research increased the understanding on the way financial institutions in the Netherlands deal with reputational risk and cyber risks. The different key findings that were identified will now be presented in to order the main research question of this research: *"How do financial institutions in the Netherlands deal with cyber risk as reputational risk?*".

When linking the findings of the analysis chapter with the theoretical framework, it can be argued that the statement on risks as put forward by van Asselt and Renn (Asselt, van & Renn, 2011, p. 431) can be confirmed: the way financial institutions in the Netherlands deal with both reputational and cyber risks is surrounded by complexity and ambiguity. And indeed, it seems that many of the risks discussed in this chapter are 'manufactured' by the sector itself, and follow decisions that are taken by the policymakers of financial institutions. In this sense, this is in line with the arguments put forward by Giddens (Giddens, 1999). The focus of financial institutions on the technical security side of cyber risks, makes it complicated to link cyber risks with the management of reputational risk.

Based on the findings of this research, a visualization or model has been created in order to explain the relation between cyber risk and reputational risk can be understood. This model can be found in figure 7. Accordingly, cyber risks are perceived 'a risk of' reputational risk, that in turn is 'a risk of' the multiple non-financial risks that are, next to financial risks, part of the overarching, comprehensive risk framework of financial institutions. The non-financial part can be explained by the fact that both cyber- and reputational risks appeared difficult to quantify in terms of money. The financial risks can however influence the reputational risks, as the findings demonstrated that for example liquidity or solvency of financial institutions is key to the amount of trust stakeholders have. The model further demonstrates that reputational risk as a 'risk of risk' can also be influenced by other non-financial risks such as compliance risk.

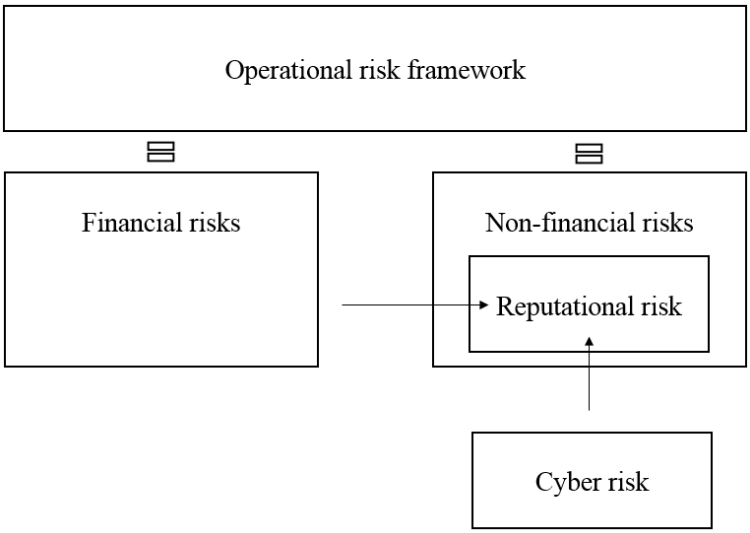

Figure 7 Cyber- and reputational risks: understanding the relationship

This model also demonstrates that the findings of this research stand in contrast with Bonime-Blanc (2016) argument; the direct involvement of all departments and the Board when dealing with cyber-reputational risks. Within the Dutch financial sector, this is only in exceptional situations the case.

One the one hand, most institutions integrated both risks to a certain extent as cyber is seen as a strategic risk, a risk to their reputation, so a 'risk of a risk'. On the other hand, it is perceived still too technical, which thus in practice means that it is not integrated enough. However, most financial institutions do not regard cyber security as an asset yet, while they do so with corporate reputation. This imbalance thus indirectly answers the question on how institutions in the financial sector do *not* deal with cyber security as a reputational risk.

To conclude, this research will end with a recommendation remark from Specialist 3 as "compliance will only keep you out of jail, but will not keep you out of the papers". This means that just compliance is not enough, and here is where changes lie for cyber security to be used as an asset, and where a proactive, inclusive reputational strategy comes, or should come, into play.

5.2 Limitations

To begin with, due to feasibility and time constraints, it proved impossible to consider all potentially related aspects of either cyber or reputational risk. Furthermore, the complex nature of the concepts that were studied, together with the qualitative design, left room for interpretation by the researcher, which can be considered a limitation. Another limitation concerns the relatively low amount of interviewees.

Nonetheless, this can be put in perspective as, the specialists that were interviewed have worked, and currently still work for multiple prominent Dutch financial institutions. As they were consequently able to represent reliable, real-world data, specially due to their high-profile access, the low number of interviewees limits the findings of this research only to a certain extent. Even more, the statements of the specialists were to a large extent underpinned and elaborated on by the findings resulting from primary sources such as institutions' official documents. Another limitation of this research is that the fact that the names of financial institutions, the so called 'clients' of PwC, were not allowed to be mentioned due to the confidentiality code of PwC. As a result, it was not in all cases possible to provide certain statements interviewees made with a concrete example. In conclusion, it could thus be stated that the findings of this research present a valuable impression of the way the Dutch financial sector deals with cyber and reputational risks. It can serve as a starting point for further and detailed research into the integration of cyber and reputational risks.

5.3 Recommendations for further research

In order to develop a comprehensive and holistic framework that includes as many as possible relevant aspects of the relation between cyber risks and reputational risks, further research into several focus areas would be necessary. First, the analysis of this research demonstrated that financial intuitions face difficulties with concretizing and measuring cyber- and reputational risks. Therefore, it would be recommended to conduct further research into the measurement, especially in financial terms, of both risks. Such a concretisation on the actual impacts or consequences of both risk can be proved valuable for integrating cyber- and reputational risks in a more structured manner within the organizational contexts of financial institutions. Second, and with respect to cyber risks, it is recommended to conduct further research into the non-technical consequences and impacts of the cyber activities of financial institutions. This would help further understandings into, for example, how financial institutions can use cyber risks deliberately as an asset and as a proactive part of their reputation and strategy. Finally, with specific regard to the Dutch financial market, it would be recommended to further investigate the relation between the high concentration rate within the market the largest Dutch banks have, and their reputational risk management strategies. It would be interesting to investigate whether there would be any links between the absence of a structured way of dealing with reputational risk, the focus on 'just' compliance to regulations, and the enormous power they have within the Dutch market.

6 Bibliography

ABN AMRO. (2017). *Annual Report 2017.* ABN AMRO Group N.V.

Accenture; Ponemon Institute. (2017). *Cost of Cyber Crime Study: Insights on the security investments that make a difference.* Retrieved March 10, 2018, from Accenture: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Adams, S., Brokx, M., Dalla Corte, L., Galič, M., Kala, K., Koops, B.-J., . . . Škorvánek, I. (2015, November). The Governance of Cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK. *Universiteit van Tilburg*, 1-166.

Asselt, van, M., & Renn, O. (2011, April). Risk governance. *Journal of Risk Research, 14*(4), 431–449.

Banken.nl. (2018, May 29). *Ranglijst grootste Nederlandse banken 2018*. Retrieved November 10, 2018, from Banken.nl: https://www.banken.nl/nieuws/20909/ranglijst-grootste-nederlandse-banken-2018

Baumfield, V. (2016, August 31). Stakeholder theory from a management perspective: Bridging the shareholder/stakeholder divide. *Bond University*, 1-23.

Beck, U. (1992). *Risk Society, Towards a New Modernity.* London: SAGE Publications.

Berg, van den , J., Zoggel, van, J., Snels, M., Leeuwen, van, M., Boeke, S., Koppen, van de , L., . . . Bos, de, T. (2014, October 13-14). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. *NATO STO/IST-122 symposium*, 12.

Bonime-Blanc, A. (2014). Reputation Risk Is A Strategic Risk: What Are Your Plans? *Ethical Boardroom*, 1-3. Retrieved from https://www.reprisk.com/content/6-news/1-media-coverage/236-2014-12-29-reputation-risk-is-a-strategic-risk-what-are-your/2014-12-29-reputation-risk-is-a-strategic-risk-what-are-your.pdf

Bonime-Blanc, A. (2016, March 21). *Mitigating cyber-reputation risk.* Retrieved March 23, 2018, from Ethical corporation: http://www.ethicalcorp.com/globalethicist-mitigating-cyber-reputation-risk

Bonime-Blanc, A. (2017). *The Reputation Risk Handbook: Surviving and Thriving in the Age of Hyper-Transparency.* New York: Routledge.

Bureau for Economic Policy Analysis. (2018). *Risicorapportage Cyberveiligheid Economie 2018.* Retrieved from https://www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-15okt2018-Risicorapportage-Cyberveiligheid-Economie-2018.pdf

Burgess, A., Wardman, J., & Mythen, G. (2018). Considering risk: placing the work of Ulrich Beck in context. *Journal of Risk Research, 21*(1), 1-5. doi:10.1080/13669877.2017.1383075

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43–62.

Collier, P. (2003). *Accounting for Managers: Interpreting Accounting Information for Decision Making.* Wiley.

Committee on Payments and Market Infrastructures; Board of the International Organization of Securities Commissions. (2016, June). *Guidance on cyber resilience for financial market infrastructures.* Retrieved May 30, 2018, from BIS: https://www.bis.org/cpmi/publ/d146.pdf

Cook, V., Phillips, D., & Holden, J. (2006, December 6). Geography fieldwork in a 'risk society'. *Area*, 413–420.

Coombs, W. (2007). Attribution Theory as a guide for post-crisis communication research. *Public Relations Review, 33*(2), 135-139.

CPB. (2018, October 15). *Risicorapportage Cyberveiligheid Economie 2018.* Retrieved December 29, 2018, from https://www.cpb.nl/publicatie/risicorapportage-cyberveiligheid-economie-2018

Crisanto, J., & Prenio, J. (2017, August). *Regulatory approaches to enhance banks' cyber-security frameworks.* Retrieved June 2, 2018, from Financial Stability Institute: https://www.bis.org/fsi/publ/insights2.pdf

De Nederlandsche Bank. (2015). *Visie op de structuur van de Nederlandse bankensector.*

De Nederlandsche Bank. (n.d.). *How does DNB promote financial stability?* Retrieved November 14, 2018, from DNB: https://www.dnb.nl/en/about-dnb/duties/financial-stability/how-does-dnb-promote-fs/index.jsp

Deloitte. (2014, October). *2014 global survey on reputation risk* . Retrieved March 21, 2018, from Deloitte: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report.pdf

Dutch Authority for the Financial Markets (AFM). (2018, October 29). *The Netherlands to become the centre of European financial trading post Brexit*. Retrieved November 10, 2018, from AFM: https://www.afm.nl/en/consumenten/nieuws/2018/okt/trendzicht-2019

Dutch National Coordinator for Security and Counterterrorism. (2018, February 1). *Factsheet Weerbare Vitale Infrastructuur.* Retrieved from NCTV: https://www.nctv.nl/binaries/Factsheet%20Weerbare%20Vitale%20Infrastructuur%20NL%202018_tcm31-234709.pdf

Dutta, A., & McCrohan, K. (2002, October 1). Management's Role in Information Security in a Cyber Economy. *California Management Review, 45*(1), 67-87.

Economist Intelligence Unit. (2005). *Reputation: risk of risks - white paper.* Retrieved from Data Breach Insurance: https://databreachinsurancequote.com/wp-content/uploads/2014/10/Reputation-Risks.pdf

European Central Bank. (2017, October). *Report on financial structures.* doi:10.2866/349729

Financial Conduct Authority. (2018, January 01). *Building cyber resilience.* Retrieved March 10, 2018, from Financial Conduct Authority: https://www.fca.org.uk/news/speeches/building-cyber-resilience

Fiordelisi, F., Soana, M.-G., & Schwizer, P. (2012, June 27). Reputational losses and operational risk in banking. *The European Journal of Finance, 20*(2), 105-124.

Fobrun, C. (2012). The Building Blocks of Corporate Reputation: Definitions, Antecedents, Consequences. In T. G. Barnett, *The Oxford Handbook of Corporate Reputation* (pp. 94-110). Oxford University Press.

Gatzert, N. (2015, November 2). The impact of corporate reputation and reputation damaging events on financial performance: Empirical evidence from the literature. *European Management Journal, 33*(6), 485-499.

Gaultier-Gaillard, S., Louisot, J.-P., & Rayner, J. (2009). Managing reputational risk – From theory to practice. In J. Klewes, & R. Wreschniok, *Reputation Capital* (pp. 161-178). Berlin: Springer.

Giddens, A. (1999, January). Risk and Responsibility. *The Modern Law Review, 62*(1).

Heidinger, D., & Gatzert, N. (2018, June). Awareness, determinants and value of reputation risk management: Empirical evidence from the banking and insurance industry. *Journal of Banking and Finance, 91*, 106-118.

IEX. (2018, May 9). *ING krijgt er fors meer klanten bij*. Retrieved June 3, 2018, from IEX: https://www.iex.nl/Nieuws/ANP-090518-027/ING-krijgt-er-fors-meer-klanten-bij.aspx

ING. (2017). *ING Bank Annual Report 2017.* ING.

ING. (2017, October 25). *ING launches ING Ventures: a EUR 300 million fintech fund*. Retrieved December 29, 2018, from ING: https://www.ing.com/Newsroom/All-news/Press-releases/ING-launches-ING-Ventures-a-EUR-300-million-fintech-fund.htm

ING. (2018, May 26). *ING BeleggersBarometer: vertrouwen weer in de lift*. Retrieved June 5, 2018, from ING: https://www.ing.nl/nieuws/nieuws_en_persberichten/2018/mei/ing_beleggersbarometer_vertrouwen_weer_in_de_lift.html

Jacobs, J., & Dijst, D. (2018). Seminar informatiebeveiliging en cybersecurity: Resultaten onderzoeken 2017 en vooruitblik. De Nederlandsche Bank.

Jebb, A., Parrigon, S., & Eun Whoo, S. (2017, June). Exploratory data analysis as a foundation of inductive research. *Human Resource Management Review, 27*(2), 265-276.

Johnson, K. (2015). Cyber Risks: Emerging Risk Management Concerns for Financial Institutions. *Georgia Law Review, 50*(131), 131-142.

Johnson, K. (2015, Fall). Cyber Risks: Emerging Risk Management Concerns for Financial Institutions,. *Georgia Law Review*, 131-142.

Johnston, M. (2014). Secondary Data Analysis: A Method of which the Time Has Come. *Qualitative and Quantitative Methods in Libraries (QQML)*, 619 –626.

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016, May 9). Systematic methodological review: developing a framework for aqualitative semi-structured interview guide. *JAN*, 2954-2965.

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology.* SAGE Publications.

Kumar, R. (2011). *Research Methodology: a step-by-step guide for beginners.* SAGE Publications.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security , 45*, 58-74.

Larkin, J. (2002). Strategic Reputation Risk Management. Palgrave Macmillan UK.

Management Team. (2018, September 27). *MT 500 2018: De lijst*. Retrieved November 25, 2018, from MT: https://www.mt.nl/management/reputatie/mt-500-2018-de-lijst/559930

Merriam, S. (2009). *Qualitative Research: A Guide to Design and Implementation.* San Francisco: Jossey-Bass, A Wiley Imprint.

Miklaszewska, E., & Kil, K. (2016). Reputational Risk: Problems with Understanding the Concept and Managing its Impact. *Bezpieczny Bank, 4*(65), 96-115.

Mukherjee, N., Zambon, S., & Lucius, H. (2008, July 2015). Do banks manage Reputational Risk? - a case study of European Investment Bank (working paper). 1-25.

Mythen, G. (2004). *Ulrich Beck : a critical introduction to the risk society.* London: Pluto Pres.

National Coordinator for Security and Counterterrorism. (2018). *Cyber Security Assessment Netherlands 2018.*

National Institute of Standards and Technology. (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1.* Retrieved May 23, 2018, from NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nederlandse Vereniging van Banken. (2014). *Toekomstgericht Bankieren - Maatschappelijk Statuut - Code Banken - Gedragsregels.* Retrieved October 20, 2018, from Nederlandse Vereniging van Banken: file://vuw/Personal$/Homes/20/s2055619/Downloads/000733_toekomstgericht-bankieren-statuut-code-banken-gedragsregels.pdf

Netherlands Authority for the Financial Markets. (2015, April 9). *AFM: Verandering moet meer uit financiële sector zelf komen om vertrouwen te herstellen*. Retrieved July 20, 2018, from AFM: https://www.afm.nl/nl-nl/nieuws/2015/apr/sector-herstel-vertrouwen

NOS. (2018, March 13). *ING trekt omstreden salarisvoorstel topman Hamers in.* Retrieved October 12, 2018, from NOS.nl: https://nos.nl/artikel/2222107-ing-trekt-omstreden-salarisvoorstel-topman-hamers-in.html

Platt, J. (1992). "Case Study" in American Methodological Thought. *Current Sociology, 40*(1), 17-48.

PwC. (2014). Retrieved October 20, 2018, from Retail Banking 2020 Evolution or Revolution?: https://www.pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf

PwC. (2014). *Retail Banking 2020: Evolution or Revolution?* Retrieved July 20, 2018, from PwC.com/banking: https://www.pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf

PwC. (2018). *Cybersecurity in financial services.* Retrieved March 10, 2018, from PwC: https://www.pwc.com/us/en/industries/financial-services/research-institute/top-issues/cybersecurity.html

PwC. (n.d.). *Financial services should focus on their workforce when building digital trust*. Retrieved 2019, from PwC: https://www.pwc.nl/en/insights-and-publications/services-and-industries/financial-sector/digitaal-vertrouwen-begint-voor-financials-bij-medewerkers.html

Rabobank. (2017). *Annual Report 2017.* Rabobank.

Radar. (2014, March 13). *30% ING-klanten overweegt overstap*. Retrieved July 10, 2018, from Radar: https://radar.avrotros.nl/testpanel/uitslagen/item/30-ing-klanten-overweegt-overstap/

Rance, S. (2014). *Cyber Resilience: bridging the business and technology divide Stuart Rance.* Retrieved March 18, 2018, from Axelos: http://www.inxelerate.com/wp-content/uploads/2015/02/Cyber-Resilience.pdf

Rayner, J. (2004). Managing Reputational Risk: Curbing Threats, Leveraging Opportunities. John Wiley & Sons.

Renn, O. (2005). White Paper on Risk Governance: Towards an Integrative Framework. *International Risk Governance Council*, 1-157.

Rijksoverheid. (n.d.). *Gezonde financiële sector.* Retrieved 2018, from Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/financiele-sector/gezonde-financiele-sector

Rijksoverheid. (n.d.). *Misbruik in financiële sector tegengaan*. Retrieved November 24, 2018, from Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/financiele-sector/misbruik-in-financiele-sector-tegengaan

Scandizzo, S. (2011, September). A Framework for the Analysis of Reputational Risk. *Journal of Operational Risk, 6*(3), 41-63.

SIS. (n.d.). *Desk Research*. Retrieved October 13, 2018, from SIS International Research : https://www.sisinternational.com/solutions/qualitative-quantitative-research-solutions/desk-research/

Spelier, P. (2014, March 25). *ING haalt 'Big Data' kastanjes uit het vuur voor de andere banken*. Retrieved October 21, 2018, from Emerce: https://www.emerce.nl/opinie/ing-haalt-big-data-kastanjes-uit-vuur-andere-banken

The Dutch Authority for the Financial Markets. (2017). *Annual Rapport 2017.* Retrieved from https://www.afm.nl/nl-nl/verslaglegging/jaarverslag

The Dutch Authority for the Financial Markets. (2019). *Trend Monitor: A survey of trends and risks on the financial markets.* Retrieved from file://vuw/Personal$/Homes/20/s2055619/Downloads/rapport-2019-eng%20(1).pdf

TNO. (2017). *Innovating in Cyber Security: Shared research 2017.* Retrieved from https://www.tno.nl/media/9419/innovating-in-cyber-security.pdf

Tonello, M. (2007). Reputation Risk: A Corporate Governance Perspective. *The Conference Board*, 1-47.

Wetenschappelijke Raad voor het Regeringsbeleid. (2016). *Samenleving en financiële sector in evenwicht.* The Hague.

Yin, R. (2009). *Case Study Research: Design and Methods.* Los Angeles: Sage Publications.

Yin, R. (2011). *Qualitative Research from Start to Finish.* New York: The Guilford Press.

7 Appendices

Annex 1: Planning of the interviews

Respondent	**Specialisation (within the financial sector)**	**Date and time**	**Location**
Specialist 1	Specialised in cyber security	*11/04/2018, 10:30 - 11:15*	Amsterdam
Specialist 2	Specialised in cyber security	*11/04/2018, 10:30 - 11:15*	Amsterdam
Specialist 3	Specialised in operational risk	*18/05/2018, 13:30 – 14:00*	Amsterdam
Specialist 4	Specialised in risk within financial services consulting	*23/05/2018, 13:00 - 13:30*	Amsterdam
Specialist 5	Specialised in cyber risk, new technology and risk	09/07/2018, 09:30 – 10:15	Amsterdam

Annex 2: Interview questions

	Question
1	Could you briefly introduce yourself? Please elaborate on job description, specialization and relation to the financial sector.
2	How do financial institutions describe, or perceive, reputational risk? Follow- up questions: could you give any examples?
3	How do financial institutions try to mitigate reputational damage? Follow-up questions: Do they have a certain model or framework for that?
4	Could you give an example of a reputational crisis? Follow-up question: what departments of the financial institution were involved with this crisis?
5	How do financial institutions describe, or perceive, cyber risks? Follow- up questions: could you give any examples?
6	What departments of financial institutions are involved when dealing with cyber risks?
7	Could you give an example of a cyber crisis in the financial sector?
8	How do financial institutions deal with cyber risk as a reputational risk?

Annex 3: Analysis scheme

Concept	Concept	Indicators	Supporting literature
Relation and link between cyber risks and reputational risk	Reputational risk	Nature of the risk: - no risk - risk of risk - self-standing - strategic	(Bonime-Blanc, 2017, p. 49; Heidinger & Gatzert, 2018)
		Leadership: - awareness - resources	(Bonime-Blanc, 2016)
		Organizational context (departments, integration within the entire strategy)	(Bonime-Blanc, 2016)
	Cyber risk	Nature of the risk: - no risk - risk of risk - self-standing - strategic	(Bonime-Blanc, 2017, p. 49; Heidinger & Gatzert, 2018)
		Leadership: - awareness - resources	(Bonime-Blanc, 2016)
		Organizational context (departments, integration within the entire strategy)	(Bonime-Blanc, 2016)
		Cyber risks - Technical layer - Tech-socio layer - Cyber risk exposure	(Berg, van den , et al., 2014; Bonime-Blanc, 2016)