ECONOMIC BARRIERS & CYBER SECURITY INVESTMENT – A VIEW ON THE DUTCH TRANSPORT AND LOGISTICS SECTOR

by

MAXIME NIEUWENHUIZEN
S0983462

MASTER THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR A DEGREE IN

CRISIS & SECURITY MANAGEMENT

UNIVERSITEIT LEIDEN
SUPERVISED BY: DR. JOERY MATTHYS
SECOND READER: DR. EDWIN BAKKER

15-03-2016

ABSTRACT

This master thesis strives to map the problem of economic barriers in the Dutch transport and logistics sector. Critical infrastructure such as main transport systems are increasingly becoming dependent on network communication systems. The use of these network communication systems creates new cyber security vulnerabilities for the critical infrastructure. In addition, economic barriers in the market constrain cyber security improvements to overcome these new vulnerabilities.

Although academia pinpoint the economic barriers of misaligned incentives, asymmetric information and network externalities as a significant cause for the lack of cyber security, it should be questioned if this theory applies to all sectors and countries. This research will challenge the economic barrier theory and analyse if the theory applies to the Dutch transport and logistics sector. The academic field of economics of information security will assist in determining the threat economic barriers pose to the Dutch transport and logistics sector. Multiple set criteria will be used to analyse the Dutch transport and logistics sector and the vulnerability to economic barriers in regards to cyber security investments.

This study is not about the individual application of technical protection mechanisms to improve cyber resilience, but rather to understand the severity of the problem in the Dutch transport and logistics sector. It is therefore important to understand that this thesis does not search a way to establish 100 percent security, but this research focusses on mapping the threat of economic barriers to find a way to enhance cyber security and overcome the market failures in the IT market.

This research will be conducted at the Leiden University as a thesis assignment for the Master Crisis and security Management

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation and thanks to my supervisor Dr. Joery Matthys for his continues advice and feedback. A special gratitude to Linda van Moors, Arthur van Dijk, Monic van der Heyden and Ernst-Jan Zwijnenberg who were willing to show me the world of the Dutch transport and logistics sector. And a special thank for Ed Nieuwenhuizen who was always supportive and able to broaden my horizon on the topic.

Table of contents

1. INTRODUCTION

1.1 Research problem

The Netherlands is one of the front runners of Internet use in the public and private sector.[1] Many companies use the Internet to provide their services. Especially the transportation and logistics sector relies on the use of Internet to execute their services.[2] According to the Ernst and Young ICT barometer survey in 2011 more than 85 percent in the transport and logistics sector managers state that their companies are extremely dependent on ICT. Two years earlier this number was 69 percent, the dependency on ICT in the transport and logistics sector has risen rapidly.[3] The 'Cyber Security Beeld Nederland' (CSBN) report is a governmental rapport that addresses the current cyber security threats in the Netherlands. The report assesses dependency on cyber security as a challenge for the Dutch government. The report states that "*Dutch transport and logistics sector processes often become more dependent on IT due to laws and regulations in the sector. If any systems are breached, the impact of such breach will be more substantial.*"[4] The CSBN report explains that multiple cyber security breaches in the Dutch transport and logistics sector eventually can lead to negative economic consequences. For instance, that transport organizations will move their business to other countries. This could even cause potential problems for the Dutch food supply.[5]

While the companies are extremely dependent on ICT, a report of The Hague Centre of Strategic Studies stated that the transport and logistics sector is one of the sectors that compared to the other sectors is behind on cyber security.[6] Only 25 percent of European companies in the transport and logistics sector have a formally defined an ICT security policy. In the financial sector already 78 percent of EU companies have formalized an ICT security policy.[7] It is quite

[1] NCTV, (2013) Cybersecurity Strategy 2. Cybersecurity Nederland
< https://www.nctv.nl/onderwerpen/cybersecurity/>
[2] Nationaal Cyber Security Centrum (2015) Cybersecuritybeeld Nederland 2015. Ministerie van Veiligheid en Justitie. < https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015%5B2%5D.html>
[3] Ernst & Young (2011) 'ICT Barometer over cybercrime' Jaargang 11Beveilginswereld
<http://www.beveiligingswereld.nl/files/ICTBarometercybercrime2011.pdf>
[4] Nationaal Cyber Security Centrum (2015) Cybersecuritybeeld Nederland 2015. Ministerie van Veiligheid en Justitie. < https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015%5B2%5D.html>
[5] Ibid.
[6] Gehem, M., Usanov, A. Frinking, E. Rademaker, M. (2015) Accessing Cyber Security, A Meta-Analysis of Threats, Trends, And Responses to Cyber Attacks. The Hague Centre for Strategic Studies, The Hague, pp. 1-101
[7] Ibid.

worrisome that such a vital factor as ICT is not seen as an important factor to protect and invest in by the Dutch transport and logistics sector.

Furthermore, the Internet revolution brought drastic change in companies' and government's ways in communicating and conducting business.[8] Nowadays, data is shared by transportation and logistics companies via web-based applications that reveal information regarding shipments throughout the entire supply chain. However, tracking systems using barcodes, RFID tags and GPS systems are vulnerable targets for hackers and cybercriminals, because criminals can extort the vulnerability and gain access to the tracking data. [9] Especially crypto ware attacks and spear phishing attacks are used to disrupt the Dutch transport and logistics sector.[10] The CSBN report states that criminals pose the biggest threat to the Dutch transport and logistics sector. Criminals focus their effort on infiltrating network communication systems and manipulating data in order to smuggle or steal valuable goods.[11] There has been an increase of reported attacks on network communication system of the Dutch transport and logistics sector in 2015.[12]

Cyber security-attacks and data breaches come with great losses for the Dutch society. The Hague Security Delta calculated in their research that annually cybercrime costs the Dutch economy approximately 8.8 billion euros.[13] 7 percent of these costs are accounted to the transportation and logistics sector. These tremendous costs makes cyber security a serious issue in the Dutch transport and logistics sector and puts combating cybercrime on the top of the Dutch political agenda.[14] Cyber security costs in the Netherlands are specifically interesting because on average the loss of cyber-attacks represents 1.5 percent of the Dutch GDP annually. While other European countries only experience an average loss of 0.8 percent of their GDP.[15]

[8] Mueller, M. (2010) Networks and States, The Global Politics of Internet Governance. The Mitt Press. First edition

[9] Trade, R. (2014) Cyber Liability Risks for Transportation and Logistics Companies. Insurance for trade and transportation. latest accessed on 19-11-2015 <https://www.roanoketrade.com/cyber-liability-risks-transportation-logistics-companies/>

[10] Nationaal Cyber Security Centrum (2015) Cybersecuritybeeld Nederland 2015. Ministerie van Veiligheid en Justitie. < https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015%5B2%5D.html>

[11] Ibid

[12] Ibid.

[13] HSD, (2014) Cyber Crime Costs The Netherlands 8.8 Billion Euros Per Year. The Hague Security Delta Website. Latest accessed on 14-01-2015 <https://www.thehaguesecuritydelta.com/news/newsitem/191>

[14] Bos, H., Etalle, S., Fransen, F. and Poll, E. (2013) NCSRAII, National Cyber Security Research Agenda. <https://www.iipvv.nl/sites/stw.demo.infi.nl/files/mediabank/NCSRA-II.pdf>

[15] Gehem, M., Usanov, A. Frinking, E. Rademaker, M. (2015) Accessing Cyber Security, A Meta-Analysis of Threats, Trends, And Responses to Cyber Attacks. The Hague Centre for Strategic Studies, The Hague, pp. 1-101

Creating policies to decrease cyber-attacks losses, combat cybercrime, increasing security measures and regulate online behaviour is difficult. There are structural limitations embedded in the nature of Internet governance, because nobody 'owns' the Internet.[16] This struggle is notable because investment in cyber security remains low. Especially in the private sector many companies fall short in focus and investment because cyber security does not have a place on their business agenda.[17] For example according to a research of Ernst and Young only 40 percent of the companies invested in some way in cyber security measures to prevent data breaches.[18] The other 60 percent decided not to invest to protect themselves from the vulnerabilities that come with the use of the Internet for various reasons. [19] This research tries to map these reasons in order to get an overview of the problem.

Over the years the view on cyber security has changed. It is not that simple to apply technical protection mechanisms. In the nineties the field expanded with political and legal influences and more recent in the last 10 year the economic line of thought entered the cyber security debate.[20] In order to improve and ensure cyber security for a state or a company economic barriers need to be overcome and managed. This research focusses on the problem of economic barriers. It is important not to analyse cyber security from the technical side only but also investigate the problematic economic side of cyber security.

1.2 Research question

The research question of this master thesis is: *In how far is the Dutch transport and logistics sector vulnerable to economic barriers regarding investments in cyber security?*

This study is going to research if the Dutch transport and logistics sectors is vulnerable to economic barriers regarding cyber security investment. Determining if these economic barriers pose a threat to the Dutch transport and logistics sector is crucial in deciding where regulation is needed to diminish the market failures. Identification of the economic barriers is fundamental

[16] Mueller, M. (2010) Networks and States, The Global Politics of Internet Governance. The Mitt Press. First edition
[17] Gehem, M., Usanov, A. Frinking, E. Rademaker, M. (2015) Accessing Cyber Security, A Meta-Analysis of Threats, Trends, And Responses to Cyber Attacks. The Hague Centre for Strategic Studies, The Hague, pp. 1-101
[18]Ernst & Young (2011) 'ICT Barometer over cybercrime' Jaargang 11Beveilginswereld <http://www.beveiligingswereld.nl/files/ICTBarometercybercrime2011.pdf>
[19] Ibid.
[20] Mueller, M. (2010) Networks and States, The Global Politics of Internet Governance. The Mitt Press. First edition

for finding a more structural solution for cyber security issues. The research will also investigate which barriers are most applicable to the Dutch cyber domain in the transport and logistics sector.

Summarizing:

This research aims:

- to create a theoretical understanding of economic barriers regarding cyber security
- to map the problem and the vulnerability to economic barriers in the Dutch transport and logistics sector
- to research if these economic barriers are recognized by the Dutch transport and logistics sector

In this research only the Netherlands will be used as a case study, because a case study of one country can provide a more detailed description of the situation of cyber security problems in that country. The unit of analysis will therefore be the national level which is a macro perspective.[21] Besides that this research will concentrate on only one of the cyber security sectors. A wider perspective would make the research unfeasible in the given time period.

Furthermore, this research uses the Netherlands as a case study because it is the third country in the world regarding the use of Internet in their economic sector.[22] Most of the Dutch private and public industry rely on the Internet. It is therefore important to sustain and preserve a level of cyber security.[23] Thereby, the Dutch government indicated in their National Cyber Security Research Agenda that more research is necessary to map the problem and the threat economic barriers might pose to critical infrastructures in the Netherlands.[24] This research can help to develop strategies for allocating the essential resources concerning cyber security threats towards Dutch critical infrastructure.

[21] Bryman, A. (2012) 'Social Research Methods. 'Oxford University Press. 4th Edition.
[22] NCTV, (2013) Cybersecurity Strategy 2. Cybersecurity Nederland
< https://www.nctv.nl/onderwerpen/cybersecurity/>
[23] Ibid.
[24] Bos, H., Etalle, S., Fransen, F. and Poll, E. (2013) NCSRAII, National Cyber Security Research Agenda.
<https://www.iipvv.nl/sites/stw.demo.infi.nl/files/mediabank/NCSRA-II.pdf>

1.3 Knowledge gap

As stated above, governments are in need for more research concerning economic barriers to investigate the cyber threat it causes for the Netherlands.[25] There is an academic debate that discusses and analyses causes and solutions for economic barriers in the information security field and the IT market. The theories that will be used are developed in the academic field of 'Economics and Information Security'. Main academia in this field are: Taylor Moore, Ross Anderson, Michiel van Eeten, Bruce Schneier, Milton Meuller, Johannes Bauer, Shari Pfleeger and Rachel Rue, Rowe Brent, Michael Gallaher and Böhme Rainer .[26] Their theories and views on economic barriers and policy options to improve cyber security for the critical infrastructure of the transport and logistics sector will be used in this thesis. However these are mainly general theories and are not tested and especially applied to the Dutch transport and logistics sector. In addition, the possible Dutch economic barriers have not been reviewed from a theoretical and practical perspective. This thesis will try to provide an overview from the diverse arguments from both perspectives in order to understand why cyber security is constrained in the Dutch transport and logistics sector.

1.4 Social and academic relevance

The social relevance of this thesis is that currently the Netherlands is facing a new cyber threat because their critical infrastructure is becoming rapidly more dependent on ICT.[27] Furthermore, the cybercrime costs of the transport and logistics sector are extremely high.[28] It is important to understand this threat and map out the problem. Research on understanding and mapping this threat can be an important factor in developing new policies and eventually assist in increasing cyber security for the entire Dutch society.

The academic relevance of this thesis is that this research does not focus on the technical aspect of cyber security which is mostly studied, but focus on the economic factors that play a role in

[25] Bos, H., Etalle, S., Fransen, F. and Poll, E. (2013) NCSRAII, National Cyber Security Research Agenda. <https://www.iipvv.nl/sites/stw.demo.infi.nl/files/mediabank/NCSRA-II.pdf>
[26] ISE Website. Economics of Information Security. Home page, latest accessed on 01-02-2016 <http://infosecon.net/>
[27] Nationaal Cyber Security Centrum (2015) Cybersecuritybeeld Nederland 2015. Ministerie van Veiligheid en Justitie. < https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015%5B2%5D.html>
[28] Gehem, M., Usanov, A. Frinking, E. Rademaker, M. (2015) Accessing Cyber Security, A Meta-Analysis of Threats, Trends, And Responses to Cyber Attacks. The Hague Centre for Strategic Studies, The Hague, pp. 1-101

increasing cyber security. Additionally, the academic relevance of this thesis is that it applies the theory of economic barriers and the proposed solution to a new case study. This study also adds value to the debate on economic government intervention in the field of cyber security. This debate is relatively new and is in need for analysis from different perspectives.

1.5 Structure of the thesis

This thesis consist of six chapters which will all add to the construct for an answer to the research question. In this first chapter the research problem and the urgency of this research was clarified. The next chapter will elaborate on the theories and concepts of the academic field of 'economics of information security'. It will explain the theory that will be used in this research to create an understanding of economic barriers and the cyber security challenges the Dutch transport and logistics sector face. Further, the third chapter will discuss and justify the research methods of this research. It will provide operationalization and outline the criteria set to investigate economic barriers of the Dutch transport and logistics sector.

The fourth chapter will provide an elaborate overview of the Dutch transport and logistics sector based on perspectives in the literature and the field. The profile of the Dutch transport and logistic sector will be discussed to analyse if the sector shows multiple characteristics that instigate economic barriers in the market. The fifth chapter will be concluding the results of this research and offer a discussion on the research. The last chapter will provide an overview of the used literature in this research.

2. THEORETICAL FRAMEWORK

This theoretical chapter will consist of a conceptualization of key concepts and a concise overview on the theoretical background of the academic field of economics and information security. First, the key concepts regarding the economic and information security field and the key concepts of the research question will be explained. Following the chapter will outline the main body of literature in the academic field of economics and information security and provide an overview of the different arguments set out by the main scholars.

2.1 Key Concepts

The following section will explain the terminology used in this research and the research question. Key concepts such as cyber security, cyber-attacks, economic barriers, and the transport and logistics sector will be discussed. All these terms will be conceptualized to create a concrete understanding of the research topic.

2.1.1 Cyber security

The concept of cyber security is fundamental to comprehend and answer the research question. It is a necessity to explain the concept of cyber security because the goal of the research is to understand, analyse and map the threat economic barriers pose to the cyber security in the Netherlands. Without understanding what cyber security is we cannot analyse the level of cyber security or influencing factors on cyber security in the Netherlands. According to the second Dutch cyber security strategy developed by the National Cyber Security Centre (NCSC), cyber security refers to "*the pursuit to prevent damage caused by: disturbance, breakdowns in or abuse of ICT. And repairing the damage if and when it occurs*."[29] This definition clearly shows the broadness of the topic cyber security and that it entails more than for example installing a virus scan on your computer. For instance cyber security can present itself as: cyber security crisis response teams, security awareness training for employees, installing firewall, security by design protocols or improving data base processes. Cyber security is therefore spread over a broad spectrum and can come in many forms.[30]

[29] NCTV, (2013) National Cybersecurity Strategy 2. Cybersecurity Nederland
< https://www.nctv.nl/onderwerpen/cybersecurity/>
[30] Ibid.

Besides the variety in how cyber security can occur it is also important to understand the difficulty of being successful in the "pursuit". Cyber security is difficult to accomplish because of the fast changing threats and new risks that appear. It is a continuous battle between finding vulnerabilities and protecting them.[31]

In addition, in the last 10 years cyber security has become more than just applying technical protection mechanism. The technical field has been expanded with economic, political, and legal influences.[32] This thesis will mainly focus on the economic influences in the pursuit to prevent damage in any kind to the ICT of the transport and logistics sector, because this research investigates economic barriers and their influence on cyber security in the transport and logistics sector.

Furthermore, in the definition of the NCSC cyber security is referred to as a 'pursuit' because it is difficult to measure cyber security.[33] Hence, measuring the level of cyber security is difficult because it is hard to measure crime inflicted actions by ICT. If you cannot measure the problem how can you measure the solution? Academia have come up with cyber risk indicators to establish a baseline and improvement.[34] Guidelines, standards and best practices documents are developed which all mainly focus on measuring the effectiveness, assurance and results through for example the Common Vulnerabilities and Exposures and the Common Vulnerabilities Common Scoring System.[35]

In this research insufficient cyber security is established through the extensive damages reports from: The Hague Security Delta, National Cyber Security Centre, the Dutch ministry of economic affairs and The Hague Centre for Strategic Studies.[36] All these institution point out the insufficient cyber security for the Dutch transport and logistics sector. For example, The Hague Security Delta stated that 7 percent of the total cyber-attack damage are accounted for by the Dutch transport and logistics sector. In addition, the National Cyber Security Centre, the Dutch ministry of economic affairs and The Hague Centre for Strategic Studies concluded in

[31] NCTV, (2013) National Cybersecurity beeld 4. Cybersecurity Nederland
< https://www.nctv.nl/onderwerpen/cybersecurity/>
[32] Anderson, R., Böhme, R., Clayton, R. and Moore, T. (2008) 'Security Economics and The Internal Market.' Research Report ENISA pp 1-114
[33] Ibid.
[34] King, S. (2009) "Measuring Cyber Security and information assurance". IATAC SOAR, <https://buildsecurityin.us-cert.gov/sites/default/files/MeasuringCybersecurityIA.PDF>
[35] Ibid.
[36] Gehem, M., Usanov, A. Frinking, E. Rademaker, M. (2015) Accessing Cyber Security, A Meta-Analysis of Threats, Trends, And Responses to Cyber Attacks. The Hague Centre for Strategic Studies, The Hague, pp. 1-101

their report on ‘Assessing Cyber Security’ that there has been an extreme increase in in the last 5 years of successful cyber security attacks where information was breached in the transport and logistics sector. [37]

Therefore, currently cyber security in the Dutch transport and logistics sector is perceived as low and inadequate. The theory of economic barriers which is used in this research describes why investments and development in cyber security are deficient. This research aims to establish if the Dutch transport and logistics sectors is vulnerable to economic barriers in regards to cyber security.

2.1.2 Cyber-attack, incident or breach?

With dependency on ICT many dangers arise, this section will explain what happens during an attack. In the literature multiple stages of attacks and the caused damage are described. The difference in definition lies therefore with the severity of the cyber-attack. It is important to understand the difference, because each stage of a cyber-attack has different economic consequences and effect on the concerning organization.

- Attack: “*A malicious attempt to gain unauthorized access in order to collect, disrupt, degrade or destroy information or resources of a system.”*[38]
- Incident: “*Actions taken through the use of a computer network that compromises the integrity and possess a threat to an information system.”*[39]
- Breach: “*The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.”*[40]

Cyber-attack is used in the literature as the overall word to express cyber security problems. However, there is an important difference between the term ‘incident’ and the term ‘breach’. It expresses the severity of the problem and hereby also the economic consequences for the

[37] Gehem, M., Usanov, A. Frinking, E. Rademaker, M. (2015) Accessing Cyber Security, A Meta-Analysis of Threats, Trends, And Responses to Cyber Attacks. The Hague Centre for Strategic Studies, The Hague, pp. 1-101
[38] Ibid.
[39] NATO Cooperative Cyber Defence Centre of Excellence ‘Cyber Definitions.’ CCDCOE, NATO Website, latest accessed on 19-11-2015 <https://ccdcoe.org/cyber-definitions.html>
[40] National Initiative for Cyber security Careers and Studies. (2015) ‘Explore Terms: A Glossary of Common Cybersecurity Terminology’. NICCS, latest accessed on 19-11-2015 <http://niccs.us-cert.gov/glossary#letter_B>

organization. When an incident occurs it means that the system is compromised but actual data or vital information is not obtained. While by a breach sensitive information is obtained and hereby causes a larger problems for the organization.

When an organization uses ICT it is important that it protects itself against such events as the consequences of an attack, incident and breach are negative. Chapter four will go further in providing a theoretical description of who execute attacks and how criminals execute these attacks in the transport and logistics sector.

2.1.3 Transport and logistics sector

In this research the focus will lie on the Dutch transport and logistics sector. The Dutch transport and logistics sector consists of 10 percent of the Dutch economy and is one of the 9 top sectors in the Netherlands.[41] The transport and logistics sector comprises of executing the tasks of planning and physical transportations of goods.[42] In addition the transport and logistics sector represent the Dutch critical infrastructure as the harbours, rail roads and other transport networks are vital for the Dutch society and economy to function.

For a good to surpass the entire supply chain and arrive at the right destination on time, a complex process of planning is necessary. The transport and logistics sector are dependent on the use of Internet, because a network communication systems makes the complex logistics process easier to execute. Also multiple equipment and machineries to facilitate the transport through the entire supply chain are Internet dependent. [43] The Internet is an essential factor in the logistic process and the physical transportation process to execute the task. The transport and logistic sector is therefore an excellent candidate to focus this research on because there are multiple vulnerabilities to exploit.[44] These vulnerabilities will be explained in more detail in the chapter four of this research.

---

[41] Ministerie van Economische Zaken (2015) 'Topsectoren, Logisitek' Jaarbericht Sectoren http://topsectoren.nl/documenten/topsectoren/Jaarbericht-sectoren-2015_2015-02-13_204.pdf
[42] Government Industry Canada (2015) 'Logistics and Supply Chain Management' Government Definitions and Statistics. Latest accessed on 19-05-2014 <http://www.ic.gc.ca/eic/site/dsib-logi.nsf/eng/h_pj00541.html>
[43] Ruske, K. (2011) 'Transportation & Logistics 2030 Volume 4: Securing the supply chain'. PwC Supply Chain Management Institute. pp. 1-52 < http://www.pwc.com/tl2030.>
[44] Ministerie van Economische Zaken (2015) 'Topsectoren, Logisitek' Jaarbericht Sectoren http://topsectoren.nl/documenten/topsectoren/Jaarbericht-sectoren-2015_2015-02-13_204.pdf

The transport and logistics sector includes the four transportation modes of trucking, rail, air and marine.[45] However, in order to make the research more manageable in the current time frame this research will mainly put emphasis on the marine and trucker mode of transport. Because the sector still contains wide range of companies, organizations, products and users this research will focus on the entities that use Portbase as their network communication system. Portbase offers a port community system which is both used by the Port of Amsterdam and the Port of Rotterdam to communicate with their entire supply chain. Thus, this research will mainly refer to parties connected to the network of Portbase communication system.

2.1.4 Economic barriers

Economic barriers is the main problem where this research is focusing on when studying the transport and logistic sector. In order to comprehend the problem that these barriers cause for the market and the entire safety of the Dutch cyber society it is important to understand what economic barriers are.

Economic barriers are common to all sorts of markets but the effect depends on the characteristic of the specific market. An economic barrier to the cyber security market is an obstacle that hinders companies or civil society to reach and optimal level of cyber security.[46] These economic barriers have an effect on the governments and markets ability to improve the level of cyber security in the Netherlands as it disturbs the market process. These barriers are initially seen as market failures because without direction or policy the problem will not solve itself.[47] Examples of economic barriers in the cyber security field are: misaligned incentives, asymmetric information and network externalities. All these barriers constrain cyber security investment and improvement in the private and public sector. These barriers will be explained and applied to the transport and logistic sector in more detail in the next section of this chapter.

---

[45] Government Industry Canada (2015) 'Logistics and Supply Chain Management' Government Definitions and Statistics. Latest accessed on 19-05-2014 <http://www.ic.gc.ca/eic/site/dsib-logi.nsf/eng/h_pj00541.html>

46 Moore, T. (2011) Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University, Center for Research on Computation and Society. pp 1-21

47 A Anderson, R., Böhme, R., Clayton, R. and Moore, T. (2008) 'Security Economics and The Internal Market.' Research Report ENISA pp 1-114

2.2 Theories about economic barriers

This section will go deeper into the theory behind economic barriers and provide an overview of the perception on the theory of main scholars in the academic field of economic and information security.

2.2.1 Introduction

Michiel van Eeten and Johannes Bauer argue that for many years there was one common view which proclaimed that cyber security depended on the quality of the technical protection measures.[48] The focus lay only on the technical aspect of security, which created a competitive competition between hackers and ICT security firms to undo each other's work. For instance security effectiveness could be increased by enhanced access of control policy models, updated firewalls and superior proof of cryptology protocols. Van Eeten points out that the thought was that a lack of cyber security simply could be solved if better technical detective and evaluation mechanisms are developed.[49] Nowadays, a more nuanced and economical line of thought has made its entrance in the information security debate.

The first causes of insufficient cyber security were already researched and analysed by academia in the beginning of the nineties. The causes were explained by legal, political and structural implications that the use of Internet generates.

Bibi van den Berg explains that a lack of cyber security can be explained through legal implications.[50] There are indefinite legal jurisdiction issues due to that cyber-attacks easily can be executed across borders. Thereby due to the rapid development of new technics it is difficult to create law that can comprehend all the technical problems.

According to Milton Meuller there are also many political causes for insufficient cyber security due to the limitations embedded in the very nature of the Internet and its technical structure. Governments, private organizations and users all try to influence and control the Internet, but the technical structure of the Internet and cyberspace prevents one entity to control all.[51]

---

[48] Bauer, J. and van Eeten, M. (2009), 'Cybersecurity: Stakeholder incentives, externalities, and policy options.' Telecommunications Policy, Science direct, Vol 33, Nr 10, pp. 706–719

[49] Ibid.

[50] Van den Berg, B. and Leenes, R, (2013). 'Abort, retry, fail: Scoping techno-regulation and other techno-effects.' Human Law and Computer Law: Comparative Perspectives, edited by M. Hildebrandt and J. Gaakeer. Dordrecht, Heidelberg, London: Springer.

51 Mueller, M. (2010) Networks and States, The Global Politics of Internet Governance. The Mitt Press. First edition

Therefore ownership is shared between governments, private companies and the users. Because nobody owns the Internet and cyberspace, it is difficult to apply rules and regulations. All parties need to be involved to apply the rules. The willingness to cooperate of governments, companies, users are all necessary to apply and uphold the rules.[52]

The technical structural causes are that the Internet offers many new opportunities for people to take an advantage of the Internet and commit a crime. The structure of the Internet thereby also offers anonymity and a way to come away with the crime. An example of a structural cause is: that even though almost all parties in the world are against child pornography, there is still an online community of child pornographers that are able to exchange materials in their network. Thus, creating perfect regulating mechanism by design is not possible because skilled people can work around these regulations by design.[53]

However, in the beginning of the 21st century Taylor Moore and many other scholars brought a more economical line of thought in the information security debate.
Moore started to look and search beyond technical measures to improve cyber security. The thought that technical measures are critical for maintaining cyber security remains, but Moore started arguing that regulation on the Internet is more complex and does not only depend on technical measures.[54] Since 2001 academia have tried to synthesize the knowledge of information systems and security with an economic perspective to create an interdisciplinary field of Information Security Economics.[55] Over the years an extensive body of knowledge and multiple economic theories were developed. The new field focuses on the idea that vulnerability of internet security lies not only on the technical factors, but is also driven by economic incentives.[56] There will always be a competition between superiority of the hackers who attack systems and by people who develop technical protection mechanisms. But the balance of the fight can be influenced by using economic incentives.[57]
Moore argues that the following economic barriers influence the improvement of cyber security: information asymmetries, misaligned incentives and network externalities. In this research these three barriers are researched in regards to the Dutch transport and logistics sector.

52 Mueller, M. (2010) Networks and States, The Global Politics of Internet Governance. The Mitt Press. First edition
53 Ibid.
54 Moore, T. (2011) Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University, Center for Research on Computation and Society. pp 1-21
55 van Eeten, M. and Mueller, M. (2013) Where is governance in Internet Governance? New Media Society, 15
56 Ibid.
57 Ibid.

According to Moore these barriers are based on the premises that security systems often fail due to the fact that organizations who are in charge of the security do not bear the full costs of a security failure.[58]

Besides Moore other scholars introduce economic perspective and economic barrier theories as a threat to a safe cyber domain. For example, according to Brent Rowe and Michael Gallaher there are two main economic barriers which constrain cyber security improvement and investments. The first economic barrier is that there is a lack of complete information concerning cyber security and cyber-attacks. [59] Fabio Bisogni agrees with Rowe and Gallaher and recognizes the challenges of uncomplete information and low availability of cyber-attacks data.[60] Bisogni states that information sharing is key to overcome this barrier.

Obstacles of the sharing of information and its negative consequences has been widely recognized in the literature for instance, by Stewart Baker and Melanie Schneck-Teplinsky. They state that the fear of reputation damage is one of the main obstacles to information sharing. When organizations withhold information regarding cyber-attack the consequence is that the public quality assurance is impaired.[61]

The second barrier Rowe and Gallaher propose is the economic barrier of negative externalities. They argue that negative externalities and the public-goods nature of cyber security in markets causes organizations to underinvest in cyber security. The state that organizations' cyber security investments will generate more social benefits in excess of the targeted private benefits.[62] Thus, the motivations and goals of the market clash and these negative externalities causes organizations to invest less than the optimum level of investment.[63]

---

[58] Moore, T. (2011) Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University, Center for Research on Computation and Society. pp 1-21
Rowe, B. and Gallaher, M. (2006) 'Private sector cyber security investment strategies: An empirical analysis.' 5th workshop WEIS06. latest accessed on 19-11-2015 <http://www.econinfosec.org/archive/weis2006/docs/18.pdf>

[60] Bisogni, F., Cavallini, S. and Di Trocchio, S. (2011) 'Cybersecurity at European Level: The Role of Information Availability.' Communication & Strategies, Vol 81 Nr. 1, pp 105-124.

[61] Baker, S. and Schneck-Teplinsky, M. (2010) 'Spurring the Private Sector: Indirect Federal Regulation of Cybersecurity in the US. in Cybercrimes: A Multidisciplinary Analysis, Springer. Chapter 15, pp 239-263

[62] Rowe, B. and Gallaher, M. (2006) 'Private sector cyber security investment strategies: An empirical analysis.' 5th workshop WEIS06. latest accessed on 19-11-2015 <http://www.econinfosec.org/archive/weis2006/docs/18.pdf>

[63] Ibid.

In addition, Nathan Sales argues that organizations refrain from investing in cyber security because negative externalities and free-riding challenges. Sales states that due to these challenges organization act out of self-interests in order to ensure business continuity. [64]

Moreover, Ross Anderson and Böhme Rainer proposes another economic barrier. Namely the economic barrier of network externalities. This barrier focusses on the 'winner takes it all effect' and stimulates organizations to only invest when the rest of the market is willing to invest in cyber security.[65] This barrier is caused by the principle that most security products only are value when multiple other users have made the same choice of investing in the security product.

Taylor Moore, Ross Anderson, Michiel van Eeten, Bruce Schneier, Milton Meuller, Johannes Bauer, Shari Pfleeger and Rachel Rue, Rowe Brent, Michael Gallaher and Böhme Rainer are the main scholars in the academic field of economics of information security. This literature review is used to create an overview of the scholars' understanding of the imperfections in the information security market. This will assist in the operationalization of economic barriers in order to map the problem in the Dutch transport and logistics sector. The theory of economic barriers describes why investments and development in cyber security are deficient. This research aims to establish if the Dutch transport and logistics sector is vulnerable to these economic barriers in regards to cyber security investment.
Although scholars uses different names for similar economic barriers and some only point out one or two, this research will focus on the following three economic barriers which play a role in the security investment process and are addressed in the literature. These economic barriers are: misaligned incentives, information asymmetric, and network externalities. The next sections of this chapter will explain and discuss all three theoretical economic barriers in regards to cyber security.

[64] Sales, N. (2013) 'Regulating Cybersecurity.' Northwestern University Law Review. Vol. 107 Nr 4, pp 1503 – 1568.
[65] Anderson, R., Böhme, R., Clayton, R. and Moore, T. (2008) 'Security Economics and The Internal Market.' Research Report ENISA pp 1-114

2.2.2 Misaligned incentives

Moore argues that misaligned incentives is the key problem which functions as an economic barrier to improve cyber security. He states that the risk of using online systems is allocated poorly. A security system often fails when the one who pays is not the one who bear the costs.[66] Moore explains that the players in the market have different incentives and reasons to enhance cyber security or not. As long as the risks are allocated unequally, some players of the market are unwilling to make the necessary investments in cyber security.[67] Most likely a choice for reducing costs and increasing efficiency will be made.
For instance, why would the Port of Rotterdam focus more in cyber security to protect their system, if an attack and breach of their container position system does not cost them? The costs are transferred to the customer whose package was not delivered because criminals emptied the container before the content could be transported further through the supply chain.[68]

In addition, in the Dutch society companies endeavor to create profit, therefore their short- and long-term decisions are based on profitability.[69] The companies try to find a balance between reducing cost and creating for example secure software. Bruce Schneier argues that the companies are overlooking some of the additional unexpected costs and benefits because they for instance pay attention to the total costs of insecure software or other security products. Schneier points out that a lot of costs are not calculated in the business models of the companies. This problem is known as an externality, which is basically: "*the costs of a decision that is borne by people other than those making the decision*."[70] According to Schneier companies will not spend more money on cyber security because, the costs are not reflected in the market transaction. For example, the transport companies have found out that having both their control systems and IT network run on the same IP infrastructure offers extensive efficiency gains.[71] However, this architecture of the system creates extra vulnerabilities in the system. The safer option would be to use separate infrastructures. But unfortunately, using separate IT networks

[66] Moore, T. (2008) Information Security Economics and Beyond. Information Security Summit. latest accessed on 19-11-2015 <http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf>
[67] Moore, T. (2011) Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University, Center for Research on Computation and Society. pp 1-21
[68] Europol Public Information (2013) 'Hackers deployed to facilitate drugs smuggling', Intelligence Notification 004-2013, The Hague
[69]Schneier, B. (2006) Information Security and Externalities, European Network and Information Security Agency Quarterly. Vol 2, Nr 4. <http://www.enisa.europa.eu/publications/eqr-archive/issues/eqr-q4-2006-vol.-2-no.-4>
[70] Ibid.
[71] Moore, T. (2011) Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University, Center for Research on Computation and Society. pp 1-21

is more expensive for the companies and requires more investment.[72] However, the companies are not at risk for extensional damages when the vulnerabilities in the system are exploited. The customers and users have to account for the damages and these costs are not reflected in the market transaction. Hereby, companies have an incentive to focus on efficiency instead of investing in security.

Thus, there is a challenge to find a balance between efficiency and resilience of the IT system. This means there is a trade-off between security and efficiency, which also suggests there is an optimal level of insecurity and investment.[73] However, it is important to understand that even when there is an optimal level of investment, no supply chain will ever be 100 percent secure.[74] Technology can help increase security, but people will always be the most critical link.[75] A level of insecurity will always play a role. Insecurity is accepted by the market, because not using the Internet at all will eventually cost the market more than the damage of cyber-attacks. For instance, the time that a parcel will surpass the entire supply chain in the transport and logistics sector will dramatically increase when no IT and network communications systems can be used.

Unfortunately over the years organizations have taken more and more risks and increasing their insecurity level concerning cyber security. Benjamin Dean argues that even a moral hazard occurs because the one making the decisions and taken the risks does not endure the burden and costs of those risks.[76] Dean explains when there is a lack of liability and responsibility in the market regarding cyber security organizations tend to act on self-interests. It is therefore good for the market to find a balance between the trade-off of security and efficiency.

Summarizing, the problem is that the party making the decision on the trade-off of security and efficiency is not the one bearing the cost and the loss in the end. The party taking the risks will not be hold accountable for the negative consequences. This misaligned incentive makes improving cyber security in an IT system difficult.

[72] Moore, T. (2011) Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University, Center for Research on Computation and Society. pp 1-21
[73] Ibid.
[74] van Eeten, M. and Mueller, M. (2013) Where is governance in Internet Governance? New Media Society, 15
[75] Ruske, K. (2011) 'Transportation & Logistics 2030 Volume 4: Securing the supply chain'. PwC Supply Chain Management Institute. pp. 1-52 < http://www.pwc.com/tl2030.>
[76] Dean, B. 'Why Companies Have Little Incentive to Invest in Cybersecurity.' The Conversation. Accessed on 4-04-2015 <http://theconversation.com/why-companies-have-littleincentive-to-invest-in-cybersecurity-37570

2.2.3 Asymmetric information

Another economic barrier is the problem of asymmetric information. Many companies nowadays argue that there is too much data and information and that they are overwhelmed by this.[77] However according to Rowe Brent and Michael Gallaher the problem is that the data and information is asymmetric, there is namely a scarcity of relevant data regarding cyber security. This scarcity and lack of relevant data creates an inefficient market which constrains cyber security improvement.[78] For instance, all the numbers regarding cybercrime attacks and costs are rough estimations.

Shari Pfleeger and Rachel Rue argue that most companies do not want to share their security breaches with the public because doing so they will reveal the weaknesses of their company. The companies fear that their tarnished reputation will cost them customers, because they will switch to another company who did not have to encounter a cyber-attack.[79] Furthermore, companies fear that sharing information on data breaches reveals crucial information to competitors. In this case the company can lose their competitive position in the market if they have to reveal the ins and outs of their technology. [80]

When companies conceal their vulnerabilities and cyber-attacks it becomes unclear which company or product is secure or insecure. This combination of secrecy and uncertainty creates a problem for the market. George Akerlof explains this problem through his thought experiment of a market of 'lemons' (bad used cars).[81] Akerlof describes a market with good and bad products, but only the seller knows which product is good and which product is bad. The good product is worth 4.000 euro while the bad product is only worth 2.000 euro.[82] The problem is that one might expect that the price of the product will be 3.000 euro. However, not one person with a good product will sell the product. Eventually driving the market price to 2.000 euro which causes the market to be flooded with bad products because nobody with a good product is willing to sell. The theory is that no customer wants to pay for quality that he or she cannot

[77] Moore, T. (2008) Information Security Economics and Beyond. Information Security Summit. latest accessed on 19-11-2015 <http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf>
[78] Rowe, B. and Gallaher, M. (2006) 'Private sector cyber security investment strategies: An empirical analysis.' 5th workshop WEIS06. latest accessed on 19-11-2015 <http://www.econinfosec.org/archive/weis2006/docs/18.pdf>
[79] Pfleeger, S.L. and Golinelli, D. (2008), 'Cybersecurity Economic Issues, Corporate Approaches and Challenges to Decisionmaking'. RAND Research Brief. <http://www.rand.org/pubs/research_briefs/RB9365-1.html>
[80] Ibid.
[81] Akerlof, G. A. (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. Quarterly Journal of Economics, Vol 84 Nr 3, pp 488-500.
[82] Ibid.

measure.[83] In addition, no company will invest more to improve the quality and security of its product if they only expect to earn the market price of 2.000.

Anderson argues that the market of security systems is a market of 'lemons' as well.[84] IT companies state that their systems are secure, however the customer is unwilling to pay for the quality of protection of the system if it is not backed up with reliable data.[85] The resistance of the customers to pay more causes IT companies to be disinclined to improve cyber security. The lack of reliable data causes an inevitable spiral where both customer and company are unwilling to focus on cyber security. Thus, the fact that we do not know the real costs and threats of cybercrime causes constrains and barriers to reach an optimal level of cyber security.[86] Stewart Baker and Melanie Schneck-Teplinsky state that there is a great need for information sharing, but the companies in the transport and logistics sector prefer to maintain secrecy on the cyber threat their companies encounter. Baker and Schneck-Teplinsky pinpoint reputation damage, anti-trust and high competition as obstacles to information sharing and the reason why companies in the transport and logistics sector prefer secrecy.[87]

To sum up, asymmetric information in the market causes a barrier for the players to improve cyber security. The consumers who are in need of cyber security do not want to invest in cyber security because they cannot measure the quality of the product. And the security providers in the market do not invest more in their security products because they cannot have great returns from their investments if the customers are unwilling to invest and pay more for the products.

2.2.4 Network externalities

In every market there are externalities, according to Moore and Anderson cyber security improvement and investment is particularly constrained by network externalities.[88] Network externalities are created by the economic principle of the 'Winner takes it all'. It explains why

[83] Akerlof, G. A. (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. Quarterly Journal of Economics, Vol 84 Nr 3, pp 488-500.
[84] Anderson, R. (2001) 'Why Information Security is Hard: An Economic Perspective.' University of Cambridge Computer Laboratory, pp 1-8
[85] Ibid.
[86] Nieuwenhuizen, M.A.X (2015) 'Responsible partners in need of a little incentive', Governance of Cyber Security, Crisis and Security Management, Leiden University.
[87] Baker, S. and Schneck-Teplinsky, M. (2010) 'Spurring the Private Sector: Indirect Federal Regulation of Cybersecurity in the US. in Cybercrimes: A Multidisciplinary Analysis, Springer. Chapter 15, pp 239-263
[88] Anderson, R., Böhme, R., Clayton, R. and Moore, T. (2008) 'Security Economics and The Internal Market.' Research Report ENISA pp 1-114

certain tech companies, network systems and security product have such a dominance in the market. Network externality is defined as: "*a change in the benefit, or surplus, that an agent derives from a good when the number of other agents consuming the same kind of good changes."*[89]

Most markets have the problem of externalities, however in other markets than the IT security market externalities are presented as a smaller threat. This is due to the fact that in other markets consumers can respond by buying and using other products. The IT security market on the other hand is affected with by the network effect of the 'winner takes all'. There are only a couple of large IT companies who control the market. [90] Bruce Schneier argues that it is difficult for new or smaller companies to deliver security products due to monopolies and the already established network value of the other large companies. The greater the network, the more valuable it becomes because it creates an ongoing spiral.[91] For example: having the most applications and features attracts developers, which after that attracts uses, which then again attracts new developers. The 'winner takes it all' effect limits consumers in their choice and can reduce the overall quality of the security, because the monopoly on the market does not challenge companies to advance cyber security.[92]

In addition, Böhme Rainer states that network externalities apply as well for security protocols or advance technologies. Every person part of the network communication system should invest in the same security protocols or advance technology in order to create value to the security protocols and advance technology.[93] Rainer explains why many of security protocols and upgrades of Internet protocols fail to reach a widespread implementation. The benefits of these safer protocols are not realized until numerous users in the market upgraded to the same safer protocols. This discourages user to invest and implement the safer protocols early on. An example is the use of the IPv4 or IPv6 protocol to run an organizations system on. The protocol of IPv6 is much safer than the protocol of IPv4. However, the challenge is to get the entire

[89] Margolis, E. and Liebowitz, S. J. (2000) 'Network Externalities Effects.' North Carolina State University. latest accessed on 19-11-2015 <https://www.utdallas.edu/~liebowit/palgrave/network.html>
[90] Ibid.
[91] Schneier, B. (2006) Information Security and Externalities, European Network and Information Security Agency Quarterly. Vol 2, Nr 4. <http://www.enisa.europa.eu/publications/eqr-archive/issues/eqr-q4-2006-vol.-2-no.-4>
[92] Ibid.
[93] Anderson, R., Böhme, R., Clayton, R. and Moore, T. (2008) 'Security Economics and The Internal Market.' Research Report ENISA pp 1-114

market to switch and invest in the safer protocol of IPv6.[94] The value of a system depends on the weakest link in the chain because the value is derived from the network as a whole. If you are outside the network you have a disadvantage in the market. Everyone needs to switch to IPv6 to make it safe and valuable for investors to invest in.[95]
Although, it is important to remember that there are not only negative externalities because there are also positive externalities. For instance, when a consumer decides to buy a virus scan, the overall security will increase.[96]

2.3 Summary economics of information security debate

In the previous section the theory of economic barriers is discussed, along with the multiple views of the key academia in the economics of information and security debate. Summarizing, most academia recognize asymmetric information, misaligned incentives and network externalities as the most problematic economic barriers.

Although academia pinpoint the economic barriers as a significant cause for the lack of cyber security, it should be questioned if this theory applies to all sectors and countries. This research will challenge the economic barrier theory and analyse if the theory applies to the Dutch transport and logistics sector. Do the barriers pose a threat to the Dutch cyber domain?
In order to answer the research question this research will emphasize on three economic barriers presented in the beginning of the theoretical framework. The theory of the economic barriers will be used to deduce indicators to establish if the Dutch transport and logistics sector is vulnerable for economic barriers in regards to cyber security investment. The next chapter will explain how this research will be conducted in more detail.

[94] NCTV, (2013) National Cybersecurity beeld 4. Cybersecurity Nederland < https://www.nctv.nl/onderwerpen/cybersecurity/>
[95] Anderson, R., Böhme, R., Clayton, R. and Moore, T. (2008) 'Security Economics and The Internal Market.' Research Report ENISA pp 1-114
[96] Moore, T. (2011) Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University, Center for Research on Computation and Society. pp 1-21

3. RESEARCH DESIGN

This section will explain how the research will be conducted and how an answer to the research question will be constructed.

3.1 Choice of the research question

In this thesis the following research question will be answered: *In how far is the Dutch transport and logistics sector vulnerable to economic barriers regarding investments in cyber security?*
The research question in this thesis is chosen with well consideration of the academic field of economics and information security, but also due to my personal interest and curiosity for cyber security challenges. The question initially touches upon the quest to understand the problem of insufficient cyber security and the large amount of cyber-attacks in the Netherlands. It strives to find failures in the market that explain the challenge of forming a save cyber domain for the Dutch transport and logistics sector. This research will map the problem of economic barriers in the Netherlands with the focus on the Dutch transport and logistics sector.
The research question stems from the trade-off between: effectiveness vs. security. This dilemma has been in the interest of many scholars, politicians, engineers, lawyers, philosophers and economists before, and will always be highly debated.[97] Hopefully this research, presented from the different cyber security angle, will provide new insights and incite new ideas to challenge the dilemma.
This research question was specifically chosen to determine different views and perspectives of the problem of economic barriers in the Dutch transport and logistics sector. The answer to the question could possibly assist the Dutch government in reviewing their current strategy and evaluate their economic policy to diminish the economic barriers and try to increasing cyber security in the Netherlands.

3.2 Choice of methodology

In order to find an answer to the research question a qualitative research method is selected. The nature of this research will be descripto-explanatory. This means that an accurate

[97] Mueller, M. (2010) Networks and States, The Global Politics of Internet Governance. The Mitt Press. First edition

description of the profile of the Dutch transport and logistics sector and its economic barriers will assist in explaining why the sector is vulnerable to economic barrier or not.[98] The research will consist of two parts, 1) theory, 2) experiences from the field, and 3) analysis.

The first part of the research will mainly be answered through desk research. The first part of the research will consist of a literature review of the academic field of economics and information security in regards to the transport and logistics sector. Sources of evaluation papers, academic literature, policy papers, parliamentary documents, police reports, cybercrime statistics, and theoretical papers will be used to construct the literature review and the research design. In addition the theory of economic barriers in the information security market will be used to establish indicators and criteria to test if there are economic barriers in the Dutch transport sector influencing cyber security investment.
The second part of the thesis will be researched by means of a combination of desk research and interviews in the field. The second part of the research will contain the result of the desk research and in-depth interviews that will be presented in a Dutch case study with a stakeholder analysis. In the last part the case study and operationalized indicators will be used to place the phenomena of economic barriers in context, in order to deduce if the phenomena applies to the Dutch transport and logistics sector.

Thus, this thesis will consist of a qualitative research with a descripto-explanatory nature executed via a literature review of the economic barrier theory in the information security market and a case study of the Dutch transport and logistics sector.

3.3 Legitimation and data gathering

Qualitative research methods offer specific and in-depth information on situations, which eventually lead to a better understanding of a certain case.[99] The single case study perspective is therefore chosen on the grounds that it provides a detailed description and a better understanding of the circumstances of economic barriers in the Netherlands. The unit of

[98] Bryman, A. (2012) 'Social Research Methods. 'Oxford University Press. 4th Edition.
[99] Gill, P., Stewart, K., Treasure E. and Chadwic, B. (2008) "Methods of Data Collection in Qualitative Research: Interviews and Focus Groups." Nature publishing group. <http://www.academia.edu/746649/Methods_of_data_collection_in_qualitative_research_interviews_and_focus_groups>.

analysis is the national level which is a macro perspective.[100] However to make the research feasible in the given time period of the Crisis and Security Management master the research will only focus on one sector in the Dutch economy that is influenced by cyber security threats. This sector will be the transport and logistics sector with an emphasis on the supply chains were ports are involved in the transport process. This sector is chosen on the grounds that it is a recent extremely vulnerable sector for cyber-attacks. The current Internet revolution changed the way organizations in the supply chain can effectively communicate with each other. However, increasing the productivity brought new dangers to the critical infrastructure of ports involved in the supply chain. The transport and logistics sector is not only chosen because they third largest sector that encounters high cyber threat, but also because the cyber threat is quit new to the sector and will probably only increase further in the future.[101]

The method of desk research with the secondary sources of evaluation papers, academic literature, policy papers, parliamentary documents, police reports, cybercrime statistics, and theoretical papers are used to provide information on the case study and the status quo on the cyber security barriers in the Netherlands. But further research through the use of primary sources acquired via interviews with experts is necessary because it offers data on the information flow of the Dutch transport and logistics sector and as well offers information on the stakeholder incentives. The interviews in the field are used to gain more insight and knowledge into the subject. It is important to question and discuss with people from business who deal on a daily bases with the same questions. The knowledge derived from the interviews will substantiate the thesis with practical knowledge from the transport and logistics sector experts.

The interviews were held with different parties that are involved with the research problem. The interviewee of the organizations are specifically chosen based on their experience and knowledge of the Dutch transport and logistics sector and cyber security challenges of their organization.

The Interviewees were:

- Linda van Moors, Security Manger of Portbase
- Ernst-Jan Zwijnenberg, Unitmanager ICT-Security of Hoffmann Bedrijfsrecherche BV
- Monic van der Heyden, IT Manager of Port of Amsterdam

[100] Bryman, A. (2012) 'Social Research Methods. 'Oxford University Press. 4th Edition.
[101] Ministerie van Economische Zaken (2015) 'Topsectoren, Logisitek' Jaarbericht Sectoren http://topsectoren.nl/documenten/topsectoren/Jaarbericht-sectoren-2015_2015-02-13_204.pdf

- Arthur van Dijk, Chairman of Transport & Logistiek Nederland (TLN)

The following four organizations - the Port of Amsterdam, Portbase, Hoffmann and TLN - are selected for an interview because of their stakeholder position in the Dutch transport and logistics sector connected to the use of network communications systems. The stakeholder positions are: software vendors, security providers, service providers and customers. The stakeholder positions in the Dutch transport and logistics sector will be explained in more depth in section 3.4.1.

The interviewees present a view point from different stakeholders in the cyber security market. Portbase is selected because it is the network communications system provider for the Dutch ports on which this thesis specifically focusses on to narrow the subject. Hoffmann is a representative of the security providers as it is the Dutch market leader on cyber security and investigation.[102] It offers other organizations assistance in securing their network system. The Port of Amsterdam can be seen as a service provider because the organization offers transport and logistics services. The Port of Amsterdam is one of the big players in the Dutch transport and logistics sector and uses the Portbase platform to execute their services.[103] In addition, TLN is also a service provider organization as it presents the interest of smaller Dutch transport companies and their main focus is to increase quality, profit and network communications for their customers.[104] There is no interviewee who represents the last stakeholder group of customers who are in need of transport services. It is important to note that statements on customers are only derived from secondary sources and literature.

Furthermore, the experts from the four selected organization do not represent the entire Dutch transport and logistic sector, but their views offer a distinguished look in the sector. Especially on the real life challenges organizations counter of the network communication system of Portbase.

Before the arguments of the transport and logistics sector exports are discussed, the position and perspective of the sector experts needs to be analysed. It is important to understand their perspectives before placing any weight to their opinions and views on the economic barriers in

[102] Hoffmann Website, 'Over ons'. Informatie Hoffmann. Latest accessed on 19-11-2015 <https://www.hoffmannbv.nl/over-ons>

[103] Port of Amsterdam, 'Role and Vision'. Port Information. Website Port of Amsterdam, latest accessed on 19-11-2015 <http://www.portofamsterdam.com/Eng/corporate/role.html>

[104] TLN, 'Transport en Logistiek Nederland: één stem, één geluid.' Doelstellingen TLN. TLN Website, latest accessed on 19-11-2015 <http://www.tln.nl/Organisatie/Doelstelling.aspx#.VbD_3vntmko>

the transport and logistics sector. The analysis will focus on the different groups and their interest and goals. In addition, the position of the interviewee in the organization itself will be discussed.

Portbase

Portbase is an organization that strives to connect all the organization in the transport and logistics sector together because it offers the networked communication system. It is their interest to develop smart ports by using technology.[105] Currently both the Port of Amsterdam and Rotterdam are working with Portbase.

Porbase influence is high due to the monopoly they have in the Dutch market. It is important to remember that Portbase is one of the strongest players in their market.[106] Competition is not a threatening factor for the organization which can influence their investment strategy.

Furthermore, the interviewee is the security manager of Portbase, therefore she is in charge of the cyber security but does not have control on the budget allocation of the organization.

Hoffmann Bv

Hoffmann is the market leader in the field of fraud prevention, cyber security and investigation. The IT consultancy department focuses on increasing cyber security of their clients.[107] Their interest is to gain profit and to place cyber security on the business agenda of other organizations. Due to their experience, knowledge and their position as market leader they possess power to influence the policy making process and decrease the economic barriers.[108]

The interviewee is a unit manager ICT-security and can represent the views in regards to cyber security problems of the organization. However, it is important to remember that their standpoints on the extent of the economic barrier problem can be influenced by the fact that they benefit from stronger government regulations and mandatory security upgrades. Because they are the number one organization that offers advice and consultancy on the new mandatory security regulations.

---

[105] Portbase Website, 'Information Organization'. Website accessed on 19-11-2015 <https://www.portbase.com/>

[106] Ibid.

[107] Hoffmann Website, 'Over ons'. Informatie Hoffmann. Latest accessed on 19-11-2015 <https://www.hoffmannbv.nl/over-ons>

[108] Pfleeger, S.L. and Golinelli, D. (2008), 'Cybersecurity Economic Issues, Corporate Approaches and Challenges to Decisionmaking'. RAND Research Brief. <http://www.rand.org/pubs/research_briefs/RB9365-1.html>

The Port of Amsterdam

The Port of Amsterdam is an old and well established organization, but only entered the private sector three years ago when it was corporatized. The responsibilities of the port are to attract new business, maintain critical infrastructure, and manage shipping traffic safely and efficient.[109] Due to its corporatization the Port of Amsterdam's interest is to gain profit and increase continuity for the organization. It is important to remember that working towards profit in a completive field influences the investment strategy.

In addition, the interviewee is the IT manager of the Port of Amsterdam and hereby is in charge of the cyber security, but not for the specific budged dedicated to the department.

Transport en Logistiek Nederland

TLN is an association that represents the interests of small, medium and large enterprises of the transport and logistics sector. Their goal is to increase the development of the enterprises that they represent in the highly competitive sector.[110] Increasing quality, innovation, sustainability and profit is their interest.[111] TLN has the ability to influence policy making process in regards to decreasing economic barriers, due to their broad network and many members. Their influence reaches even to the European politics.[112]

The interviewee is the chairman of TLN. He can represent the view and ideas of TLN. However, it is important to understand that TLN collects knowledge and experience of the needs and desires of multiple enterprises in the private sector to represent them. But in addition TLN also has its own agenda and ideas in the economic barrier debate.[113]

Like any other person or organization, all the organizations are tainted by bias. But understanding on which position the bias is based aids in creating an understanding of the research problem of this thesis and the security vs efficiency dilemma.

The interviews followed a general interview guide approach to ensure that in every interview general areas of information were collected. However, during the interviews there was some freedom to deviate from the prepared questions.

---

[109] Port of Amsterdam, 'Role and Vision'. Port Information. Website Port of Amsterdam, latest accessed on 19-11-2015 <http://www.portofamsterdam.com/Eng/corporate/role.html>

[110] TLN, 'Transport en Logistiek Nederland: één stem, één geluid.' Doelstellingen TLN. TLN Website, latest accessed on 19-11-2015 <http://www.tln.nl/Organisatie/Doelstelling.aspx#.VbD_3vntmko>

[111] Ibid.

[112] Ibid.

[113] Transport en Logistiek Nederland (2014) 'Cover, container vervoer op de weg.'
TNL Magazine, nr. 21

The general areas of information that were discussed in the interviews are:

- Characteristics of the organization and the job position
- Which economic barriers can be recognized in the transport and logistics sector,
- The indicator questions,
- What kind of future plan the organizations have for cyber security.

3.4 Operationalization of economic barriers

The previous chapter gave a detailed explanation of the economic barriers theory in regards to the information security market. This section will expand on the research of the economic barrier theory and establish criteria to analyse if the Dutch transport and logistics sector is vulnerable to economic barriers in regards to cyber security investments.
The theory of economic barriers explains why cyber security improvement is constrained in the market and why the economic barriers appear in markets. However, the theory is not applied and tested to specific sectors in the Netherlands. The goal of this research is to analyse if the case study of the Dutch transport and logistics sector is consistence with the economic barrier theory. And perhaps, this theory could explain why the Dutch transport and logistics sector is far behind in cyber security enhancement actions compared to other sectors.
The general economic barriers theory stipulates that there are three main economic barriers that influence cyber security in general. These three economic barriers are: misaligned incentives, information asymmetric, and network externalities.

In order to analyse if the Dutch transport and logistics sectors is vulnerable to economic barriers in regards to cyber security investments, indicators and criteria are determined. These indicators and criteria are deduced from the theory of economic barriers and form the basis of the indicator questions. To test the vulnerability of the Dutch transport and logistics sector the following indicator questions will be asked to the sector experts and body of literature. The questions and indicators will be described per economic barrier in next section.

3.4.1 Misaligned incentives

An incentive is something that influence or motivates people's behaviour. There are different kind of incentives that influence people's behaviour and their decision-making process. For instance, the incentives can be based on financial, moral, natural, personal and coercive reasons.[114] The result of for example a business endeavour can be affected due to different incentives, because people's incentives controls their decision-making process.

The definition of misaligned incentives is given by Bill Novak in his work of the development of network communications systems. Novak explains that there are two types of misaligned incentives: "*(1) when the individual's interest is traded off against the group's interest, (2) when the long-term interest are traded off against short-term interests."*[115]

These two types commonly occur when there is an absence of proper rules in the market that control the penalties or reward system of the participants.[116] This is based on the underlying principle that people tent to act in their own self-interest, unless rules prevent or incentivize them to do otherwise.

Thus, these two types of misaligned incentives occur when there is high self-interest in the market. In addition, the lack of responsibility and liability in the market also account to the presence of misaligned incentives.

For instance, when people in the market are focused on their own interests and do not take reasonability for security failures it is likely that people chose efficiency over security. The same amounts for low liability because the absence of proper rules and possibility of penalties in the market encourages people to focus on their self-interests.

Summarizing, misaligned incentives in the market can cause an economic barrier because the organizations who are in charge of security system do not bear the full costs of a security system failure. This premises can be tested by using a stakeholder analysis of the sector. The stakeholder analyses will show how the incentives and goals of the different stakeholders in the Dutch transport and logistics sector are skewed.[117]

---

[114] Kolstad, C., Ulen, T. and Johnson, G. (1990). 'Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?'American Economic Review Vol. 80, Nr. 4, pp 888-901.

[115] Novak, B. (2011) "Misaligned incentives, First theme across acquisition." Software Engineering Institute, Carnegie Mellon University.

[116] Ibid.

[117] Bryman, A. (2012) 'Social Research Methods. 'Oxford University Press. 4th Edition.

The stakeholder analysis will focus on security-enhancing and security-reducing factors. And hereby, determine their position in the security vs. effectivity trade-off.
To establish the barrier of misaligned incentives in the Dutch transport and logistics sector the following questions will be used to analyse the sector.

1) Who are the stakeholders in the Dutch transport and logistics sector and what are their positions in regards to the use of network communications systems?
2) In there a high self-interest in the market to trade-off individual interests vs. group interest and long-term interests vs. short-term interests?
3) Is there lack of responsibility in regards to cyber security in the market?
4) Is there lack of liability in regards to cyber security in the market?

This research will investigate the incentives of the following stakeholder parties of the Dutch transport and logistics sector. The stakeholder parties are: security providers, network communication system providers, service providers and customers

1) Security providers,

Security providers are organizations such as Internet service providers, and white-hat hackers who offer cyber security products and services to the other three stakeholder parties. An example of a security provider firm is Hoffmann bv.

2) Software vendor/Network communication system provider

The Dutch transport and logistics sector uses multiple network communication systems. However this research mainly focusses on the network communication system of Portbase. The network communication system provider is therefore Portbase.

3) Service providers

The service providers are the transport and logistics organizations in the Netherlands. Examples of such organizations are the Port of Amsterdam and Transport and Logistiek Nederland.

4) Customers

This are people or organizations who are in need of transport and logistics services.

Characteristics, incentives and goals of stakeholders are important to investigate because it influences their decision-making processes in regards to cyber security. Is their strategy focused on efficiency or security? Since the incentives between the organizations who are responsible for security and the organizations who benefit from the protection differ in network communications systems. A stakeholder analysis is necessary to establish information on these characteristics, incentives and goals of the stakeholders in the market. In addition, the stakeholder analysis can show the stakeholders positions in regards to self-interests, responsibility and liability.

Organizations use the tool of stakeholder analysis to identify the priorities of other stakeholders in the market in order to adapt their strategy. The stakeholder analysis process offers insights on possible misunderstandings and clashing goals in the market which can threaten the success of a cooperation endeavour.[118] When multiple stakeholders are part of the network communication system, clashing goals can cause failure in the security system.

In this thesis the same method will be used to establish the goals and incentives of the stakeholders in the Dutch transport and logistics sector. The analysis is used to find the misunderstandings and clashing interests in the market. The indicator questions stated above represent the basis of a stakeholder analysis and the bases of misaligned incentives. The indicator questions are relevant in researching the sectors vulnerability for misaligned incentives in the market, because they assist in identifying the incentives of stakeholders.

Both desk research and the data from the interviews will be used to analyse the incentives of the Dutch transport and logistics sector stakeholders and investigate if they are misaligned.

3.4.2 Asymmetric information

Asymmetric information is a common concept in markets developed by G. Akerlof. He argues that asymmetric information in a market appears when five questions are answered 'Yes". These five question will be used as criteria to assess if asymmetric information applies to the Dutch transport and logistics sector. To test the barrier of asymmetric information in the Dutch transport and logistics sector, the questions will be applied to Dutch case study. The following

[118] Lewis, P., Saunders, and M. Thornhill, A. (2009) 'Research methods for business students', Pearson Education Limited, 5th Revised edition

six questions are constructed from Akerlof's theory and are adapted to the Dutch transport and logistics sector and will be used in this thesis.

1) Who are the buyer and seller of security products in the Dutch transport and logistics sector?
2) Are users of the network communication systems unable to assess the value of the additional security products they need to buy to protect the system?
3) Is there an incentive for security product sellers to pass of low quality security products for high quality security products?
4) Have security products sellers no way yet to demonstrate the quality of the product?
5) Is it important for the buyer to inquire the quality because a low quality security product can hurt him or her later?
6) Is there a lack of effective public quality assurance of security products in the Dutch transport and logistics sector?

These questions are selected to demonstrate possible causal factors of asymmetric information in the market. These causal factors are based on the premises that it is important to determine if customers are able to determine the quality of security products and services. These causal factors are derived from Akerlof's theory on asymmetric information in markets. Akerlof developed the theory of asymmetric information in the market based on the used car market, but the theory can be applied to other markets as well. Especially the above six questions which Akerlof uses to explain asymmetric information can be applied to markets in general.[119] Akerlof's theory is a well-established theory in the academic field of economics of information security and in the academic field of economics and decision-making processes.[120] Akerlof's theory on asymmetric information is especially selected in this research, because the conditions can be used to test if the Dutch transport and logistics sector is vulnerable for the problem of asymmetric information. Information to answer these questions will be obtained by a combination of desk research and the interviews with the experts.

[119] Anderson, R., Böhme, R., Clayton, R. and Moore, T. (2008) 'Security Economics and The Internal Market.' Research Report ENISA pp 1-114

[120] Akerlof, G. A. (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. Quarterly Journal of Economics, Vol 84 Nr 3, pp 488-500.

3.4.3 Network externalities

Although externalities play a role in every market, three characteristics of a market increase the negative effect network externalities can have on cyber security. The three characteristics of a market which causes significant network externalities are: a strong network effect, high homing costs and a low demand for differentiated products.

1) Strong network effect

A network effect is strong when the value of the product increases if more people use the product. For instance, Facebook becomes more valuable and popular, the more people sign up. The value is derived from the network as a whole. If you are outside the network you have a disadvantage in the market.

2) High homing costs

High homing costs come from multihoming which is the use of multiple similar services from different providers. For instance, an Internet user can connect his or her computer device to multiple Internet Services Providers. The cost of using two Internet Services Providers are higher than just connecting to one of the competitive organizations that provide internet services. It does not only cost more money to use both services, but also more time to constantly switch between the two services. The higher the homing costs will be the more likely the customer is to lose his or her motivation to maintain affiliation with both of the competing Internet Services Providers.[121] High homing costs incites people to choose for one organization or network.

3) Low demand for differentiated products.

The last characteristics of the market is that there is a low demand for differentiated products. When there is a low demand for differentiated products it is difficult to sell slightly modified

[121] Song, V. (2013)'Comments Off on Social Networks: Winner Takes All?' The online economy, Strategy and entrepreneurship. Harvard University

but not identical product to consumers.[122] When there is no need for special tailored products it is difficult for the completive companies in the market to brand their product as different or special to create demand.

Thus, to analyze if cyber security improvement is constrained by network externalities the following questions will be used:

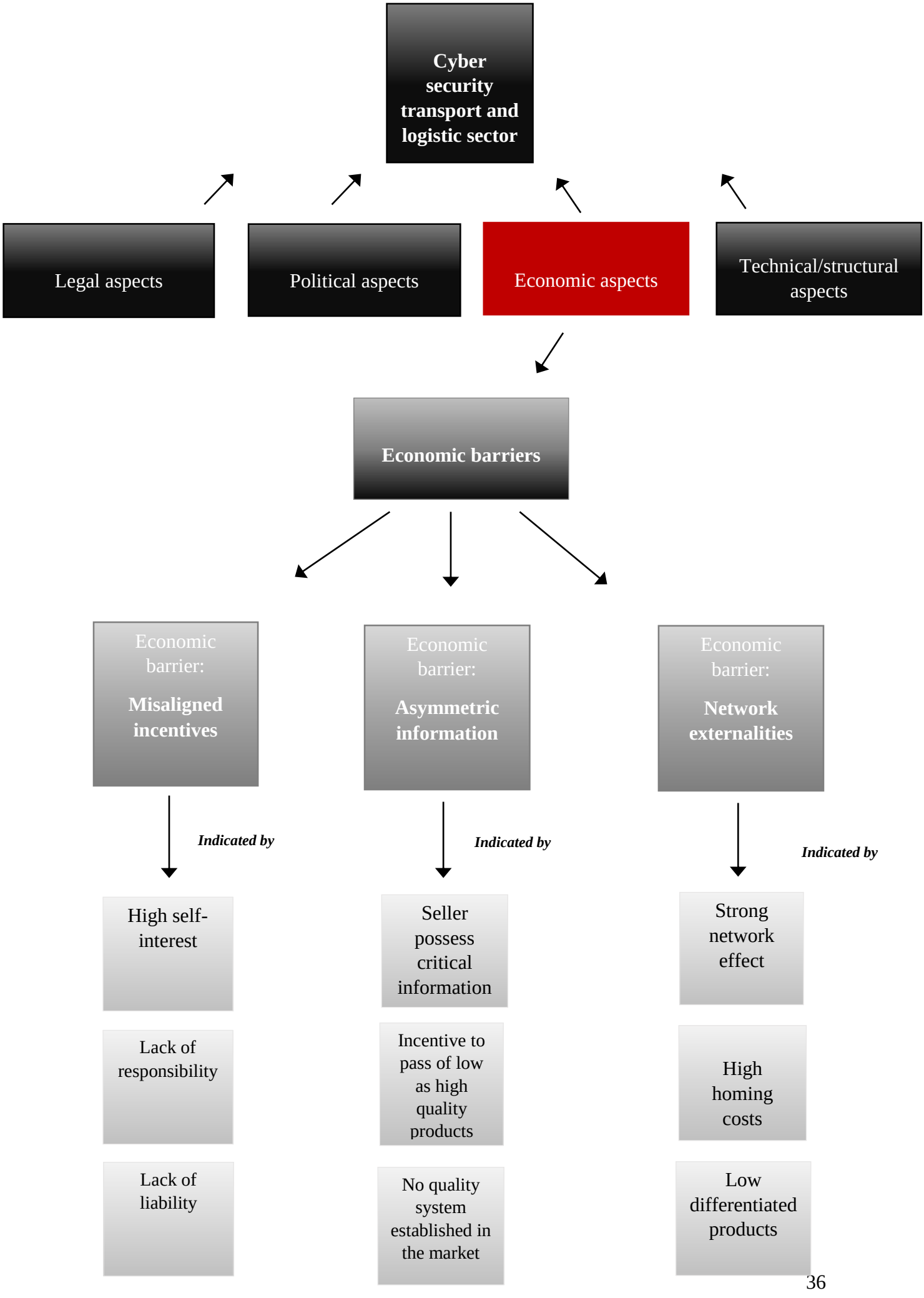
1) Is there a strong network effect for security products in the Dutch transport and logistics sector?
2) Are there high homing costs, when the Dutch transport and logistics sector uses different security product providers?
3) Is there a low demand for differentiated security products in the Dutch transport and logistics sector?

These indicator questions are selected because a positive answer to these questions represent the basis of the problem of the economic barrier of network externalities. The economic barrier of network externalities is likely to affect markets when the characteristics of high homing costs, a strong network effect and a low demand for differentiated products can be found in the market. These indicator questions assist in determining if the Dutch transport and logistics sector is vulnerable and threatened by the economic barrier of network externalities. A combination of desk research and interviews with transport and logistics sector experts will be used in order to check if the three criteria apply to the Dutch transport and logistics sector.

Overall, these question are specifically selected to understand and graph a better picture of the economic barriers and the Dutch transport and logistics sector. Many characteristics of the market influence the threat economic barriers pose to the sector. The indicators and the characteristics of the Dutch transport and logistics sector can assist in mapping the point of failure in this market. It is therefore important to examine the entire problem of insufficient cyber security and not only point to the barriers itself. The profile of the Dutch transport and logistic sector will be discussed in the next chapter to analyse if the sector shows multiple characteristics that instigate economic barriers in the market.

[122] Merholz, P., Wilkens, T., Schauer, B. and Verba, D. (2008) 'Subject To Change: Creating Great Products & Services for an Uncertain World: Adaptive Path on Design' O'Reilly Media, First edition

As explained, there are reasons why the barriers arise and why a sector is more or less vulnerable to economic barriers in regards to cyber security. Theory of the academic field of economics of information security explains causal links between indicators, economic barriers and cyber-attacks. This thesis is not verifying the causality of these links, but this thesis tries to falsify the theory of economic barriers by researching if the Dutch transport and logistics sector shows the same indicators and conditions the theory describes. Thus, to test whether the theory of economic barriers is true in the situation of the Dutch transport and logistics sector. On the next page a scheme will illustrate all facets of the economic barrier problem. This scheme will assist in focussing on the entirety of the markets problems, vulnerabilities and failures.


Cyber security transport and logistic sector
Legal aspects
Political aspects
Economic aspects
Technical/structural aspects
Economic barriers
Economic barrier: Misaligned incentives
Economic barrier: Asymmetric information
Economic barrier: Network externalities
Indicated by
Indicated by
Indicated by
High self-interest
Lack of responsibility
Lack of liability
Seller possess critical information
Incentive to pass of low as high quality products
No quality system established in the market
Strong network effect
High homing costs
Low differentiated products

3.6 Limitations of this choice of methodology

Any research methodology comes with its vulnerabilities. This also accounts for the qualitative research method with the focus on a descripto-explanatory method. Qualitative research especially combined with a single case study perspective lacks in statistics and the evidence that the same phenomena or theory can apply to other case studies. This research will therefore only make statements on the Dutch case study.

In addition, the interviews are done with transport and logistics sector experts, but they only account for 4 opinions and views of the sector. Their views will not be generalized but their origin of their arguments will be studied and placed in the debate on economic barriers in the Dutch transport and logistics sector. Every research has to endure some bias, but to limit this effect the case study will clarify the positions and companies of the interviewee.

Concluding, the qualitative research design of descripto-explantory is appropriate to research the economic barriers in the Dutch transport and logistics sector because descripto-explanatory offers practical information and an insight on the disruption of the barriers to the market.[123]

[123] Lewis, P., Saunders, and M. Thornhill, A. (2009) 'Research methods for business students', Pearson Education Limited, 5th Revised edition

4. DUTCH CASE STUDY

4.1 Introduction

The Dutch transport and logistics sector is like any sector in the Netherlands a target for cyber-attacks and obligated to consider cyber security.[124] This chapter will elaborate on why the Dutch transport and logistics sector is especially in need of cyber security. Furthermore this chapter will discuss the cyber security threat towards network communications systems in the Dutch transport and logistics sector in more detail. In addition, this chapter will review the characteristics of the Dutch transport and logistics sector. The focus will especially be on the characteristics which make the sector more vulnerable for insufficient cyber security of the Dutch cyber domain. The characteristics will be discussed from the literature and sector experts' perspective. In the end the vulnerability to the Dutch transport and logistics sector per economic barrier will be analysed and discussed.

4.2 Cyber security and the Dutch transport and logistics sector

Over the years the Dutch transport and logistics sector grew rapidly and created two large mainports: Schiphol and the area of Rijnmond which is mainly based around the Port of Rotterdam. The two mainports placed the Netherlands on a top-position in Europe in regards to the transport and logistics sector.[125] The Netherlands are seen as the gateway to Europe. In order for these logistics hubs to function and develop the use of Internet was essential.[126] For instance, the Internet is used in the transport and logistics sector for: GPS track and trace, communication between the different transport parties such as forwarders, transport companies, logistic centres and terminals and various governmental parties like customs and environmental authorities, and controlling transport equipment machinery.[127] These services created opportunities for the Dutch transport and logistics sector to progress. The Port of Rotterdam even promotes itself as

[124] Nationaal Cyber Security Centrum (2015) Cybersecuritybeeld Nederland 2015. Ministerie van Veiligheid en Justitie. < https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015%5B2%5D.html>
[125] Rijksoverheid (2013) 'Strategisch aanvalsplan The Netherlands: Digital Gateway to Europe'. <https://www.rijksoverheid.nl/documenten/rapporten/2013/07/02/strategisch-aanvalsplan-the-netherlands-digital-gateway-to-europe>
[126] Ibid.
[127] VPRO (2015) 'De slimste haven van de wereld'. Tegenlicht Uitzending 30 April 2015 <http://www.npo.nl/vpro-tegenlicht/26-04-2015/VPWON_1232883>

the smartest port based on their extensive use of technology and communications systems.[128] Nowadays, the transport and logistics sector grew with the use of the Internet into one of the nine Dutch economic top sectors, and is for 10% accountable for the total economic added value in the Netherlands.

Besides, the advantages the use of Internet offers, there are also pitfalls that come with the use of Internet. For instance, since the transport and logistics sector is a growing and technological developing sector, it is also vulnerable to cybercrime. Every year the Dutch economy loses over Euro 8.8 billion due to cybercrime. The transport and logistics sector is accountable for 7 percent of these cybercrime costs.[129]
The next section will elaborate on the risks the Dutch transport and logistics sector encounter with the use of internet and network communications systems. First, the specific threat that comes with the use of network communications system in the Dutch transport and logistics sector will be explained. In addition, examples of other threats towards the Dutch transport and logistics sector will be discussed below.

4.3 Current cyber threats, risks and assets

As explained above the transport and logistics sector gradually increases the use of ICT. The use of ICT can tremendously maximize the capacity and efficiency of the transport process.[130] A continuous flow of data between companies and governments throughout the entire supply chain is necessary to achieve this capacity.[131] However, with the newly established dependency on ICT the possible damage that can be caused by a cyber-attack rises as well. New weak points in the sector develop when systems like GPS tracking or real-time control applications are more frequently used.[132] This section will explain the vulnerabilities in greater detail.

[128] VPRO (2015) 'De slimste haven van de wereld'. Tegenlicht Uitzending 30 April 2015 <http://www.npo.nl/vpro-tegenlicht/26-04-2015/VPWON_1232883>
[129] HSD, (2014) Cyber Crime Costs The Netherlands 8.8 Billion Euros Per Year. The Hague Security Delta Website. Latest accessed on 14-01-2015 <https://www.thehaguesecuritydelta.com/news/newsitem/191>
[130] Ruske, K. (2011) 'Transportation & Logistics 2030 Volume 4: Securing the supply chain'. PwC Supply Chain Management Institute. pp. 1-52 < http://www.pwc.com/tl2030.>
[131] Ibid.
[132] Ibid.

4.3.1 System vulnerability

Cybercrime and cyber-attacks in the transport and logistics sector occurs as a significant threat to the Netherlands. Every day companies in the transport and logistics sector in the Netherlands are confronted with cyber-attacks.[133] For example, especially the Dutch ports encounter high risk of cyber-attacks as their operation system offer opportunities for drug trafficking and looting.[134] There is always a hidden 'backdoor' in the system which criminals can use to exploit the system for their own advantages. These system vulnerabilities refer to technique, the human factor or the organization.[135] Criminals can access and hack the system from their own computer or gain access by simply handing a tempered USB to one of the people who are working in the port.

These vulnerabilities can account for any organization, but the transport and logistics sector presents more vulnerable.[136] The multiple organization involved in the entire supply chain and the lack of continuous responsibility of a good that is transported through the entire supply chain makes it extra vulnerable. There is not one person or organization that is responsible for a good all the time which creates extra 'backdoors' in the entire system.[137]

These 'backdoors' in the system are used by people for their own advantaged and allowing people to infiltrate the GPS tracking system and use the data for drug trafficking and looting.[138] However, there are also other threats such as cyber terrorism and political hacking because the transport and logistics sector present as a suitable target because the sector is responsible for some critical infrastructure.[139]

4.3.2 GPS tracking and network communication systems

The ports use a network communication system that works on an open mobile network that offers a platform where all the information and data on the location of ships and the containment

---

[133] Gehem, M., Usanov, A. Frinking, E. Rademaker, M. (2015) Accessing Cyber Security, A Meta-Analysis of Threats, Trends, And Responses to Cyber Attacks. The Hague Centre for Strategic Studies, The Hague, pp. 1-101

[134] Nationaal Cyber Security Centrum (2015) Cybersecuritybeeld Nederland 2015. Ministerie van Veiligheid en Justitie. < https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015%5B2%5D.html>

[135] Hoffman Website, 'Cyber security strategy'. Hoffmann bv website, Latest accessed on 19-11-2015 <http://www.hoffmannbv.nl/diensten/ict-security>

[136] WeiS, 'Information Security Economics' WeiS website, latest accessed on 19-11-2015 http://infosecon.net/

[137] Ruske, K. (2011) 'Transportation & Logistics 2030 Volume 4: Securing the supply chain'. PwC Supply Chain Management Institute. pp. 1-52 < http://www.pwc.com/tl2030.>

[138] Ministerie van Economische Zaken (2015) 'Topsectoren, Logisitek' Jaarbericht Sectoren http://topsectoren.nl/documenten/topsectoren/Jaarbericht-sectoren-2015_2015-02-13_204.pdf

[139] NCTV, (2013) National Cybersecurity beeld 4. Cybersecurity Nederland < https://www.nctv.nl/onderwerpen/cybersecurity/>

are stored.[140] This system provides efficiency as all the parties in the supply chain can communicate with each other and access data of the transport process. For instance, when a container ship arrives at the port it has to report to the harbourmaster and inform him or her about the content of its shipment. To increase the process of the containers through the port it is efficient when the companies who will be responsible for transporting the containers further down the supply chain are already aware that the container has arrived in the port.[141] Through the network communication system the other transport companies can access the data of all the shipments and trace where the containers are. Besides that, the data of the shipments only have to be entered in the data base once, while formerly the data had to be sent individually to for instance the harbourmaster, customs and other transport companies. Most of the data is based on GPS tracking information. Thus, the network communication system offers efficiency and adds to the smartness of the process.[142]

Except from the great opportunities the network communication systems offer in regards to GPS tracking it also creates negative opportunities for hackers to access the system and collect data.[143] An example of such a cyberattack and threats it creates is the 2013 attack on the Belgium port of Antwerp. In this case a Dutch drug trafficking group used hackers to enter the network community system of the port of Antwerp.[144] The hackers were able to access data on all the container locations by placing malware in the system. In addition they were also capable of manipulating the system which gave them the opportunity to pick up the containers which contained drugs without making the port and the shipping companies aware of this collection.[145] Having control over the movement and location of the containers for two years the drug traffickers in the Antwerp port were able to actually know where the drugs were and when they needed to be picked up. What they did was infiltrating the system using malware and in only one year time the drug trafficking group was already able to use thousands of containers to ship drugs.[146] The problem of the port of Antwerp was that they were unaware of the holes in their system and cyber risks and threat. The Europol report on the attack concluded that if the port

[140] Portbase Website, 'Information Organization'. Website accessed on 19-11-2015 <https://www.portbase.com/>
[141] VPRO (2015) 'De slimste haven van de wereld'. Tegenlicht Uitzending 30 April 2015 <http://www.npo.nl/vpro-tegenlicht/26-04-2015/VPWON_1232883>
[142] Ibid.
[143] Ibid.
[144] Europol Public Information (2013) 'Hackers deployed to facilitate drugs smuggling', Intelligence Notification 004-2013, The Hague
[145] Ibid
[146] Wainwright, R. (2014) The Internet Organised Crime Threat Assessment. The -IOCTA Report EUROPOL <https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta>

of Antwerp had taken better responsibility for security and had had a stronger security policy in which they had focused more on cyber-attack, the damaging information breach could have been prevented.[147]

Besides drugs trafficking, looting is also a common crime where cybercriminals infiltrate the GPS tracking system to find out where precious and valuable cargo is transported from the port with trucks to easy accessible parking lots. Transport & Logistiek Nederland presented in their research of security on the road that the amount of looting rises every year and the dependency on Internet is one of the causing factors of the increase.[148]

4.3.3 Other cyber threats

On top of infiltrating the network communication system to track the containers and use for drugs trafficking the network community system is also targeted by cybercriminals for other purposes. These purposes could be: human trafficking, cyber espionage, cyber terrorism, political hacking or just for fun.

Besides, drugs, laptops and mobile phones the precious cargo could also be human beings. This highly illegal activity still take place and hackers could misuse the communication system to their advantage. Human trafficking is a serious problem and only becomes more difficult to detect when cyber-attacks are used to pass through the system undetected.

The transport and logistics sector is also vulnerable for cyber espionage. For example, the port of Rotterdam is a target for cyber espionage. The well developed and successful organization possess great business strategies and techniques where other organizations might be interested in.[149]

Another threat could come from cyber terrorists or political hackers who want to send a message or damage the critical infrastructure. Hackers could for example execute Ddos attacks in order to overflow the system. If the system overflows the communication platform is not reachable and no longer able to provide it services to the clients. Such an attack could have tedious consequences because nobody has access to the data. The entire supply chain will lock up. Furthermore, another threat could be a virus or malware that crashes or corrupt the entire system

[147] Wainwright, R. (2014) The Internet Organised Crime Threat Assessment. The -IOCTA Report EUROPOL <https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta>

[148] Transport en Logistiek Nederland (2014) 'Cover, container vervoer op de weg.' TNL Magazine, nr. 21

[149] Wainwright, R. (2014) The Internet Organised Crime Threat Assessment. The -IOCTA Report EUROPOL <https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta>

and also disrupts the execution of the task of the companies that use the network communication systems.

However, the problem of the lack of cyber security in the supply chain is not easy to solve. The transport and logistics sector problem of cyber security is not only because of their change towards a technical system. Many other factors, parties and stakes play a role in the security process. For instance, some of these threats are easy for the ports to protect themselves from with relatively little effort. For instance, investing in awareness training for the employees prevents easy infiltration attacks through spear phishing mails and USB's. However, to protect themselves from other vulnerabilities may require more investment and large steps taken by the private and public sector.

4.4 Initiatives and countermeasures to improve cyber security

In the economics of information security debate academia propose multiple solutions to diminish economic barriers and reduce the vulnerability of a sector. The theoretical solutions discussed in the literature are: cyber-insurance, liability regulations and information disclosure. The public and private sector can implement these options to enhance cyber security investments in the Dutch transport and logistics sector. Due to the large amount of cybercrime costs, threats and vulnerabilities in the Dutch transport and logistics sector, cyber resilience and security should be an important focus point for the Dutch government and the private sector. Some steps have been taken by both the Dutch government and the private sector, but the focus and development on cyber security are still low.[150]

However, the Dutch government started some initiatives to fight cybercrime and improve the safety of the Dutch cyber domain. For instance, the Netherlands created their first cyber security strategy (NCSS) in 2011.[151] The main vision of the Dutch cyber security policy is based on the four concepts of: self-regulation, cooperation, transparency and knowledge development. The goal of the Dutch government is to go from 'being aware' to 'being capable' in the cyber

[150] Gehem, M., Usanov, A. Frinking, E. Rademaker, M. (2015) Accessing Cyber Security, A Meta-Analysis of Threats, Trends, And Responses to Cyber Attacks. The Hague Centre for Strategic Studies, The Hague, pp. 1-101

[151] NCTV, (2011) National Cybersecurity Strategy 1. Cyber security Nederland <https://www.nctv.nl/onderwerpen/cybersecurity/>

security domain.[152] However, the current strategy has not lead to a concrete legal framework, political or economic strategy to increase cyber security.

Furthermore, another step taken by the government that can affect barriers in the market is that the Dutch government is trying to create laws for critical infrastructure to improve information sharing. Information Sharing and Analysis Centres (ISAC's) is the main initiative with the focus on information sharing. ISAC's are based on voluntary public-private collaboration relationships which are organized per sector.[153] For example, the Dutch ports have their own ISAC as well. Their goal is to create a knowledge network where the participants exchange information and experience with each other on cyber security. The information is only shared on a strategic level in order to prevent the sharing of personal data. The problem of the ISAC is that it will always have to remain small and operate with a trusted group of people in order for companies to feel safe to share inside information on a voluntary basis.[154] In addition to that it takes time to build up trust and the relationships between the organizations and the ISAC's. Moreover the ISAC co-operates only with large companies; small companies therefore are not approached.

In order to increase the process of information sharing the Dutch government is at the moment working on legislation that forces companies to report to authorities and harmed customers if there was a breach of personal data or if the breach presents a threat towards the society.[155] On June 17, 2013 a proposal of the new bill is presented to the Second Chamber of The Netherlands. Eventually on the 10th of February 2015 the new bill was approved by the Second Chamber.[156] The new data breach bill adds to the Data Protection bill a duty to report data breaches of personal data. Both private and public organizations that process personal data in their systems

[152] NCTV, (2013) National Cybersecurity Strategy 2. Cybersecurity Nederland
< https://www.nctv.nl/onderwerpen/cybersecurity/>
[153] NCSC (2013) 'ISACS, Publieke-Private samenwerking.' Nationaal Cyber Security Centrum, samenwerking dossier. latest accessed on 19-11-2015 <https://www.ncsc.nl/samenwerking/publiek-private-samenwerking/isacs.html>
[154] Nieuwenhuizen, M.A.X (2015) 'Responsible partners in need of a little incentive', Governance of Cyber Security, Crisis and Security Management, Leiden University.
[155] Rijksoverheid (2015) 'Meldplicht datalekken en uitbreiding boetebevoegdheid Cbp 1 januari 2016 van kracht.' Actueel Rijksoverheid nieuws. latest accessed on 08-10-2015 <http://www.rijksoverheid.nl/nieuws/2015/07/10/meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-cbp-1-januari-2016-van-kracht.html>
[156] Eerste Kamer der State Generaal (2013) 'Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp.' Eerste Kamer Wetvoorstellen. Latest accessed by 03-08-2015 <https://www.eerstekamer.nl/wetsvoorstel/33662_meldplicht_datalekken_en>

are required to report security breaches that lead to theft, loss or abuse of personal data.[157] If the organization does not report the breach to the Dutch Data Protection Authority (DPA) and, also inform the persons concerned, the organization can be charged with a fine of €810.000 or 10% of the profit of the organization.[158]

With this newly created obligation to report data leaks, the government wants to limit the consequences and improve the preservation and restoration of the personal data. Additionally, the reports of the data breaches offer a way to gather more information about the attacks and breaches of security systems. This legislation is a step in the right direction to overcome the economic barrier of information asymmetric. Especially because the Dutch government proposes firm fines when companies do not apply with the legislation. However, the Council of State argues that the definition of personal data is not wide enough to obligate companies to report all cyber-attacks on their IT systems. Companies have still room for maneuver to hide their vulnerabilities of their services from the outside world. [159] This also accounts for the terms 'socially destabilizing', 'theft', 'abuse' or a 'threat' towards society. For example when an attack to the system occurs the company only is enforced to report the attack when actually personal data is stolen or changed. When the system is just entered but not changed the company does not have the legal obligation to report the attack.[160] The bill will be enforced on the first of January 2016. Since, the Dutch government is still working on the implementation of this kind of legislation it is unclear how effective the legislation will be.

Thereby, the private sector remains very vulnerable in regards to cyber security and is not eager to advance cyber security. According to the security company Hoffmann 90 percent of the companies systems in the transport and logistics sector can still easily be breached by a cyber-attack.[161] In addition, according to the ICT barometer survey barley 25 percent of the Dutch companies have established and formalized an official cyber security policy. And only 40

[157] Rijksoverheid (2015) 'Meldplicht datalekken en uitbreiding boetebevoegdheid Cbp 1 januari 2016 van kracht.' Actueel Rijksoverheid nieuws. latest accessed on 08-10-2015 <http://www.rijksoverheid.nl/nieuws/2015/07/10/meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-cbp-1-januari-2016-van-kracht.html>

[158] Eerste Kamer (2015) 'Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens.' Staatsblad van het Koninkrijk der Nederlanden. <https://www.eerstekamer.nl/behandeling/20150619/publicatie_wet/document3/f=/vjuvb9mu87zu.pdf>

[159] Raad van State (2014) 'Samenvatting advies nota van wijziging meldplicht datalekken.' Samenvattingen Adviezen. latest accessed on 19-11-2015 <https://www.raadvanstate.nl/adviezen/samenvattingen/tekst-samenvatting.html?id=288&summary_only=>

[160] Ibid.

[161] Nieuwenhuizen, M.A.X 29-05-2015 Interview met Ernst-Jan Zwijnenberg, Unitmanager ICT-Security of Hoffmann Bedrijfsrecherche BV, Almere

percent of the Dutch transport and logistics companies consider to focus on cyber security in the coming 5 years.[162]
In addition, the Dutch governmental campaign to promote the safer protocol of IP v6 instead of the IP v4 protocol has not been effective yet in stimulating organizations to invest in IP v6. Most of the Dutch transport and logistics sector companies still run on the IP v4 protocol. [163]

Unfortunately, the fact remains that the current strategy of the transport and logistics sector and the Dutch government does not lead to a concrete legal framework and political or economic strategy to increase cyber security. The Dutch government and the sector have not shown many initiatives to focus on increasing cyber security. Only on the topics of child pornography, terrorism and privacy the Dutch government focussed their policy. However, there is no policy in place that focusses on critical infrastructure of the Dutch transport and logistics sector.

Furthermore, this thesis focuses on the economic reason why the threat towards the supply chain is so high and why the transport and logistics sector is reluctant to advance cyber security. Theories on which factors and characteristics cause the problem of lack of cyber security in the transport and logistics sector will be discussed in the next section.

4.5 Analysis

This section will provide an overview of the perspectives and experiences of the Dutch transport and logistics sector experts and the perspectives offered in the literature. The fact that the economic barriers theoretically apply to the Dutch transport and logistics sector does not necessary mean that the sector encounters them as economic barriers and recognizes the sector's vulnerabilities. Through the in-depth interviews diverse views on the economic barriers came to light. Experts from the sector might experience different economic barriers in practice than what academics predicted. Thus, this section will provide an overview of the vulnerabilities of Dutch transport and logistics sector concerning economic barriers based on the literature and sector expert's interviews.

[162] Ernst & Young (2011) 'ICT Barometer over cybercrime' Jaargang 11 Beveilginswereld <http://www.beveiligingswereld.nl/files/ICTBarometercybercrime2011.pdf>
[163] NCTV, (2013) National Cybersecurity beeld 4. Cybersecurity Nederland < https://www.nctv.nl/onderwerpen/cybersecurity/>

4.5.1 Misaligned incentives

The economic barrier of misaligned incentives stems from the trade-off between security and efficiency. The possible Dutch transport and logistics sector vulnerability to economic barriers regarding cyber security investments will be analysed by using the indicator questions presented in chapter 3 of this research.

1) Who are the stakeholders in the Dutch transport and logistics sector and what are their positions in regards to the use of network communications systems?

The stakeholders in the Dutch transport and logistics sector regarding cyber security are: software vendors, security providers, service providers and customers. The software vendors are responsible for the creation of the network communications system. In this research Portbase is the network communications system provider. Portbase delivers the platform and is in control of creating the security software of the system itself.[164] If transport and logistics companies want to use additional cyber security such as firewalls, virus scans and cyber protocols they can buy the assistance of security providers who offer the infrastructure, services and products to secure companies.

The service providers are part of the network communication system because they use it to communicate with all the other companies in the supply chain and send or collect data through the system. The customer is also part of the network and communications system because they can follow the containers with track and trace options.

2) In there a high self-interest in the market to trade-off individual interests vs. group interest and long-term interests vs. short-term interests?

Yes, there is a high self-interest in the market to choose individual interests over the group interests and the short-term interests over the long-term interests.

[164] Portbase Website, 'Information Organization'. Website accessed on 19-11-2015 <https://www.portbase.com/>

First, interviewee from Portbase recognizes the economic barrier of misaligned incentives in the Dutch transport and logistics sector and the sectors vulnerability for it. The interviewee from Portbase acknowledge the difficulties that come with the dilemma of security vs efficiency. For instance, Portbase clients base consist of a couple of large companies, but a great portion of the clients are medium or small size companies. Linda van Moors from Portbase says that it is especially difficult for the small companies to comply with the expensive and time sensitive cyber security protection mechanism. Cyber security therefore is not a topic on their business agenda. Therefore, efficiency is on top of the business agendas of most companies in order to compete in the competitive market.[165] Self-interests is very important for Portbase customers, because their business continuity is dependent on it.

In general the Dutch transport and logistics sector is known for the skills, services and knowledge on goods and information flows. The sector focusses on effective, durable and efficient transport through the entire chain from raw materials to the final product.[166]

In order to execute their services the sector is characterized by low profit margins and high investments in ICT.[167] The sector is highly competitive, and to improve continuity and their position in the market the companies in the sector focus on cost minimization and revenue maximization. The companies in the sector are driven to invest in ICT to increase the smartness and efficiency of their transport services.[168] However, due to the low profit margins and liability clauses, security features in the system and security products are not a priority of the companies

In addition, the competition is excessively in the sector, it does not matter how or who transports a package, the goal of the customer is that it arrives on the predestined place safe and on time. There is no need for specific tailored services for the customers. But there is a demanding customer culture, because the customer expects an efficiency and a fast transport process. There are many other companies customers can select to deliver their cargo. Therefore, the Dutch transport and logistics sector is also characterized by the high competition in the market. Already explained above the sector companies' focus on decreasing costs and minimalizing revenue in order to improve their position in the market. Besides that, the companies are also driven by development and growth. They will invest in new technologies and new equipment,

[165] Nieuwenhuizen, M.A.X 26-05-2015 Interview met Linda van Moors, Security Manger of Portbase, Rotterdam

[166] Ministerie van Economische Zaken (2015) 'Topsectoren, Logisitek' Jaarbericht Sectoren http://topsectoren.nl/documenten/topsectoren/Jaarbericht-sectoren-2015_2015-02-13_204.pdf

[167] Ministerie van Economische Zaken (2015) 'Topsectoren, Logisitek' Jaarbericht Sectoren http://topsectoren.nl/documenten/topsectoren/Jaarbericht-sectoren-2015_2015-02-13_204.pdf

[168] VPRO (2015) 'De slimste haven van de wereld'. Tegenlicht Uitzending 30 April 2015 <http://www.npo.nl/vpro-tegenlicht/26-04-2015/VPWON_1232883>

but are less prone to focus on continuity and durability. There is little awareness in regards to cyber security and continuity of the company.

In addition, the interviewee Monic van der Heyden from the Port of Amsterdam recognized the economic barrier of misaligned incentives and the sector's vulnerability for it. Especially the class between long and short term incentives are identified as a troubling factor to improve cyber security. Heyden claims that it is difficult to change the organizations culture towards cyber security protection mechanisms. The managers do not see the use and value of updating the software all the time. Initially, because the business managers of the Port of Amsterdam find it displeasing and time sensitive especially because they do not see and understand the direct profit of these actions. In addition, the Port of Amsterdam is not to blame or has to bear the costs when the Port of Amsterdam' system fails due to a cyber-attack. [169]
Furthermore, the interviewee from Hoffmann experiences the economic barrier of misaligned incentives in the Dutch transport and logistics sector and recognizes the sector's vulnerability to the economic barrier. The interviewee form Hoffmann argues that the problem of misaligned incentives is one of the most important economic barriers of constraining the transport and logistics organisations to invest in cyber security. This economic barrier is recognizable in the fact that many companies do not see the short term benefit of investing in cyber security, especially because they do not bear the cost when there is a security breach.[170] Ernst-Jan Zwijnenberg the interviewee form Hoffmann point out that there is no good business case for cyber security and therefore the incentives are misaligned. Cyber security is nowadays seen as an IT problem while it should be seen as a business problem. Business managers do not place cyber security on the business agenda because they think there are no direct cost to the company when it encounters a cyber-attack.[171]

Thus, the problem of the stakeholders in the Dutch transport and logistics sector is that the sector's characteristics of high competitiveness forces many companies to act on self-interests. Both forms of misaligned incentives can be found in this case study.

[169] Nieuwenhuizen, M.A.X. 20-05-2015 Interview met Monic van der Heyden, IT Manager of Port of Amsterdam, Amsterdam
[170] Moore, T. (2011) Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University, Center for Research on Computation and Society. pp 1-21
[171] Nieuwenhuizen, M.A.X 29-05-2015 Interview met Ernst-Jan Zwijnenberg, Unitmanager ICT-Security of Hoffmann Bedrijfsrecherche BV, Almere

1) When the individual's interest is traded of against the group's interest,

Example: A security software vendor decides to save money on extra encryption code in order to increase the benefits of functionality. The software vendor saves money, but takes risks for the customer who does not buy a secure product.

2) When the long-term interests are traded off against short-term interests.

Example: a security provider decides to introduce a product early without full test trials to the market in order to be the first, save money and improve their market position. Later on it is most likely that the cost of vulnerability patching due to a lack of test trails will increase rapidly.

Below, table one shows an overview of the incentive for security enhancing and security reducing actions from the different stakeholders. The structure of the table is based on Baurer's perspective of the misaligned incentive economic barrier.

Table 1 Stakeholder analysis based on Baurer's perspective of the misaligned incentive economic barrier. [172]

Stakeholders	Security enhancing	Security reducing
Security providers: Internet service providers, Organizations such as Hoffmann	- Cost of customer help/support - Fear of brand damage and loss of repuation	- Cost of protection measures - High self-intersts - Lack of legal responsibility - Lack of liability regulations - Privacy and anti-trust issues
Software vendors: Network communication system provider Portbase	- Cost of vulnerability and backdoor patching - Fear of brand damage and loss of repuation	- Cost of software development and testing - High self-interst - Benefits of functionality - Lack of legal responsibility - Licensing agreements including hold harmless clauses
Service providers: Transport and logistics companies	- Awareness of cyber security risks - Realistic self-efficacy - Exposure to cybercrime and cyber-attacks	- Poor understanding of risks - Overconfidence - Cost of security products and services
Customers: of transport and logistics services	- Awareness of cyber security risks - Exposure to cybercrime and cyber-attacks	- Poor understanding of risks

The Dutch transport and logistics sector is vulnerable for the economic barrier of misaligned incentive due to fact that it sector has competitive circumstances. It is important for the companies to decrease cost to create a competitive position in the market. The companies will therefore focus on decreasing the costs and minimalizing profits. Hereby, they trade-off individual interests vs. group interest and long-term interests vs. short-term interests.

[172] Bauer, J. and van Eeten, M. (2009), 'Securing cyberspace: Realingin economic incentives in the ICT value net.' TU Delft. WebSci 2009

3) Is there lack of responsibility in regards to cyber security in the market?

Yes, there is low responsibility in the Dutch transport and logistics sector in regards to cyber security. The Dutch transport and logistics sector is characterized by their long supply chain. In the supply chain it is unclear who is responsible for the security and liable for the vulnerabilities in the system. Due to the ambiguity around responsibility organizations start a blame-game when the security of a system fails.[173]

For instance, the long supply chain increases the interdependence between the multiple organizations and contribute to a blame-game of insufficient security.[174] The long supply chain obscures the responsibility feelings for an organization. In the supply chain the accountability of the cargo or container changes fast, which makes it difficult for most companies to imagine and feel the cost when the cargo is stolen. The transport and logistics sector never owns the cargo and therefore does not have to bear the cost when something goes wrong.[175] If the responsibility can be shifted to another party, the companies do not need to fear of reputation losses.[176] Therefore, these companies are not stimulated to invest in cyber security or focus on improving the cyber security of their systems. In the Dutch transport and logistics sector there is a lack of integrated vision between the many freestanding organizations. There is a need for a comprehensive strategy which calls for action of the entirety of the transport and logistics sector to focus on cyber security.

In addition, the interviewee Arthur van Dijk from TLN experiences the economic barrier of misaligned incentives and the vulnerability of the sector. Van Dijk states that between the trade-off of security and efficiency companies in the Dutch transport and logistics sector priorities efficiency. Especially the fact that the companies do not feel responsible for security because they do not bear the costs when the system fails increases the focus on efficiency. Moreover, the interviewee TLN explains that the economic crisis even increased the problem

[173] Bauer, J. and van Eeten, M. (2009), 'Securing cyberspace: Realingin economic incentives in the ICT value net.' TU Delft. WebSci 2009
[174] Ibid.
[175] Ruske, K. (2011) 'Transportation & Logistics 2030 Volume 4: Securing the supply chain'. PwC Supply Chain Management Institute. pp. 1-52 < http://www.pwc.com/tl2030.>
[176] Bauer, J. and van Eeten, M. (2009), 'Securing cyberspace: Realingin economic incentives in the ICT value net.' TU Delft. WebSci 2009

of misaligned incentives in the transport and logistics sectors further, because the small and medium companies do not have the money to priorities security over efficiency.[177]

Furthermore, the interviewee from Port of Amsterdam says that the lack of awareness and responsibility feeling in the Dutch transport and logistics sector is a major influence on why companies are reluctant in advancing cyber security. The interviewee from the Port of Amsterdam states that they had some basic cyber security mechanism in place, but when they recently encountered an attack not only the IT department recognized the necessity of cyber security mechanism but the business managers saw the necessity as well. Shortly after the attack they decided to be responsible and invest more in cyber security. Absence of awareness and experience with cyber-attacks is one factor which constrains cyber security advancement and taking responsibility according to the Port of Amsterdam.[178] Creating awareness could decrease the sector's vulnerability for misaligned incentives because it could incite the sense of reasonability by companies.

4) Is there lack of liability in regards to cyber security in the market?

Yes, there is a lack of liability in regards to cyber security in the Dutch transport and logistics sector. There are little specific liability regulation to protect the critical infrastructure of the Dutch transport and logistics sector.

The interviewee from Hoffmann is aware of the new liability regulation of the Dutch government that enforces companies to take reasonability and notify customers if there was a data breach concerning their personal data. The interviewee from Hoffmann argues that the new Dutch legislation is a large step in the right direction especially because they work with fines and penalties system. He explains that penalty systems is an effective way to stimulate companies to invest and work on the cyber security. Especially when the penalties are high enough to financially disrupt the companies. But, he argues that there is still a necessity for more legislation and that liability in general remains low. The proposed definitions of a security breach are unclear and the Dutch government has a long way to go to perfect its legislation

[177] Nieuwenhuizen, M.A.X 01-06-2015 Interview met Arthur van Dijk, Chairman of Transport & Logistiek Nederland (TLN), Lisserbroek
[178] Ibid.

regarding information disclosure. He definitely expects from the Dutch government to take a strong position to stimulate companies to invest in cyber security[179].

In addition, the interviewee form TLN compares the situation to the Dutch financial sector. The financial sector has seen a rapid grow of cyber security investments in the Netherlands and greatly challenges their cyber security problems. The interviewee from TLN does not detected this trend in the Dutch transport and logistics sector. He argues that this difference is caused by the fact that the financial sector in unable to continue their tasks if they do not focus on security. Moreover, the Dutch government creates strict laws in regards to bank security, thefts and cyber-attacks. A bank is liable when a bank account is hacked, while on the other hand security providers, software vendors and service providers of the Dutch transport and logistics sector are not liable when a data breach occurs. The interviewee from TLN suggests that the Dutch government should consider new liability regulations for the Dutch transport and logistics sector in order to enhance cyber security improvement.[180]

Difference between the literature and the interviews

Both the literature and the interviews describe the economic barriers as a threat towards the Dutch cyber domain. The economic barrier of misaligned incentives is one of the barriers that the sector experts especially appoint to be influencing cyber security and where the Dutch transport and logistics sector is vulnerable to. All the interviewees point out that the cyber security is not presented as a good business case. And for many companies the priority remains on efficiency instead of security. In the literature there is no specific weight connected to the severity of the threat. However, the roots of the misaligned incentive barrier and the dilemma of efficiency vs. security influence the sector's vulnerability of the other economic barriers of asymmetric information and network externality.

Summarizing, if the incentives of the multiple stakeholders are placed together it is only possible to end at an equilibrium where barriers challenge cyber security. Especially the problem for the Dutch transport and logistics sector companies and customers is that there incentives are misaligned with the other stakeholders. The Dutch transport and logistics sector is vulnerable for the barrier because cyber security does not reach the business manager table,

[179] Nieuwenhuizen, M.A.X 29-05-2015 Interview met Ernst-Jan Zwijnenberg, Unitmanager ICT-Security of Hoffmann Bedrijfsrecherche BV, Almere
[180] Nieuwenhuizen, M.A.X 01-06-2015 Interview met Arthur van Dijk, Chairman of Transport & Logistiek Nederland (TLN), Lisserbroek

but remains a responsibility of the IT departments. Security has no priority compared to efficiency. High competiveness, necessary self-interest and a lack of responsibility and liability in the Dutch transport and logistics sector make the sector more susceptible to the economic barrier of misaligned incentives.

4.5.2 Asymmetric information

1) *Who are the buyer and seller of security products in the Dutch transport and logistics sector?*

The software vendors and the security product providers are the sellers. Security products are for instance: encryption protocols, firewalls, and security protocols.

The buyers are the transport and logistics sector companies and the customers who are in need of transport and logistic services.

2) *Are users of the network communication systems unable to assess the value of the additional security products they need to buy to protect the system?*

Yes, the buyers are unable to establish the security quality of for instance the network communication system Portbase. Neither can the buyers assess the quality of other additional security products. The buyers are unable to establish the value of the security products because the sellers are unwilling to show reliable data regarding the quality of the security products.

There is however an ISAC in which Portbase is a partner and shares cyber security challenges. Unfortunately this valuable information to assess quality is only shared with the organizations in the ISAC. The parties in the ISAC's are the Dutch government, the NCSC, the Dutch ports and some large private companies. Customers and the majority of the transport and logistics companies do not have access to the information.

Furthermore, the excessive competition in the sector creates the unwillingness to share information concerning cyber security with the competition. The companies choose secrecy in order to remain there reputation and position in the market.[181]

[181] Ministerie van Economische Zaken (2015) 'Topsectoren, Logisitek' Jaarbericht Sectoren http://topsectoren.nl/documenten/topsectoren/Jaarbericht-sectoren-2015_2015-02-13_204.pdf

3) *Is there an incentive for security product sellers to pass of low quality security products for high quality security products?*

Yes, there is an incentive for security product sellers to pass of low quality product for high quality products. The market is very competitive and in order for the companies to preserve their place in the market they need to attract consumers with supposedly more secure product.

However, the interviewee from Portbase experiences less pressure for performance and competition, due to that they are currently the only organization that provides network communication system services for ports in the Netherlands. Thus, this competitive drive is mainly an incentive for the security product providers.

4) *Have security products sellers no way yet to demonstrate the quality of the product?*

In the cyber domain there are some security labels that demonstrate that the products are up- to date and apply certain standards. Unfortunately there are non-such labels for network communications systems. Thus, besides the ports ISAC and the security labels there is no way yet to determine quality of the security product. Of course no product can be 100 percent secure, but the sellers cannot measure the quality. Especially in regards to cyber security there are very little statistics and data available to assess the quality of cyber security. Also, cyber security products are very complex products where most buyers do not possess the knowledge to establish the quality.

The interviewee from the Port of Amsterdam confirmed asymmetric information as an economic barrier for the Dutch transport and logistics sector and confirms its vulnerability for the economic barrier. The lack of information of cyber threats and the inability of the consumers to establish quality in the sector discourage companies to invest in cyber security. The reason given by the Port of Amsterdam was that the clients do not know where the cyber security problems lie when there is no information regarding cyber threat. The lack of this information available to the public conceals the value of quality. Although the interviewee from the Port of Amsterdam is aware of certain security labels system which are used to indicate security quality levels. She points out that these security labels are very limited and only offer quality indication of a small range of Internet products and services. The interviewee from the Port of Amsterdam

calls attention to the need for a security label which challenges the security quality of the entire supply chain.[182]

Moreover, the interviewee from Hoffmann also experiences the problem asymmetric information and recognizes characteristics of the Dutch transport and logistics sector which makes the sector vulnerable for this economic barrier. The interviewee from Hoffmann recognizes some initiatives of security label system to establish public quality ensures. Unfortunately these initiatives are incapable of tackling the economic barriers down. In order to diminish the effect of the economic barriers yearly audits regarding cyber security and cyber-attacks are necessary for companies. Without major data collecting and sharing methods the cyber security deficit in the Dutch transport and logistics sector will remain.

Hoffmann even states that asymmetric information is key in solving insufficient cyber security. The fact that information of cyber threats requires better availability to the public and the inability of the consumers to establish quality discourage companies to invest in cyber security. According to the interviewee from Hoffmann equal information is necessary to establish numbers and statistics that cyber security is a good business case and forces business managers of companies to focus on cyber security enhancement.

On the other hand, the problem of asymmetric information is not pointed out by the interviewee from Portbase as an economic barrier which constrains cyber security improvement. The interviewee from Portbase points out the growing opportunities and success of the already existing information sharing mechanisms. Moors states that the barriers effect is taken away by information sharing initiatives in the Dutch transport and logistics sector. She acknowledges the effectiveness of the port's ISAC and argues that the ISAC diminish the problem of insufficient public quality assurance methods.

In addition, the interviewee from Portbase strongly suggests that information disclosure should remain on a voluntary basis, because mandatory information disclosure will only increase the threshold for companies to share information. If information disclosure is mandatory, an administrative task will follow after a cyber-attack. Especially smaller companies will be discouraged by this administrative threshold to share information. These companies will try

[182] Nieuwenhuizen, M.A.X. 20-05-2015 Interview met Monic van der Heyden, IT Manager of Port of Amsterdam, Amsterdam

even more to keep the cyber-attack secret, which eventually will stimulate the companies more to withhold information.[183]

5) *Is it important for the buyer to inquire the quality because a low quality security product can hurt him or her later?*

Yes, it is very important for the buyer to inquire the quality. Buying low quality security products comes with a great risks of cyber-attacks and information breaches. The buyer can get serious hurt if the product is not capable of delivering the services it supposed to do. Important data can be breached or the settings in the system can be changed. Cyber-attacks can cause great damage to a company.

6) *Is there a lack of effective public quality assurance of security products in the Dutch transport and logistics sector?*

Yes, currently the security providers and software vendors are not hold responsible for low quality products and the security providers try to keep the vulnerability in the products and services quiet. There is however a new law developed that forces companies to inform their customers when there is a personal data breach in the system. This law only focuses on a breach of personal data, other cyber-attacks are not mandatory to report.

Overall, the Dutch transport and logistics sector is vulnerable for the economic barrier of asymmetric information due to the high competiveness in the sector and the inability to assess the quality of the security products. The interviewee from Hoffman even argues that asymmetric information is the main economic barrier constraining the transport and logistics sector to improve cyber security. The fact that cyber security is not presented as good business case worries the interviewee from Hoffmann. This problem can only be solved by showing quality and efficiency of security products. In order to measure the quality and efficiency the problem of asymmetric information need to be solved by sharing information. People will only become aware and focus on cyber security if they can see the results of their investments. The

[183] Nieuwenhuizen, M.A.X 26-05-2015 Interview met Linda van Moors, Security Manger of Portbase, Rotterdam

interviewee from Hofmann focusses for the future on making people aware of the possibilities and the efficiency of security products.[184]

In addition, the interviewee from TLN recognizes the economic barrier of asymmetric information. TLN specialises also in executing research in the Dutch transport and logistics sector to advance knowledge and business strategies for their customers. Van Dijk from TLN explains that they have difficulty accessing and collecting data in regards to cyber security and cyber-attacks. Even their own customers are not enthusiastic on sharing information with the association.

Moreover, Van Dijk argues that the lack of information sharing is a great problem in the entire Dutch transport and logistics sector. Without sharing the value of quality of security products companies remain discourage to invest in cyber security and eventually cause a downwards market price spiral in the market.

The difference between the literature and the interviews

Academia are all aware of the threat asymmetric information possess to the Dutch transport and logistics sector. However, not all the experts recognize the sector's vulnerability of asymmetric information on cyber security. The interviewee from Portbase strongly suggest that the Dutch government already broke the barrier down by creating ISAC's where information regarding quality of the products can be shared between buyer and seller. The other three sector experts disagree with the interviewee from Portbase and argue that asymmetric information still is working as an economic barrier constructing cyber security improvement.

Summarizing, asymmetric information plays a role of constraining cyber security enhancement especially for the transport and logistics market because it is a competitive sector which prefers secrecy to prevent reputation loss when there is a cyber-attack. When the interviewee from Port of Amsterdam loses its reputation the clients can easily choose to bring their business to the Port of Rotterdam or Antwerp. When the organization decide to keep information regarding security and cyber-attacks secret the consumers cannot determine the quality of the ports or for example other transport organizations. The consumers need this information to make a considered decision on the quality of the product. Without this information the market price

[184] Nieuwenhuizen, M.A.X 29-05-2015 Interview met Ernst-Jan Zwijnenberg, Unitmanager ICT-Security of Hoffmann Bedrijfsrecherche BV, Almere

will decrease and the transport and logistics sector will be discouraged to invest in cyber security and remain vulnerable for the economic barrier.[185]

4.5.3 Network externalities

The characteristics of the Dutch transport and logistics sector demonstrate that the sector is prone to experience the disadvantages of the economic barrier of network externalities.

1) *Is there a strong network effect for security products in the Dutch transport and logistics sector?*

Yes, there is a strong network effect for security products in the Dutch transport and logistics sector. The Dutch transport and logistics sector shows characteristics that are vulnerable for network externalities. Namely the fact that in order for the network communication system of Portbase to work most efficient and with the lowest homing costs all the companies in the supply chain need to be connected and have access to the platform of Portbase. For instance, it will only be efficient if everybody shares the data and can collect it. The transport process of a container will only improve if from the beginning to the end the information is available. For example, a container ships send information in regards of its cargo and time of arrival in the port. The port will respond by sending information out when the containers are loaded on the dock. The trucker can access this data and knows when he can start driving towards to port to pick up the container. If one of these actors is not part of the network there will be an information gap and the transport process cannot be executed efficiently. Furthermore, the fact that there is such a strong network effect in the market provides Portbase with the opportunity to create a monopoly. Their monopoly decreases the incentive for Portbase to invest in the quality of cyber security, because the pressure to outperform other companies is low.

Another example that shows that there is a strong network effect in the transport and logistics sector is the use of IP v6 instead of IP v4. The protocol of IPv6 is much safer than the protocol of IPv4.[186] However, it is difficult to get the entire market to switch and invest in the safer protocol of IPv6.[187] In the Dutch transport and logistics sector only a small amount of

[185] Akerlof, G. A. (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. Quarterly Journal of Economics, Vol 84 Nr 3 pp 488-500.
[186] NCTV, (2013) National Cybersecurity beeld 4. Cybersecurity Nederland
< https://www.nctv.nl/onderwerpen/cybersecurity/>
[187] Ibid.

companies switched to IP v6. Most companies remained on the old protocol of IP v4.[188] Thus, the problem remains that the value of a system depends on the weakest link in the chain. The value is derived from the network as a whole. If you are outside the network you have a disadvantage in the market. The problem is that the network of IP v4 is strong and as a result companies do not want to invest in the IP v6 protocol which is safer.[189] In the Dutch transport and logistics sector the incentives to invest in IP v6 are low due to the strong network effect of IP v4.

Furthermore, Portbase does acknowledge the economic barrier of network externality due to the strong network effect. Portbase mentions its struggle to enforce safe security communication lines when using its network communication platform.[190] For instance the change to IP v6 protocol instead of the IP v4 protocol would increase the cyber security level excessively. However, not all companies are willing to commit to this investment. In order for the platform to be effective multiple actors in the supply chain need to be granted access to the platform and all its information.[191] It is difficult to stimulate the entire supply chain to focus on cyber security and use secure communication lines to protect the entirety of the platform.[192]

Portbase highlighted the problem of network externalities as one of the main barriers which challenges cyber security. For instance, the fact that their network communication system security is dependent on the cyber security enhancement actions their customers take. Portbase sees this barrier as main challenges and proposes that an independent actor should investigate the cyber security problem of the entire supply chain.[193] Even though that the threat for many companies is still low, the risks are high for everyone. Portbase plans to implement stricter security criteria for their customers in the coming 10 years. The time frame is long because they do not expect that the barrier of network externalities will be decreased soon.[194]

Besides, misaligned incentives and asymmetric information the interviewee from TLN recognizes network externalities as an economic barrier in the Dutch transport and logistics

[188] NCTV, (2013) National Cybersecurity Strategy 2. Cybersecurity Nederland <ttps://www.nctv.nl/onderwerpen/cybersecurity/>
[189] NCTV, (2013) National Cybersecurity beeld 4. Cybersecurity Nederland < https://www.nctv.nl/onderwerpen/cybersecurity/>
[190] Nieuwenhuizen, M.A.X 26-05-2015 Interview met Linda van Moors, Security Manger of Portbase, Rotterdam
[191] Ibid
[192] NCTV, (2013) National Cybersecurity Strategy 2. Cybersecurity Nederland <ttps://www.nctv.nl/onderwerpen/cybersecurity/>
[193] Nieuwenhuizen, M.A.X 26-05-2015 Interview met Linda van Moors, Security Manger of Portbase, Rotterdam
[194] Ibid.

sector. A strong network effect in the market causes discouraging factors for companies to invest in enhancing cyber security. If investment only returns profit when multiple parties are willing to do the same it is difficult to start up the investment process. The interviewee from TLN stated that security externalities is even a problem on a higher level. 80 percent of the rules for the transport and logistics sector are decided on a European level. Which means that the norms and security preferences of 28 other states play a role in forming policy on security protocols. It is difficult to convince them all to invest in cyber security enhancement.[195]

Furthermore, the problem of network externalities is as well recognized by the interviewee from Port of Amsterdam as an economic barrier in the transport and logistics sector towards cyber security. Van der Heyden interviewee from the Port of Amsterdam claims that especially the nature of the transport and logistics sector enhanced this economic barrier. The transport supply chain consists of many chains which all use their own IT networks and safety protocols while they all are part of for example the same network communication system. Therefore it could be that one organization has invested a lot and uses many technical protection mechanism, while the organization can still easily be attacked because the other organizations in the system do not use the same precautions.[196]

2) *Are there high homing costs, when the Dutch transport and logistics sector uses different security product providers?*

Yes, there are high homing costs in the Dutch transport and logistics sector when they use different security products providers.[197] The Dutch transport and logistics sector uses multiple technologies and ICT services to provide their services.[198] As explained in the beginning of chapter four, these product range from board computers to entire data warehouse systems. All these tools need different security products to secure the goods and information flow.[199] It is difficult to switch all the time between systems and it is more efficient to collect the data in one

[195] Nieuwenhuizen, M.A.X 01-06-2015 Interview met Arthur van Dijk, Chairman of Transport & Logistiek Nederland (TLN), Lisserbroek
[196] Nieuwenhuizen, M.A.X. 20-05-2015 Interview met Monic van der Heyden, IT Manager of Port of Amsterdam, Amsterdam
[197] Ruske, K. (2011) 'Transportation & Logistics 2030 Volume 4: Securing the supply chain'. PwC Supply Chain Management Institute. pp. 1-52 < http://www.pwc.com/tl2030.>
[198] Nationaal Cyber Security Centrum (2015) Cybersecuritybeeld Nederland 2015. Ministerie van Veiligheid en Justitie. < https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015%5B2%5D.html>
[199] Margolis, E. and Liebowitz, S. J. (2000) 'Network Externalities Effects.' North Carolina State University. latest accessed on 19-11-2015 <https://www.utdallas.edu/~liebowit/palgrave/network.html>

system and invest in cyber security products based on that system.[200] Portbase offers a platform for the supply chains that pass by the Dutch ports of Amsterdam and Rotterdam. Without the network communication system of Portbase the homing costs would be even higher for the companies in the Dutch transport and logistics sector.[201] However, it is important to know that even though Portbase decreases homing costs, they have trouble enforcing cyber security standards and applying security products to the system. Thus, homing cost for addition security products besides Portbase system are still high.

The Dutch transport and logistics sector is characterized by the interdependency of multiple ICT tools and systems that are necessary to execute the sector's tasks. 90 percent of the Transport and logistics companies are highly dependent on the use of ICT.[202] For example tools and products that they use are: navigation systems, board computers, Radio Frequency Identification, Warehouse Management Systems and Transport Management Systems.[203] Portbase offers a platform where all these services can be combined with the network communication system. This system is necessary because otherwise it would be very difficult for companies to apply all these services at the same time. Plus, multiple providers offer these services and products and it is therefore difficult to switch between the services.[204] The network communication system is a necessary platform for the Dutch transport and logistics sector to connect all their ICT tools with each other.

In addition, another characteristic of the Dutch transport and logistics sector is that the sector consists in a couple of large companies, but that there is also space for multiple smaller companies. For example: the larger companies are: TNT, Vos logistics, Port of Rotterdam and P&O Nedlloyd.[205] But, there are also many smaller family companies which offer transport and logistics services. The sector is dependent on network communication systems to execute their services, which means that all the large and small companies share one system. However, it is

[200] Margolis, E. and Liebowitz, S. J. (2000) 'Network Externalities Effects.' North Carolina State University. latest accessed on 19-11-2015 <https://www.utdallas.edu/~liebowit/palgrave/network.html>
[201] Portbase Website, 'Information Organization'. Website latest accessed on 19-11-2015 <https://www.portbase.com/>
[202] Ernst & Young (2011) 'ICT Barometer over cybercrime' Jaargang 11Beveilginswereld <http://www.beveiligingswereld.nl/files/ICTBarometercybercrime2011.pdf>
[203] Kindt P. and van der Meulen, M. . S.J. (2012) 'ICT in transport en logistiek, Voorsprong door initiatief en focus.' ING Sectormanagement Transport & Logistiek <https://www.ing.nl/media/ING_sectormanagement-transport-logistiek_voorsprong-door-initiatief-focus_tcm162-72860.pdf>
[204] Ibid.
[205] Topsectoren (2015) 'Topsector Logisitek, bouwt internationale toppositie uit.' latest accessed on 19-11-2015 <http://topsectoren.nl/logistiek>

more difficult for the smaller companies to find resources to invest in cyber security and keep up with the ICT developments.[206] Therefore, the network communication system is as strong as its weakest link. Thus, the variety of actors in the sector is recognized as a characteristic of the Dutch transport and logistics sector. Another characteristics is that in the last couple of years the sector grew rapidly and with that the dependency of ICT to improve the smartness of the information flows grew as well.[207] This makes it even more difficult for the sector to keep up with the cyber security investment.

Furthermore, the economic barrier of network externalities is as well recognized by the interviewee from Hoffman in the Dutch transport and logistics sector. The interviewee from Hoffmann states that especially the nature of the transport and logistics sector enhanced this economic barrier.[208] The transport supply chain consists of many chains which all use their own IT networks and safety protocols. They need a network communication system to connect them all. Unfortunately due to the 'winner takes it all' effect in the IT market Portbase controls the sector. Portbase does not have competition in the market and therefore the incentive to invest in the quality of the product decreases.[209]

3) *Is there a low demand for differentiated security products in the Dutch transport and logistics sector?*

Yes, in the Dutch transport and logistics sector there is a low demand for differentiated security products. The low demand is caused because the consumer does not need specific tailored products.[210] The consumer is just in need of a product that secures its system, it does not matter who or how this security is established. In addition, security products are not especially branded to the transport and logistics sector, because there is no demand for it.

[206] Kindt P. and van der Meulen, M. . S.J. (2012) 'ICT in transport en logistiek, Voorsprong door initiatief en focus.' ING Sectormanagement Transport & Logistiek <https://www.ing.nl/media/ING_sectormanagement-transport-logistiek_voorsprong-door-initiatief-focus_tcm162-72860.pdf>
[207] Ministerie van Economische Zaken (2015) 'Topsectoren, Logisitek' Jaarbericht Sectoren http://topsectoren.nl/documenten/topsectoren/Jaarbericht-sectoren-2015_2015-02-13_204.pdf
[208] Nieuwenhuizen, M.A.X 29-05-2015 Interview met Ernst-Jan Zwijnenberg, Unitmanager ICT-Security of Hoffmann Bedrijfsrecherche BV, Almere
[209] Ibid.
[210] Ruske, K. (2011) 'Transportation & Logistics 2030 Volume 4: Securing the supply chain'. PwC Supply Chain Management Institute. pp. 1-52 < http://www.pwc.com/tl2030.>

The difference between the literature and the interviews

Both the academia and the sector experts argue that the economic barrier of network externality constrain cyber security improvement. Although the interviewers mostly focus on the strong network effect, the interviewee Hoffmann is the only one who mentions the difficulty of high homing costs.

Moreover, the network externality barrier is also a constraining factor, because the Dutch transport and logistics sector is such a large and important part of many supply chains and is therefore in contact with numerous companies.[211] The special characteristics and nature of the transport and logistics sector creates the extra vulnerability of the security network externalities economic barrier. There are many different actors involved which all have to work with the same protocol, platform and software to use the port communication system. It is therefore difficult to change to a more secure provider that offers similar services, because the entire supply chain needs to be convinced. One company alone will not invest in another product if it is not sure the rest of the supply chain companies will do the same.[212]

4.5.4 Future problems and actions

The sector experts explained their future plans in regards to cyber security investment. They also explained which barrier they assessed most important to challenge concerning the sector's vulnerability of the barriers.

The interviewee from Portbase highlighted the problem of network externalities as one of the main barriers which challenges cyber security. For instance, the fact that their network communication system security is dependent on the cyber security investment and actions their customers take. The interviewee from Portbase sees this barrier as main challenges and proposes that an independent actor should investigate the cyber security problem of the entire supply chain. Even though that the threat for many companies is still low, the risks are high for everyone. Portbase plans to implement stricter security criteria for their customers in the coming

[211] Ruske, K. (2011) 'Transportation & Logistics 2030 Volume 4: Securing the supply chain'. PwC Supply Chain Management Institute. pp. 1-52 < http://www.pwc.com/tl2030.>
[212] Loeb, M.P. and Gordan, L.A. (2003) Sharing Information on Computer Systems Security: An Economic Analysis. Journal of Accounting and Public Policy, Vol 22 Nr. 6

10 years. The time frame is long because they do not expect that the barrier of network externalities will be decreased soon.[213]

On the other hand, the interviewee from the Port of Amsterdam emphasis on the economic barrier of misaligned incentives as main problem. They argue that the companies only focus on the risky short term advantages and not the safer long term options. The Port of Amsterdam will focus on changing the culture of the organization and try to bring cyber security to the business-manager table.[214]

The interviewee from Hoffman argues that asymmetric information is the main economic barrier constraining the transport and logistics sector to invest in cyber security. The fact that cyber security is not presented as good business case worries the interviewee from Hoffmann. This problem can only be solved by showing quality and efficiency of security products. In order to measure the quality and efficiency the problem of asymmetric information need to be solved by sharing information. People will only become aware and invest in cyber security if they can see the results of their investments. The interviewee from Hofmann focusses for the future on making people aware of the possibilities and the efficiency of security products.[215]
The interviewee from TLN agrees with Hofmann and hopes that soon a switch can be made where company cyber risk continuity is an important item during business meetings. The interviewee from TLN hopes that with time the idea of cyber security investment is seen as normal as investing in fire alarms. However, the interviewee from TLN also points out the danger of network externalities. The characteristic of a long supply chain in the transport and logistics sector increase the risk and containment of investment heavily.[216]

[213] Nieuwenhuizen, M.A.X 26-05-2015 Interview met Linda van Moors, Security Manger of Portbase, Rotterdam
[214] Nieuwenhuizen, M.A.X. 20-05-2015 Interview met Monic van der Heyden, IT Manager of Port of Amsterdam, Amsterdam
[215] Nieuwenhuizen, M.A.X 29-05-2015 Interview met Ernst-Jan Zwijnenberg, Unitmanager ICT-Security of Hoffmann Bedrijfsrecherche BV, Almere
[216] Nieuwenhuizen, M.A.X 01-06-2015 Interview met Arthur van Dijk, Chairman of Transport & Logistiek Nederland (TLN), Lisserbroek

4.6 Summary

The Dutch transport and logistics sector has many characteristics that are in common with the indicators of the economic barrier theory. The sector is a highly competitive and fast developing sector. The large supply chain and the use of a network communication system cause problems such as: lack of responsibility, great competition and large network effects which eventually can cause barriers in the market. Also the interviewee recognize the problem of economic barriers and point out the threat these barriers pose to the Dutch society.

The first barrier recognized by the organizations is the problem of misaligned incentives. This economic barrier is recognizable in the fact that many companies do not see the short term benefit of investing in cyber security, especially because they do not bear the cost when there is a security breach.[217] All the companies point out that there is no good business case for cyber security and therefore the incentives are misaligned.

The second barrier of asymmetric information is pointed out by all of the interviewed organization as an economic barrier except by Portbase. First reason given was: the clients do not know where the cyber security problems lie when there is no information regarding cyber threat. And second: the lack of information conceals the value of quality.[218] Why should they invest in expensive security software or other security product if they do not feel and notice the difference in productivity of the security product?

Third, the economic barrier of network externalities is as well recognized by all the organizations as an economic barrier in the transport and logistics sector towards cyber security. Other economic barriers that were mentioned by the interviewee were the lack of awareness and the demanding customers in the Dutch transport and logistics. These problems are not mentioned intensively in the literature on economics of information security, but was recognized by all the experts as an important factor influencing cyber security for organizations.[219] All the interviewed organization pointed out that there is a severe lack of awareness in the transport and logistics sector. They all compared it to the financial and banking

[217] Moore, T. (2011) Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University, Center for Research on Computation and Society. pp 1-21
[218] Nieuwenhuizen, M.A.X 29-05-2015 Interview met Ernst-Jan Zwijnenberg, Unitmanager ICT-Security of Hoffmann Bedrijfsrecherche BV, Almere
[219] Anderson, R., Böhme, R., Clayton, R. and Moore, T. (2008) 'Security Economics and The Internal Market.' Research Report ENISA pp 1-114

sector where cyber security is already an important issue, the transport and logistics sector seems to stay behind on this area.
Thus, the experts of the sector recognized most of the economic barriers discussed in the literature, but also experienced problems of two other economic barriers. The academics view and the transport and logistics sector's views will be analysed and compared in the following chapter.

The theory of economic barriers in the IT market is argued from a general point of view.[220] But the characteristics of the transport and logistics sector show that the economic barrier theory definitely applies to the Dutch transport and logistics sector. In order to develop and use a safe network community systems for the entire transport and logistics sector the Dutch market has to overcome the economic barriers of: asymmetric information, misaligned incentives and security externalities. The indicators questions of the barriers deduced form theory discussed in chapter three of this thesis are used to analyse step by step the sector's vulnerability to economic barriers. The answers showed that the barriers pose a threat to the Dutch cyber domain because the sector possess many susceptible characteristics. However, the Dutch government and the private sector have already taken some step to lessen the effect. Unfortunately, these initiatives are not enough to eradicate the threat the economic barriers pose to the Dutch cyber domain and the Dutch transport and logistics sector. The sector is still constructed by the barriers and should be taken seriously if the Dutch transport and logistics sector wants to continue with their business and develop further.

[220] Anderson, R., Böhme, R., Clayton, R. and Moore, T. (2008) 'Security Economics and The Internal Market.' Research Report ENISA pp 1-114

5. CONCLUSION & DISCUSSION

5.1 Introduction

The objectives of this research were:

- to create a theoretical understanding of economic barriers regarding cyber security
- to map the problem and the vulnerability to economic barriers in the Dutch transport and logistics sector
- to research if these economic barriers are recognized by the transport and logistics sector

The next sections of this chapter will provide an answer to the research question and summarize the objectives of this research. Next this chapter will revisit the methodology of the research and discuss the limitations that come with research design. Furthermore this chapter will offer some policy recommendations for the Dutch government based on the research results. In the end, possible future researches will be discussed.

5.2 Answers to the research question

This thesis has investigated the question: *In how far is the Dutch transport and logistics sector vulnerable to economic barriers regarding investments in cyber security?*

This research used the theory of economic barriers in regards to cyber security to study the deficient cyber security in the Dutch transport and logistics sector. This sector applies new technologies such as network communication systems to increase its efficiency. However, in order to achieve this dependency on ICT increases. This new established efficiency also conveys new vulnerabilities. Multiple scholars argue that the vulnerabilities are not resolved due to economic barriers in the market. The economic barriers are misaligned incentives, asymmetric information and network externalities.

By studying the literature on economic barriers of cyber security and applying this to the Dutch transport and logistics sector, it showed that the sector is vulnerable to economic barriers. The indicators of the economic barriers are all identified and present to a certain level in this sector. In addition, the profile of the Dutch transport and logistic sector shows that the sector has multiple characteristics that instigate economic barriers in the market. These characteristics are: highly competitive, cost reducing, revenue maximizing, diversity of actors and companies, long

supply chains, the necessity of network communications systems, rapid growth of the market and lack of liability and responsibility.

In the field, the economic barriers are recognized by the Dutch transport and logistics sector as an influencing factor in the market. Furthermore, in the field it is recognized that practical initiatives of the government and the private sector lessened the negative effect and consequences of the economic barriers. The ISAC's, the new privacy information sharing legislation, cyber security awareness campaigns and security labels all lessen the effect the barriers have on cyber security. Although, a vulnerable situation remains due to the fact that most initiatives are in an initial phase. More initiatives should be established to reduce the risks of damaging cyber-attacks and improve cyber security in the Dutch transport and logistics sector.

Which barrier the Dutch transport and logistics sector the most vulnerable to is difficult to assess, but the barrier of misaligned incentives represents inequality and which is by itself most difficult to overcome. Moreover, the interviewee put most emphasis on the fact that cyber security is a bad business case and that the perception of cyber security needs to be changed. Changing perception and strategy of the market also serves the mitigation of the other two barriers asymmetric information and network externalities. In addition, for the latter two, first steps to tackle the barriers have been set by the government and the private sector.

Concluding, the barriers are definitely recognized in the literature and by the sector experts. The Dutch transport and logistics sector demonstrates many characteristics and indicators that influence the barriers to obstruct the market. Some initiatives from the government and the private sector are at work in order to weaken the sector's vulnerability of the economic barriers. Yet, in order to tackle the vulnerabilities and the threat the economic barriers pose in regards to cyber security, more steps has to be taken.

5.3 Revisiting the research method

In order to find an answer on the research question this research used a qualitative research method. The method consist of a comprehensive desk research and in-depth interviews with sector experts. In addition, a single case study perspective was used to gain a greater understanding of the Dutch situation in the transport and logistics sector in regards to economic barriers.

First of all, it is important to note that only four interviews were conducted which provides an insight in the arguments and opinions on economic barriers in the transport and logistics sector but does not offer a determined claim, since four is not enough to represent the entire sector. The interviews are influenced by the bias of the interviewer and the interviewees and only represents for a small view in the transport and logistics sector. However, taken these limitations in mind, the results of the interviews do offer valuable information on the Dutch transport and logistics sector and the economic barriers. It presents us with insights on the nature of arguments and the challenges that are necessary to overcome to map the barriers in the Netherlands. This also points to the generalization of this research. This research does not make any claims on the entire sector. This research is designed as a single case study and the results may therefore only account for the Dutch transport and logistics sector. Furthermore research is necessary to determine if the results apply to other countries' transport and logistics sectors or other sectors in general as well.

Moreover, this research adds to the generalization process because this research tests if the general theory of economic barriers in regards to cyber security also can be abstracted and applied to the specific Dutch transport and logistics sector. Even though the research of the phenomena of economic barriers is time and context specific, it does provide an insight in the phenomena and adds to entire body of knowledge or theory. This research adds to the theory of economic barriers in regards to cyber security because it demonstrates that it does not falsify the theory. But on the other hand it also shows through the in-depth interviews that the problems that the literature described are not the only problems recognized that can cause a lack of cyber security investment. In-depth case study research offers more than simple falsification, it also offers a perspective of the falsification line which is important in stimulating further theory building.

Third, it is important to note that this research is partially based on desk-research which is a secondary research source and does not add new information to the subject. However, it does provide a new perspective on the subject which is of course an important part of developing the research field of economics and information security.

Last, this thesis tries to falsify the theory of economic barriers by researching if the Dutch transport and logistics sector shows the same indicators and conditions the theory describes. If new research demonstrates that the causal links between the indicators and economic barriers are not causal, the conclusions of this research should be revaluated.

5.4 Future research

Based on my experiences of this research project a number of recommendation for future research will be discussed in this section.

Foremost, additional research on the theory of economic barriers applied to the Dutch transport and logistics sector is necessary to validate the conclusions and recommendations made in this research, since it is one of the first times that that the Dutch transport and logistics sector is researched in the field of economics and information security.

Second, additional in-depth research is necessary in order to obtain greater understanding of the dilemma, which economic policies and instruments can be used in the transport and logistics sector. This research was only conducted with a small number of sector experts to gain an understanding of the reach of the problem and analyse the view on economic barriers. It would be fascinating to research more sector experts and to analyse their arguments.

And in addition it would be very interesting to find companies which are similar in regards to the structure and position of the companies used in this research. Using similar companies can offer an understanding if the characteristics of the companies influence the arguments on economic barriers.

Furthermore, during the research multiple aspects of this research came up that require additional research. For instance, this research only applies to the Dutch transport and logistics sector but it would be interesting to research if similar results can be found in other European countries. Also this research was mainly focused on the users of Portbase which is only one of the network community systems. A broader perspective of the transport and logistics sector which contains also air transport organizations might bring other arguments in the debate.

Besides, the research can be taken even further and compare the transport and logistics sector on a continental level. It would be very noteworthy to discover how other countries react to economic barriers in the market.

Plus, this research only focussed on national problems, solutions and national economic initiatives. The transport and logistics sector is clearly a sector that does not contain itself to borders. It is therefore necessary to do further research to for instance solutions for economic barriers on the European level.

Also this research only investigated the options that might be possible for the Netherlands to apply and the beginning of the Dutch Cyber Security Strategy. In the future when the Dutch

government has developed a greater and more comprehensive economic policy it is important to research the effect of economic barriers in the Netherlands.

Moreover, another interesting research will be a more in-depth analysis of the other factors which constrain cyber security improvement. This thesis manly focused on the economic vulnerabilities and influences, it would be fascinating to study the effect of legal, political and structural implications as well. These implications can be compared to the economic side of the problem in order to grasp a comprehensive and multidimensional view of the problem of insufficient cyber security.

And finally, it is critical to investigate the effectivity of cyber security investments. An optimal level of insecurity in regards to business continuity is researched. However, this disregards the other stakeholders' interests involved. A research should be focused on the interests of all stakeholders in the market.

5.5 Discussion and recommendations

I specifically chose the theory of economic barriers in regards to cyber security in this research because the theory explains the deficient cyber security well. The theory triggered my interest when I first read about it in the National Cyber Security Research Agenda. After I studied the literature I did not expected the results of this research. I thought the Dutch government already developed an economic policy and used multiple economic instruments to intervene in the market. In addition, the sector experts' views on economic cyber security policy was more as I imagined. The reasons and arguments they offered with their views differ from my assumption I had before starting this research. After well consideration I would like to offer some policy recommendations based on the research results.

- Mandated data disclosure to create loss and security attacks statistics

Create an institute that is responsible for publishing reports on the total cost of losses in order to establish data which shows that cyber security can be a good business case. The only way the problem of cyber security is going to be placed from the IT agenda to the business management agenda is when the private sector fears of losing customers and money. The Dutch government should stimulate an economic environment in which cyber security is a determining factor of continuing in business. The data necessary to do this is out there but kept by the private

sector. Opening up and increasing transparency can stimulate cyber security investments. It is also important that the smaller companies can contribute to the data collection.

- Enhance the data protection law to increase liability and competition

Use the data protection law not only from the privacy perspective but use it as an economical instrument to stimulate competition concerning quality. If the law is used as an economic instrument it could break through the pattern of a 'market of lemons'. In addition, the law remains unclear on definitions and standards. It is important that research on norms, standards and definitions continue to improve the legislation slowly and add to the cyber security responsibility of organizations.

- Security certificates and annual checks

Laws should be developed that offer a cyber security certificate for networks similar to the certificate of fire proof buildings. This certificate ensures security throughout the entire supply chain and established annual check-ups. In addition it also creates a role and opportunity for cyber-insurance market to grow. This is especially important for the transport and logistics sector and its large supply chains, because with network communication system you are as strong as the weakest link

Summarizing, the Dutch government should divert from their focus on self-regulation and intervene with economic instruments in the market. It is important to overcome the problem of high cybercrime costs and that cyber security becomes a business case. The problem needs to be handled in the boardroom as a business problem. Awareness in the Dutch transport and logistics sector is still low, thus other measures has to be taken to make it inevitable for the board room. Information disclosure and competition forces the boardroom to acknowledge the problem of cyber security.

6. BIBLIOGRAPHY

Akerlof, G. A. (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. Quarterly Journal of Economics, Vol 84 Nr 3, pp 488-500.

Anderson, R. (2001) 'Why Information Security is Hard: An Economic Perspective.' University of Cambridge Computer Laboratory, pp 1-8

Anderson, R., Böhme, R., Clayton, R. and Moore, T. (2008) 'Security Economics and The Internal Market.' Research Report ENISA pp 1-114

AON Cyber risk (2014) 'Cyber risico's onder controle' <http://www.aon.com/risk-services/cyber.jsp> latest accessed on 19-11-2015

Baer, W. (2003) 'Rewarding IT Security in the Marketplace', Contemporary Security Policy, Social Science Research Network, Vol. 24, Nr. 1, pp. 190-208

Baker, S. and Schneck-Teplinsky, M. (2010) 'Spurring the Private Sector: Indirect Federal Regulation of Cybersecurity in the US. Cybercrimes: A Multidisciplinary Analysis, Springer. Chapter 15, pp 239-263

Bandyopadhyay, T. and Mookerjee, V. (2009). 'Why IT managers don't go for cyber-insurance products." Communications of the ACM, Vol 52, Nr 11 pp. 68-73.

Bauer, J. and van Eeten, M. (2009), 'Cybersecurity: Stakeholder incentives, externalities, and policy options.' Telecommunications Policy, Science direct, Vol 33, Nr 10, pp. 706–719

Bauer, J. and van Eeten, M. (2009), 'Securing cyberspace: Realigning economic incentives in the ICT value net.' TU Delft. WebSci 2009

Bateman, T. 'Police warning after drug traffickers' cyber-attack' BBC Europa News, BBC Website, latest accessed on 19-11-2015 <http://www.bbc.com/news/world-europe-24539417>

Bisogni, F., Cavallini, S. and Di Trocchio, S. (2011) 'Cybersecurity at European Level: The Role of Information Availability.' Communication & Strategies, Vol 81 Nr. 1, pp 105-124.

Boehme, R. and G. Schwarz. (2010). Modelling Cyber-Insurance: Towards a Unifying Framework. Cambridge.
<http://weis2010.econinfosec.org/papers/session5/weis2010_boehme.pdf.>

Bos, H., Etalle, S., Fransen, F. and Poll, E. (2013) NCSRAII, National Cyber Security Research Agenda. <https://www.iipvv.nl/sites/stw.demo.infi.nl/files/mediabank/NCSRA-II.pdf>

Brief van de Minister van Veiligheid en Justitie (2012) 'Inrichting Cyber Security Raad en Nationaal Cyber Security Centrum'. Tweede Kamer, vergaderjaar 2011–2012, 26 643, nr. 246
<http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2012Z14260&did=2012D30072>

Brief van de Minister van Veiligheid en Justitie (2012) 'Meldplicht Security Breaches' Tweede Kamer, vergaderjaar 2011–2012, 26 643, nr. 247
<http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2012Z14265&did=2012D30080>

Brief van de Minister van Veiligheid en Justitie, (2013) ‘Vrijheid en veiligheid in de digitale samenleving, Een agenda voor de toekomst’. Tweede Kamer, vergaderjaar 2013–2014, 26 643, nr. 298 <http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2013Z24736&did=2013D50467>

Bryman, A. (2012) ‘Social Research Methods. ’Oxford University Press. 4th Edition.

BSA (2014) ‘EU Cybersecurity Dashboard A Path to a Secure European Cyberspace’ Research Report The software Alliance. <http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf>

Cox, A, (2014) EU Network and Information Security Directive: Is it possible to legislate for cyber security? Technology and innovation <http://www.arthurcox.com/wp-content/uploads/2014/10/Arthur-Cox-EU-Network-and-Information-Security-Directive-October-2014.pdf>

Cyber Security Raad, (2015) ‘International cooperation between Cyber Security Councils’ latest accessed on 19-11-2015 <http://www.cybersecurityraad.nl/>

Dean, B. ‘Why Companies Have Little Incentive to Invest in Cybersecurity.’ The Conversation. Latest accessed on 4-04-2015 <http://theconversation.com/why-companies-have-littleincentive-to-invest-in-cybersecurity-37570>

Directie Cyber Security NCTV (2014) ‘Beleidsreactie Cyber Security Beeld Nederland 4, Tweede Kamerstukken’ - <http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2014Z13284&did=2014D26554>

Digital Agenda Assembly (2011) ‘Cyber Security Barriers and incentives’. Brussels <https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/04.pdf>

Dunn C. and Suter, M. (2009) Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection, International Journal of critical infrastructure protection. Vol 2, Nr 4, pp 179-187

Eerste Kamer der State Generaal (2013) ‘Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp.’ Eerste Kamer Wetvoorstellen. Latest accessed by 03-08-2015 <https://www.eerstekamer.nl/wetsvoorstel/33662_meldplicht_datalekken_en>

Eerste Kamer Der Staten-Generaal (2015) ‘Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp,’ Stand van Zaken, Latest accessed by 03-08-2015 <https://www.eerstekamer.nl/wetsvoorstel/33662_meldplicht_datalekken_en>

Eerste Kamer (2015) ‘Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens.’ Staatsblad van het Koninkrijk der Nederlanden. <https://www.eerstekamer.nl/behandeling/20150619/publicatie_wet/document3/f=/vjuvb9mu87zu.pdf>

European Commission (2013) EU Cybersecurity plan to protect open internet and online freedom and opportunity, Cyber Security strategy and Proposal for a Directive. Digital Agenda. Latest accessed by 01-9-2015 <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>

Europol Public Information (2013) ‘Hackers deployed to facilitate drugs smuggling’, Intelligence Notification 004-2013, The Hague

Ernst & Young (2011) ‘ICT Barometer over cybercrime’ Jaargang 11, Beveilginswereld <http://www.beveiligingswereld.nl/files/ICTBarometercybercrime2011.pdf>

Gehem, M., Usanov, A. Frinking, E. Rademaker, M. (2015) Accessing Cyber Security, A Meta-Analysis of Threats, Trends, And Responses to Cyber Attacks. The Hague Centre for Strategic Studies, The Hague, pp. 1-101

Gill, P., Stewart, K., Treasure E. and Chadwic, B. (2008) “Methods of Data Collection in Qualitative Research: Interviews and Focus Groups.” Nature publishing group. <http://www.academia.edu/746649/Methods_of_data_collection_in_qualitative_research_interviews_and_focus_groups>.

Government Industry Canada (2015) ‘Logistics and Supply Chain Management’ Government Definitions and Statistics. Latest accessed on 19-05-2014 <http://www.ic.gc.ca/eic/site/dsib-logi.nsf/eng/h_pj00541.html>

Grange, A. (2014) ‘Ports at risk of cyber attacks’. Port Finance International. Latest accessed on 18-07-2015 <http://www.portfinanceinternational.com/features/item/1629-ports-at-risk-of-cyber-attacks-by-aidan-grange>

Hoffmann Website, ‘Over ons’. Informatie Hoffmann. Latest accessed on 19-11-2015 <https://www.hoffmannbv.nl/over-ons>

Hoffman Website, ‘Cyber security strategy’. Hoffmann bv website, latest accessed on 19-11-2015 <http://www.hoffmannbv.nl/diensten/ict-security>

HSD, (2014) Cyber Crime Costs The Netherlands 8.8 Billion Euros Per Year. The Hague Security Delta Website. Latest accessed on 14-01-2015 <https://www.thehaguesecuritydelta.com/news/newsitem/191>

ISE Website. Economics of Information Security. Home page, latest accessed on 01-02-2016 <http://infosecon.net/>

Jean Camp, L. (2006) 'The State of Economics of Information Security.' A Journal of Law And Policy, Vol. 2, Nr. 2

Kindt P. and van der Meulen, M.S.J. (2012) 'ICT in transport en logistiek, Voorsprong door initiatief en focus.' ING Sectormanagement Transport & Logistiek <https://www.ing.nl/media/ING_sectormanagement-transport-logistiek_voorsprong-door-initiatief-focus_tcm162-72860.pdf>

King, S. (2009) "Measuring Cyber Security and information assurance". IATAC SOAR, <https://buildsecurityin.us-cert.gov/sites/default/files/MeasuringCybersecurityIA.PDF>

Kolstad, C., Ulen, T. and Johnson, G. (1990). 'Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?'American Economic Review Vol. 80, Nr. 4, pp 888-901.

Krahmann, E. (2008) 'Security: Collective Good or Commodity?' European Journal of International Relations, Vol 14, Nr 3, pp 379-404

Lewis, P., Saunders, and M. Thornhill, A. (2009) 'Research methods for business students', Pearson Education Limited, 5th Revised edition

Loeb, M.P. and Gordan, L.A. (2003) Sharing Information on Computer Systems Security: An Economic Analysis. Journal of Accounting and Public Policy, Vol 22 Nr. 6

Margolis, E. and Liebowitz, S. J. (2000) ‘Network Externalities Effects.’ North Carolina State University. latest accessed on 19-11-2015
<https://www.utdallas.edu/~liebowit/palgrave/network.html>

Merholz, P., Wilkens, T., Schauer, B. and Verba, D. (2008) 'Subject To Change: Creating Great Products & Services for an Uncertain World: Adaptive Path on Design’ O’Reilly Media, First edition

Ministerie van Economische Zaken (2015) ‘Topsectoren, Logisitek’ Jaarbericht Sectoren
<http://topsectoren.nl/documenten/topsectoren/Jaarbericht-sectoren-2015_2015-02-13_204.pdf>

Ministerie van Veiligheid en Justitie (2011) ‘ Onderzoek Report Juridisch kader, Cyber Security.’ NCTV

Moore, T. (2008) Information Security Economics and Beyond. Information Security Summit. latest accessed on 19-11-2015
<http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf>

Moore, T. (2011) Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University, Center for Research on Computation and Society. pp 1-21

Mueller, M. (2010) Networks and States, The Global Politics of Internet Governance. The Mitt Press. First edition

Nationaal Cyber Security Centrum (2015) Cybersecuritybeeld Nederland 2015. Ministerie van Veiligheid en Justitie. < https://www.ncsc.nl/english/current-

topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015%5B2%5D.html>

National Initiative for Cyber security Careers and Studies. (2015) 'Explore Terms: A Glossary of Common Cybersecurity Terminology'. NICCS, latest accessed on 19-11-2015 <http://niccs.us-cert.gov/glossary#letter_B>

NATO Cooperative Cyber Defence Centre of Excellence 'Cyber Definitions.' CCDCOE, NATO Website, latest accessed on 19-11-2015 <https://ccdcoe.org/cyber-definitions.html>

NCSC (2013) 'ISACS, Publieke-Private samenwerking.' Nationaal Cyber Security Centrum, samenwerking dossier. latest accessed on 19-11-2015 <https://www.ncsc.nl/samenwerking/publiek-private-samenwerking/isacs.html>

NCTV, (2011) National Cybersecurity Strategy 1. Cyber security Nederland <https://www.nctv.nl/onderwerpen/cybersecurity/>

NCTV, (2013) National Cybersecurity Strategy 2. Cybersecurity Nederland

< https://www.nctv.nl/onderwerpen/cybersecurity/>

NCTV, (2013) National Cybersecurity beeld 4. Cybersecurity Nederland

< https://www.nctv.nl/onderwerpen/cybersecurity/>

Nederland ICT (2014) Landschapskaart cyber security, <http://www.nederlandict.nl/Files/ICT/Cyber_Landschapskaart.pdf>

Nieuwenhuizen, M.A.X. 20-05-2015 Interview met Monic van der Heyden, IT Manager of Port of Amsterdam, Amsterdam

Nieuwenhuizen, M.A.X 26-05-2015 Interview met Linda van Moors, Security Manger of Portbase, Rotterdam

Nieuwenhuizen, M.A.X 29-05-2015 Interview met Ernst-Jan Zwijnenberg, Unitmanager ICT-Security of Hoffmann Bedrijfsrecherche BV, Almere

Nieuwenhuizen, M.A.X 01-06-2015 Interview met Arthur van Dijk, Chairman of Transport & Logistiek Nederland (TLN), Lisserbroek

Nieuwenhuizen, M.A.X (2015) 'Responsible partners in need of a little incentive', Governance of Cyber Security, Crisis and Security Management, Leiden University.

Novak, B. (2011) "Misaligned incentives, First theme across acquisition." Software Engineering Institute, Carnegie Mellon University.

Pfleeger, S.L. and Golinelli, D. (2008), 'Cybersecurity Economic Issues, Corporate Approaches and Challenges to Decisionmaking'. RAND Research Brief. <http://www.rand.org/pubs/research_briefs/RB9365-1.html>

Portbase Website, 'Information Organization'. Website latest accessed on 19-11-2015 <https://www.portbase.com/>

Port of Amsterdam, 'Role and Vision'. Port Information. Website Port of Amsterdam, latest accessed on 19-11-2015 <http://www.portofamsterdam.com/Eng/corporate/role.html>

Raad van State (2014) ‘Samenvatting advies nota van wijziging meldplicht datalekken.’ Samenvattingen Adviezen. latest accessed on 19-11-2015 <https://www.raadvanstate.nl/adviezen/samenvattingen/tekst-samenvatting.html?id=288&summary_only=>

Rijksoverheid (2013) ‘Strategisch aanvalsplan The Netherlands: Digital Gateway to Europe’.

<https://www.rijksoverheid.nl/documenten/rapporten/2013/07/02/strategisch-aanvalsplan-the-netherlands-digital-gateway-to-europe>

Rijksoverheid (2015) ‘Meldplicht datalekken en uitbreiding boetebevoegdheid Cbp 1 januari 2016 van kracht.’ Actueel Rijksoverheid nieuws. latest accessed on 08-10-2015 <http://www.rijksoverheid.nl/nieuws/2015/07/10/meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-cbp-1-januari-2016-van-kracht.html>

Robinson, N. (2012) ‘Incentives and barriers of the cyber insurance market in Europe’ ENISA

<https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe>

Robinson, N. Disley, E. (2010) Incentives and Challenges for Information Sharing in the Context of Network and Information Security, European Network and Information Security Agency. pp 1-56

Rowe, B. and Gallaher, M. (2006) ‘Private sector cyber security investment strategies: An empirical analysis.’ 5th workshop WEIS06. latest accessed on 19-11-2015 <http://www.econinfosec.org/archive/weis2006/docs/18.pdf>

Ruske, K. (2011) ‘Transportation & Logistics 2030 Volume 4: Securing the supply chain’. PwC Supply Chain Management Institute. pp. 1-52 < http://www.pwc.com/tl2030.>

Sales, N. (2013) ‘Regulating Cybersecurity.’ Northwestern University Law Review. Vol. 107 Nr 4, pp 1503 – 1568.

Schneier, B. (2006) Information Security and Externalities, European Network and Information Security Agency Quarterly. Vol 2, Nr 4. <http://www.enisa.europa.eu/publications/eqr-archive/issues/eqr-q4-2006-vol.-2-no.-4>

Scott, B., Drahos, P. and Shearing, C. (2005) ‘Nodal Governance,’ Australian Journal of Legal Philosophy, Vol. 30 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=760928>

Song, V. (2013)’Comments Off on Social Networks: Winner Takes All?’ The online economy, Strategy and entrepreneurship. Harvard University

Staatsblad van het Koninkrijk der Nederlanden (2015) Wet Meldplicht Datalekken. 230 latest accessed on 10-10-2015

< http://www.rijksoverheid.nl/nieuws/2015/07/10/meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-cbp-1-januari-2016-van-kracht.html>

Topsectoren (2015) ‘Topsector Logisitek, bouwt internationale toppositie uit.’ latest accessed on 19-11-2015 <http://topsectoren.nl/logistiek>

TLN, ‘Transport en Logistiek Nederland: één stem, één geluid.’ Doelstellingen TLN. TLN Website, latest accessed on 19-11-2015 <http://www.tln.nl/Organisatie/Doelstelling.aspx#.VbD_3vntmko>

Trade, R. (2014) Cyber Liability Risks for Transportation and Logistics Companies. Insurance for trade and transportation. latest accessed on 19-11-2015 <https://www.roanoketrade.com/cyber-liability-risks-transportation-logistics-companies/>

Transport en Logistiek Nederland (2014) 'Cover, container vervoer op de weg.' TNL Magazine, nr. 21

Van den Berg, B. and Leenes, R, (2013). 'Abort, retry, fail: Scoping techno-regulation and other techno-effects.' Human Law and Computer Law: Comparative Perspectives, edited by M. Hildebrandt and J. Gaakeer. Dordrecht, Heidelberg, London: Springer.

van Eeten, M. and Mueller, M. (2013) Where is governance in Internet Governance? New Media Society, 15.

VPRO (2015) 'De slimste haven van de wereld'. Tegenlicht Uitzending 30 April 2015 <http://www.npo.nl/vpro-tegenlicht/26-04-2015/VPWON_1232883>

Wainwright, R. (2014) The Internet Organised Crime Threat Assessment. The -IOCTA Report EUROPOL <https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta>

Walker, S. (2012) 'Economics and the cyber challenge'. Information Security Technical Report 17. pp. 9-18

WeiS, 'Information Security Economics' WeiS website, latest accessed on 19-11-2015 http://infosecon.net/

WGIG (2005) ‘Report of the Working Group on Internet Governance’, Château de Bossey.

<http://www.wgig.org/docs/WGIGREPORT.pdf>