Investing in Cybersecurity

Nicole van der Meulen

RAND Europe

RR – 1202
August 2015
Commissioned by the Research and Documentation Centre (Wetenschappelijk Onderzoek- en Documentatiecentrum, WODC)
Table of Contents

Table of Contents ....................................................................................................................................... i
Summary and Conclusions ....................................................................................................................... iii
Acknowledgements ....................................................................................................................................... x
List of abbreviations ................................................................................................................................... xi

1. Introduction and background to the research ................................................................. 1
   1.1. Introduction ................................................................................................................................. 1
   1.2. The critical infrastructure is divided into twelve sectors ........................................................ 2
   1.3. Problem statement ......................................................................................................................... 4
   1.4. Research questions ....................................................................................................................... 4
   1.5. Methodology ................................................................................................................................ 5
   1.6. Limitations ................................................................................................................................... 7

2. Cybersecurity: From definition to threat ................................................................................. 9
   2.1. From information security to cybersecurity ................................................................................. 10
   2.2. Cybersecurity as part of national security .................................................................................... 11
   2.3. Cybersecurity: more than information security? .......................................................................... 12
   2.4. Threats come together in a fragmented overview ........................................................................ 13
   2.5. Classification of threats ............................................................................................................... 14
   2.6. Developments introduce new challenges and opportunities ......................................................... 17

3. Drivers for cybersecurity investments .................................................................................... 19
   3.1. Theoretical approaches to investing in cybersecurity are difficult to apply in practice ............. 19
   3.2. Regulation causes incentive for action ......................................................................................... 21
   3.3. Incidents lead to evaluation and measures ................................................................................... 24
   3.4. Insurance companies can potentially stimulate organisations to improve their cybersecurity practices ................................................................................................................. 27

4. Nature and size of investments in cybersecurity .................................................................... 33
   4.1. Available data about investments in cybersecurity is fragmented and difficult to compare ........... 33
   4.2. A lack of a unified way of counting leads to a lack of clarity and uncertainty ............................... 35
4.3. Intermezzo: types of investments in cybersecurity .................................................................35
4.4. Cybersecurity is (too) interwoven in projects and processes..................................................38
4.5. Cybersecurity: quality over quantity .....................................................................................38
4.6. Critical reflection on the research question and the focus .......................................................39
4.7. The available data is too limited to draw conclusions ...............................................................39
4.8. Why did some organisations provide insight? ......................................................................40
4.9. Introduction of a target number is undesirable and infeasible ............................................41

5. From good to better ....................................................................................................................45
5.1. Risk acceptance as vehicle for a more holistic approach .......................................................45
5.2. From organisation to integration of the supply chain ............................................................46
5.3. Using existing crisis structures ...............................................................................................47
5.4. Inconvenient is preferable to insecure ....................................................................................47
5.5. Information exchange is important .........................................................................................48
5.6. Active dissemination ..............................................................................................................49

6. Concluding remarks ..................................................................................................................51

Bibliography .................................................................................................................................53
Appendix A Interview protocol .......................................................................................................63
Summary and Conclusions

Cybersecurity has had a prominent place in the spotlight for a while now, both in the Netherlands and abroad. Our digital dependence has led to a situation where security vulnerabilities and (potential) security incidents come accompanied by serious consequences, especially if such vulnerabilities and incidents occur within organisations in the critical infrastructure sectors. This research had as its starting point the desire to map why, how and how much organisations in critical infrastructure sectors invest in cybersecurity. The main research question was:

**On what basis, in what way and to what extent do private companies and public organisations in the critical infrastructure sectors invest in cybersecurity?**

To answer the main question, the author conducted a total of 27 interviews with representatives of organisations in the 12 critical infrastructure sectors in the Netherlands. This research commenced – and was largely completed – before the results of the reassessment of the critical infrastructure sectors were made public. As a result, organisations were selected based on the original twelve critical infrastructures as determined prior to the reassessment.

Besides the main research question, this report also aims to answer a number of other fundamental questions, which lay the groundwork to sketch the outlines of the cybersecurity landscape. This includes, first of all, the question ‘how is cybersecurity defined and operationalised?’ Second of all, a short description is provided about the different threats organisations within critical infrastructure sectors face, as a lead-in to the first part of the main question, which concerns the underlying reasons for organisations to invest in cybersecurity.

**Cybersecurity: more, less or the same as information security**

While cybersecurity as a concept has by now become integrated into our everyday lives, there is no commonly accepted or standard meaning of the concept. How cybersecurity is defined depends largely on the context. In both National Cyber Security Strategies, the Dutch government emphasises the connection with information security, especially the fundamental principles of confidentiality, integrity and availability. So there is a strong connection between information security and cybersecurity. According to many within the more technically-minded community, cybersecurity is merely a popular term for what they refer to as information security. Others consider cybersecurity to be a different – or better put, broader – phenomenon than information security. In particular, the identification of cyberspace as a new defence domain that must be protected in the interest of national security has shed a different light on the topic. This is confirmed by the report ‘The Public Core of the Internet’, published
by the Netherlands Scientific Council for Government Policy (WRR). Nonetheless, in practice, information security continues to be the dominating concept, which means that cybersecurity is predominantly approached – at least by the representatives interviewed – from the perspective of information security. The importance of having a commonly accepted definition, or to develop such a definition, is broadly recognised. The lack of one, after all, is one of the primary reasons why the collection of activities within this domain represents such a challenge, especially with respect to investments made and measures taken.

Fear of reputation damage unites a fragmented threat assessment

The absence of a commonly accepted definition of cybersecurity also has an effect on the development of a reliable and comparable threat assessment. Despite the many reports and studies available, the overview of threats is fragmented. In particular, this is due to the manner in which information is collected and subsequently published. Due to different orders of magnitude and a lack of transparency about methodology, reports are difficult to compare to one another in a reliable manner. Based on the interviews and the literature, it appears that public and private organisations perceive the possibility of reputation damage as the biggest threat. While reputation damage is perceived as the biggest threat – both in this project as well as in affiliated research projects (Libicki et al. 2015) – it is primarily a consequence or a secondary effect rather than a direct threat, since it primarily occurs as a result of incidents. Direct threats can be divided into information-related threats and system-related threats. In the area of information-related threats, the leaking of personal data – such as that belonging to clients and patients, as well as employees and corporate contacts – financial information and intellectual property is the largest concern. Intellectual property is an important asset to protect, especially for organisations in the chemical and health sectors, which means that potential incidents involving such information can lead to considerable damage; financial information is a target for threat actors, particularly within the financial sector; and personal data, such as that of clients, employees and patients, is a concern for all sectors. This is confirmed in the Cyber Security Assessment Netherlands 4.

System-related threats, such as disruptions or manipulations of processes, are a potential concern, in particular for sectors with a direct connection to the physical world. Examples include the energy, transport and water management services, as well as law and order. Distributed Denial of Service (DDoS) attacks were also mentioned as a threat, in particular because they (could) lead to reputation damage.

Even though the threat overview is fragmented – in part because of the absence of reliable (quantitative) data – it is united by the overarching concern about reputation damage. It is primarily the potential impact on the image and reputation of an organisation that is perceived and experienced as the threat by its representatives. This perceived threat also demonstrates that incidents are the strongest driver for cybersecurity measures and, therefore, provides an indirect answer to the first part of the main research question: on what basis do organisations invest in cyber security?

Incidents are the strongest driver for cybersecurity measures

While researching drivers for cybersecurity measures, incidents surfaced as one of the main reasons – if not the main reason – for organisations to decide to introduce (additional) measures in the area of cybersecurity. This is principally the case because incidents focus attention on the topic and also enhance
the risk of damage to the reputation of an organisation, or even a whole sector. Incidents lead to media attention, which can subsequently lead to parliamentary questions, which can introduce an incentive for an organisation to enhance cybersecurity measures. Besides incidents, threat analyses also play an important role in the determination of organisations to take cybersecurity measures. These threat assessments often include incidents, which reinforces the illustrative importance of incidents as an incentive for cybersecurity measures. Based on the literature, regulation also appears to be an incentive for action, but this was far less apparent during the interviews.

**Regulation is presently (still) of limited influence**

Based on the literature, regulation appears to function as an incentive for action, but during the interviews this was less apparent. Regulation will, however, start playing a larger role in the European Union (EU) once a number of regulatory proposals at the European level, such as the Network and Information Security (NIS) Directive and the EU General Data Protection Regulation (GDPR) have been approved. What becomes apparent – especially based on experiences in the United States (US) – is that an important connection exists between the value of incidents and regulation, especially, for example, in light of notification obligations. By forcing organisations to report incidents, governments can use regulation to induce the effect incidents have on organisations.

**Cyber-insurance providers do not have general criteria and do not (yet) play a role in the cybersecurity posture of organisations**

Besides regulation and incidents as primary drivers, this research report also focuses on the role played by cybersecurity insurance with regard to public and private organisations. The hypothesis is that the risks experienced cannot be exclusively covered by increased investments in cybersecurity measures, and that insurance also has an important role to play. The conditions under which such an insurance policy is provided could subsequently also function as a driver for organisations to ensure a certain basic level of cybersecurity.

The market for cyber-insurance policies is still very much in development. In theory, such insurance providers could reduce cyber-insecurity or stimulate investments in cybersecurity by introducing requirements or informing clients about best practices, as is the case with regard to minimising risks in the area of fire safety. The cyber-insurance market appears to be insufficiently mature to induce clients to make cybersecurity investments. In the Netherlands in particular, cyber-insurance policies have not yet become mainstream. Based on interviews in the Netherlands, it can be concluded that the adoption of a cyber-insurance policy or compliance with insurance provider requirements do not play a role in the determination of cybersecurity budgets or the measures taken. Not a single interviewee had a cyber-insurance policy and only one organisation was trying to determine whether such a policy would be desirable. Based on a couple of interviews with representatives from insurers in the United Kingdom (UK), it also became clear that in the UK market there are no general criteria for the provision or rejection of a cyber-insurance policy. Application forms are diverse, although at the moment a couple of parties are in the process of developing more common ones which ask the same questions. In the UK, the government has tried to use the insurance sector to stimulate organisations to comply with a number of minimum requirements in the area of cybersecurity. This happens incidentally through a requirement of
the insurance industry that Small and Medium Enterprises (SMEs) comply with minimum standards, as set out through Cyber Essentials.

The influence of cyber-insurance on the level of cybersecurity measures adopted by organisations presently remains uncertain, but upcoming regulatory proposals — including notification obligations — can potentially function as incentives for organisations to adopt insurance policies in the area of cybersecurity.

Data about size of investment is not available

The second and third parts of the main research question focused on the determination of the nature and the size of cybersecurity investments. To answer these two parts, the author conducted 27 interviews with representatives of organisations within the twelve critical infrastructure sectors. Of those 27 representatives only a small number provided insight into the size of their cybersecurity investment, while the rest of the organisations did not. Because of this, no overarching answer can be provided to the question as to how much organisations within the critical infrastructure sectors invest in cybersecurity. This, of course, prompts the question: why did they not provide such insight? The explanations provided in response to that question have been summarised in the report of the project as follows.

First, it is unclear which costs can specifically be allocated to cybersecurity. This challenge contains two interconnected aspects. First of all, there is the absence — as previously indicated — of a commonly accepted definition of the term. In the absence of such a commonly accepted definition, there is also a lack of criteria to determine which investments can be classified as cybersecurity investments. Basically, there is no cost collection model to map the requested data.

Secondly, cybersecurity appears to be an integral part of business operations because it is integrated in other projects, processes and products, which makes it difficult to isolate cybersecurity related investments. Investments made solely for the purpose of cybersecurity, such as certain employees, audits, penetration tests, awareness campaigns, etc. are identifiable. These, however, give a skewed reflection, because they are merely a fraction of the overall investment made by organisations in the area of cybersecurity.

Thirdly, the focus on investments is too narrow. To develop a holistic overview, all expenses made by organisations in critical infrastructure sectors must be included, in particular the exploitation costs. An exclusive focus on investments gives a distorted image about how much organisations spend on cybersecurity.

Fourthly, the collection and mapping of data about the nature and size of cybersecurity investments is complicated because of the qualitative approach to cybersecurity. Cybersecurity is primarily approached from a qualitative perspective because the introduction of cybersecurity measures is based on risk analysis. The point of departure, therefore, is the translation of the risk analysis into a plan of action which includes these measures. This reinforces the idea that cybersecurity is primarily approached from a qualitative rather than a quantitative perspective.

Research question is topic of discussion

The interviewees reflected critically on the main research question and the focus of this research project. As described above, interviewees found the focus on investments too restrictive, partially because it ignores
exploitation costs. A distinction has to be made between business operations and business change. The exclusive focus on investments – in case sufficient data is available and accessible – can give a distorted image about how much an organisation actually spends on cybersecurity. Secondly, the question needs to be asked whether the main research question provides the right focus. As many interviewees indicated, the focus of cybersecurity is primarily qualitative, which is why questions about the presence of qualitative measures received more support during the interviews in comparison to those with a quantitative focus. The quantitative focus is also potentially problematic, as a higher level of investment may be perceived as more effective, while actually more money may be counterproductive if it is spent on ineffective measures. Nonetheless, data collection primarily focused on qualitative measures is also subject to the same challenges as quantitative data collection. Without a broadly accepted definition and a uniform cost collection model, the collection of qualitative measures also becomes difficult to map.

Target number is undesirable and infeasible

At the start of this study, the potential introduction of a target number as a policy option was discussed and as such included in the protocol for the interviews. Target numbers are regularly used for different policy topics as an instrument to bring about a particular change, such as an increase in the number of women in leadership positions. As a result, during this research project the desirability and feasibility of the introduction of a target number has also been evaluated. However, there was much resistance to the quantification of cybersecurity measures among the interviewees when asked about the desirability and feasibility of the introduction of a target number. The introduction of a target number as an instrument to advance cybersecurity investments was perceived by the majority of interviewees as undesirable and infeasible. According to the majority of interviewees, a general target number adds little value, since every organisation is different and maintains a different risk profile. While some interviewees considered the possibility of developing a target number at a sector level, others disagreed because even at a sector level considerable diversity with respect to risk profiles exists. Many interviewees suggested that a number on its own is meaningless, considering the lack of insight it provides with respect to the measures taken by organisations, as well as its inability to offer an explanation as to why these measures are taken. According to the majority of organisations, quality is considerably more important than quantity. In addition, the introduction of a target number can have negative consequences because it can lead to a certain sense of false security. Numbers are easy to manipulate and a target number will not necessarily lead to more money for cybersecurity. An alternative option is the introduction of a set of qualitative requirements which organisations need to comply with before business can be conducted with them. Cyber Essentials in the UK is an example of such a scheme, as is the framework for organisations within the critical infrastructure introduced by the National Institute of Standards and Technology (NIST) in the US.

A focus on detection and response via risk acceptance

With an eye on making a contribution to the improvement of cybersecurity in organisations, respondents were also asked during the interviews about best practices. Interviewees recommended a number of principles to improve the current cybersecurity situation and to enhance cyber resilience. The relative character of security is the first central tenet. This means that society, including organisations within critical infrastructure sectors, needs to establish a certain level of risk acceptance. Both the interviewees
and the literature emphasise this. That incidents will happen is almost inevitable. By placing risk
acceptance as a central element of their strategy, organisations can more adequately prepare themselves for
incidents. This notion of risk acceptance also leads to the second principle, which, based on the findings,
must be better integrated: cybersecurity must be approached from a holistic perspective, where prevention
is only a part of the whole and where detection plays a more prominent role. This view appears in the
literature and was confirmed by multiple interviewees. The acceptance that incidents will take place puts a
greater focus on when and how fast such breaches can be detected.

From organisation to integration of the supply chain
The second dimension of a holistic approach is the involvement of the entire chain or sector. Attackers are
inclined to attack different organisations within a sector rather than a single organisation, or to approach
the weakest link, which, due to intra-sector dependencies, may affect the rest of the sector. This has been
recognised, for example, by the financial, retail and energy sectors. Organisations must therefore work
towards the integration of, and communication within, the supply chain. This has several benefits. Firstly,
by exchanging information with each other, organisations can anticipate possible attacks. Secondly, it
allows organisations to appreciate the impact that potential attacks could have on the entire supply chain,
rather than just their own operations. Thirdly, integration within the supply chain or the sector can lead
to cooperation with regard to the introduction of measures on different levels.

Information exchange and active dissemination
Information exchange is an indispensable element in the improvement of cybersecurity. This was also
emphasised during the interviews and additionally confirmed through legislative proposals that aim to
improve the state of information exchange both in the Netherlands and abroad. Information exchange
primarily occurs through platforms such as Information Sharing and Analysis Centres (ISACs) and other
cooperative associations, primarily at the sector level. Moreover, it is important that information is
exchanged with the objective of making the sector or the supply chain more resilient against cyberattacks.
Subsequently, it is critical – as confirmed by both the interviews and the literature – that so-called good
practices based on experiences are actively shared and disseminated among public organisations, private
organisations and perhaps even the general public, so as to reach as broad an audience as possible.

Conclusions
The above leads to a number of important conclusions that can be derived from the primary findings and
that can help to answer the main research question, as well as make a contribution to the ongoing
cybersecurity debate.

For the first part of the main research question – on what basis do public and private organisations invest
in cyber security? – it can be concluded that the fear of reputation damage operates as, and is perceived as,
the biggest threat, which makes incidents the greatest incentive to take (additional) security measures.
Regulation takes advantage of the dynamic between the fear of reputation damage and the incentive
introduced by incidents by obliging organisations to report incidents. By making incidents public or
sharing them with third parties, regulation enhances the pressure to prevent incidents.
This also has negative consequences for society because it overemphasises prevention and underemphasises detection and response. When one looks at good practices and the ways by which cybersecurity can be raised to a higher level, risk acceptance – or the realisation that incidents will take place – is an essential ingredient to instil in the whole security lifecycle, from prevention to response, with detection as an important intermediary component. Based on the above, a potential state of tension arises due to the pressure to report incidents, the fear of reputation damage, and risk acceptance as a vehicle for a holistic approach. As a result, there is an exclusive focus on preventing incidents, despite the fact that absolute security is an illusion and that the relative nature of security is precisely what needs to be emphasised to achieve a more mature level of cybersecurity.

Based on these conclusions, the reporting of incidents and the exchange of information should primarily be used to learn how to detect incidents more quickly and more effectively, with the objective of reducing damage. The adoption of a cyber-insurance policy is expected to incentivise organisations to improve their cybersecurity posture, but as of yet that is not the case.

While this research project is unable to provide an overarching overview of how much and in what ways organisations invest in cybersecurity, the interview questions have led to other findings. Data about the nature of cybersecurity investments is not generally available due to the following reasons:

- There is no commonly accepted definition of cybersecurity
- There is no overarching cost collection model
- Investments in cybersecurity are integrated into other projects, processes and products
- Cybersecurity is primarily approached from a qualitative rather than a quantitative approach, which means costs are not the primary focus.

The particular emphasis of this study on the collection of quantitative data has been called into question by representatives from public and private organisations in critical infrastructure sectors. Subsequently, representatives of organisations in critical infrastructure sectors also considered the introduction of a target number as undesirable and infeasible. Based on the findings, and in lieu of a target number, the government, in cooperation with the private sector, could emphasise the need to take qualitative measures to advance the level of cybersecurity by introducing minimum standards. For example, this could be introduced through a set of qualitative requirements that organisations have to comply with before business can be conducted with them. All of these proposals have the intention of advancing the level of cybersecurity and to further promote the necessity of detection and response, in addition to prevention.
This report has been made possible through the valuable contributions of various individuals. First of all, I wish to express my gratitude to the Chair and the members of the Steering Committee, consisting of Prof. Dr. P.A.L. Ducheine, LL.M. (Chair, University of Amsterdam – Faculty of Law), drs. M.H.G. van Leeuwen (member, Ministry of Security and Justice – National Coordinator for Counterterrorism and Security), Dr. G. Haverkamp (member, Research and Documentation Centre), L. Alderlieste-de Wit (member, Aegon), Dr. S.M. Straathof (member, Netherlands Bureau for Economic Policy Analysis), for their time and insights, which improved the quality of the report. Naturally, I would also like to thank all interviewees for their willingness to participate in this research and the insights that they have been willing to share. Considering the sensitive nature of the topic, they remain anonymous, but without their contribution this research could not have been carried out. I would also like to thank several colleagues from RAND Europe who have helped with this report. First of all, Stefan Soesanto for his research assistance during various parts of this study, from hunting down contact details of interviewees to summarising parts of the literature and helping with the references. I would like to thank Louise Taggart for her help in compiling (parts of) the bibliography. Furthermore, I also thank Kristy Kruithof for her presence and contribution during the kick-off meeting and Maurice Fermont for his help with the literature search at the beginning of the project. Finally, I would like to express a special word of thanks to the reviewers of this report, Dr. Hanneke Luth and Stijn Hoorens.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABI</td>
<td>Allied Business Intelligence</td>
</tr>
<tr>
<td>AFM</td>
<td>Netherlands Authority for the Financial Markets</td>
</tr>
<tr>
<td>BID</td>
<td>Bestuur en Informatieveiligheid Dienstverlening</td>
</tr>
<tr>
<td>BIG</td>
<td>Baseline Informatiebeveiliging Gemeenten</td>
</tr>
<tr>
<td>BIS</td>
<td>Department for Business, Innovation and Skills</td>
</tr>
<tr>
<td>BIR</td>
<td>Baseline Informatiebeveiliging Rijk</td>
</tr>
<tr>
<td>BIWA</td>
<td>Baseline Informatiebeveiliging Waterschappen</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CCDCOE</td>
<td>Cooperative Cyber Defence Centre of Excellence</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality Integrity Availability</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>CND</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>CSAN</td>
<td>Cyber Security Assessment Netherlands</td>
</tr>
<tr>
<td>CSTB</td>
<td>Computer Science and Telecommunication Board</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DNB</td>
<td>Dutch Central Bank</td>
</tr>
<tr>
<td>DRN</td>
<td>Data Recovery Nederland</td>
</tr>
<tr>
<td>DWR</td>
<td>Digitale Werkomgeving Rijk</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECSG</td>
<td>European Cyber Security Group</td>
</tr>
<tr>
<td>EFF</td>
<td>Electronic Frontier Foundation</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Network and Information Security Agency</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigations</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>IBD</td>
<td>Informatiebeveiligingsdienst voor Gemeenten</td>
</tr>
<tr>
<td>IBI</td>
<td>Interprovinciale Baseline Informatiebeveiliging</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and communication technology</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IES</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>ISAC</td>
<td>Information Sharing and Analysis Centre</td>
</tr>
<tr>
<td>ISF</td>
<td>Information Security Forum</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standardisation Organisation</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NCSC</td>
<td>National Cyber Security Centre</td>
</tr>
<tr>
<td>NCTV</td>
<td>National Coordinator for Counterterrorism and Security</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Security</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NVB</td>
<td>Dutch Banking Association</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>PAC</td>
<td>Pierre Audoin Consultants</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory control and data acquisition</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Intelligence and Event Management</td>
</tr>
<tr>
<td>SMART</td>
<td>Specific Measurable Acceptable Realistic Time-bound</td>
</tr>
<tr>
<td>SME</td>
<td>Small and Medium Enterprises</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Centre</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>US</td>
<td>United States of America</td>
</tr>
<tr>
<td>WEF</td>
<td>World Economic Forum</td>
</tr>
<tr>
<td>WEIS</td>
<td>Workshop on the Economics of Information Security</td>
</tr>
<tr>
<td>WRR</td>
<td>the Netherlands Scientific Council for Government Policy</td>
</tr>
</tbody>
</table>
1. Introduction and background to the research

1.1. Introduction

The first time the Netherlands was confronted with a (real) digital crisis was in 2011. On the night of 2 September, Piet-Hein Donner, at the time Minister of the Interior and Kingdom Relations, took his seat in front of the camera to inform the Dutch public about this digital crisis and the countermeasures taken by the government to reduce the damage as much as possible. Back then very few people had heard of the company DigiNotar, where the digital intrusion that led to the crisis had taken place. DigiNotar was a Certificate Authority (CA) for, among others, the Dutch government, and was compromised in July 2011, allowing perpetrators to generate false certificates. The presence of false certificates undermined the trust placed in DigiNotar since the authenticity of their certificates could no longer be guaranteed. This press conference held by the former minister Donner was the moment that exposed our vulnerability to digital attacks. The consequences of digital failure became tangible, or at least more tangible than before. And DigiNotar became an example showcasing the urgency of cybersecurity.

Today, cybersecurity is a daily news item, in the Netherlands as well as abroad. The stream of media reports about (data) breaches in particular instills little confidence in the public. This is worrisome considering the crucial role played by Information and Communication Technology (ICT) in contemporary society and its economy. Because the dependency of society on digital means continues to increase, digital vulnerabilities, and in particular the ways by which such vulnerabilities are being exploited, have become potentially quite impactful.

Reporting about cybersecurity incidents generates pressure on organisations – both in the private as well as the public sector – to react and take action. Through the first and second National Cyber Security Strategies (Rijksoverheid 2011; Rijksoverheid 2013), the Dutch government – in cooperation with representatives from the private sector – has already acknowledged that it recognises the seriousness of the situation. Dutch society has to become more resilient against cyberattacks, especially in critical infrastructure sectors, where the impact of a potential cyberattack can lead to the greatest damage.

As a result of the digital crisis surrounding DigiNotar, the Minister of Security and Justice introduced a legislative proposal for a new notification requirement for organisations within the critical infrastructure sectors (wetsvoorstel melding inbreuken elektronische informatiesystemen). The focus of the proposal is primarily on limiting risks after an incident by having organisations inform the National Cyber Security Centre (NCSC), which subsequently functions as a coordinating organ to help and to warn other organisations.
This indicates how public-private cooperation, sometimes facilitated through policy instruments, is necessary for the reduction of the damage caused by incidents and the enhancement of the level of cybersecurity in the Netherlands. The critical infrastructure rests in large part in the hands of the private sector. The private sector is in prime position to determine what course of action it wants to take and how much it wants to (financially) invest to increase cyber resilience. As indicated by the ‘National Cyber Security Strategy 2 – From Awareness to Capability’ (Rijksoverheid 2013), security in contemporary society has increasingly become more of a shared responsibility.

In the debate about investments in cybersecurity, the question is frequently asked whether the private sector sufficiently invests in cybersecurity and whether it also takes sufficient responsibility. This question is being asked because of different factors which facilitate market failure. Factors such as information-asymmetry, externalities and transfer of liability can all function as economic barriers (Anderson et al. 2009; Kox & Straathof 2014). The thought process is that a lack of economic incentives to take action leads to a lack of measures taken, in particular by private companies.\(^1\) Rowe and Gallaher (2006) have indicated what roles different drivers play in the decisionmaking process of a number of organisations in the United States (US) with respect to their investments in cybersecurity. Based on their findings, it becomes clear that regulation is the biggest driver for cybersecurity investments.

The quantitative aspect of cybersecurity investments, however, only tells half the story. Beside the ‘how’ question, research about cybersecurity investments also has to pose the question ‘in what?’ to develop the most comprehensive overview of the current state of affairs in this area. A systematic study carried out by Anderson et al. (2012) indicates – based on all available reports on the costs of cybercrime – that the current approach of investing in cybercrime is very inefficient. According to Anderson et al. (2012), too much is being invested in preventive measures, such as antivirus and firewalls, and too little in the response to cybercrime, such as investigative capacity.

The current debate with regard to investments in cybersecurity requires, for a variety of reasons, further research. First of all, research is needed to gain a better understanding of the nature and the size of investments in cybersecurity by organisations in both the public and the private sectors. Second of all, research is needed to look at what kind of differences can be discovered between the nature and size of investments and how these can be explained based on the findings. Third of all, research is needed to determine whether government interference is necessary and desirable considering the current state of affairs with respect to investments in cybersecurity in both the public and the private sectors.

1.2. The critical infrastructure is divided into twelve sectors

This research is specifically focused on public organisations and private companies within the critical infrastructure in the Netherlands, which is divided into twelve sectors. These twelve critical sectors were established in 2004 (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2004). They are:

---

\(^1\) The Workshop on the Economics of Information Security (WEIS) has – for over a decade – devoted attention to the interaction between economic approaches and information security.
In 2005 the Dutch government carried out its first content analysis of the critical infrastructure sectors whereby it examined, both by sector and by other criteria, which products and services are critical for the functioning of society. This resulted in a final list of 33 products and services which were labelled as critical products and services in 2005. It was then determined, by sector, precisely which elements or objects are critical to these products, services and processes (NCTV 2010, 4). Several years later, in 2009, a second content analysis was carried out of the critical infrastructure sectors.

At the start of this research project, the 12 critical infrastructure sectors were the same as those established in 2004, but the number of products had been reduced from 33 to 31. Although the Minister of Security and Justice announced the reassessment of the critical infrastructure sectors in 2013, this exercise was still ongoing at the start of this study (Ministerie van Veiligheid en Justitie 2013).

The goal of the reassessment was to maintain as high a level of protection of the critical infrastructure as possible and to take into account the changes in threats, as well as society’s increasing dependency on it.

In May 2015, the Minister of Security and Justice shared the results of the reassessment with the Dutch parliament (Ministerie van Veiligheid en Justitie 2015). In the new list of critical infrastructure sectors, a distinction has been made between two categories, category A and category B.

Category A contains the critical infrastructure that in case of disruption, degradation or failure affects the lower limits of at least one of the following four impact criteria:

- Economic consequences: more than approximately 50 billion euros damage or approximately 5.0% decline in real income.
- Physical consequences: more than 10,000 individuals dead, seriously wounded or chronically ill.
- Societal consequences: more than 1 million individuals experience emotional problems or serious issues related to societal existence.
- Cascade consequences: loss as a result of failure of at least two other sectors.

Category B contains the critical infrastructure that in case of disruption, degradation or failure affects the lower limits of at least one of the following three impact criteria:

- Economic consequences: more than approximately 5 billion euros damage or approximately 1.0% decline in real income.
• Physical consequences: more than 1,000 individuals dead, seriously wounded or chronically ill.
• Societal consequences: more than 100,000 individuals experience emotional problems or serious issues related to societal existence.

1.3. Problem statement

The overarching problem statement for this research is:

**On what basis, how and to what extent do private companies and public organisations in the critical infrastructure sectors invest in cyber security?**

As indicated by the members of the Steering Committee during the kick-off meeting, this is more a main research question than a problem statement. The answer to the main research question should, however, be able to provide valuable input to answer the following three follow-up questions:

1. Are there national and international best practices of tested measures within the critical infrastructure that can function as examples for organisations?
2. What efforts do companies in the private sector and public organisations in the critical infrastructure have to make, based on those best practices, to improve their resilience in the area of cybersecurity?
3. How can this be implemented and what sort of policy instruments (such as self-regulation, legislation, etc.) does the government have at its disposal to guarantee the level of cybersecurity of private companies and public organisations within the critical infrastructure sectors?

These three follow-up questions, however, require a response to the main question.

1.4. Research questions

This study contains a total of ten research questions divided into four categories.

**State of the Art**

1. How is cybersecurity defined and operationalised?
2. What sort of cybersecurity threats can be distinguished within the critical infrastructure sectors?
3. What is known about the developments in the area of cybersecurity?

The first three questions will be discussed in chapter two. These questions have primarily been answered through the literature review, but for question two input from the interviews has also been incorporated.

**Nature and size**

4. What types of investments are there in cybersecurity and what is the level of investments in cybersecurity by both public organisations and private companies within critical infrastructure sectors?

This question will be answered – to the extent possible – in chapter four, based on the interviews.

5. What criteria do private companies maintain to insure or deny insurance to other organisations in the area of cybersecurity?
Investing in Cybersecurity

This question will be answered in chapter three, based on the interviews.

6. What are the security requirements, based on regulation and industrial standards, for the different sectors within the critical infrastructure?

This question will be indirectly discussed in chapter three, based on the literature review and interviews.

7. What differences exist in terms of investments in cybersecurity between countries, and between private companies and public organisations within the named critical infrastructure sectors, and on what basis can those differences be explained?

Due to the reasons described in chapter four, this question remains largely unanswered.

**Best practices and examples**

8. What examples and/or best practices are available for companies and public organisations, both at the national as well as the international level, in the area of cybersecurity? And what are they based on?

Best, or preferably-named good practices, are discussed in a broad sense in chapter five. This is done based on the interviews, literature review and analysis.

**Target numbers and implementation**

9. Can criteria or target numbers for cybersecurity be formulated, which can function as a benchmark for other companies and public organisations in the different critical infrastructure sectors? If yes, in what way? If no, why not?

10. What is the best way to implement these target numbers based on the existing regulatory framework?

These questions will be discussed in chapter four, based on the interviews.

**1.5. Methodology**

A combination of qualitative methods has been used to carry out this research.

**1.5.1. Literature review**

First, a literature review has been carried out to determine what findings relevant to the purposes of this research were already available. The literature review included academic literature and other sources, such as news articles in the media, reports by companies and policy documents. During the literature review, several topics and search terms were used to search for relevant literature in Google Scholar and Google. These were, among others:

- Cyber-insurance
- Cybersecurity insurance
- Cybersecurity investment
- Cyber investment
- Cyber budgets
Subsequently, a selection of the literature was made based on its relevance to this research. This happened through a quick scan of the titles and the abstracts to determine whether the literature was sufficiently relevant to answer the research questions.

1.5.2. Interviews

Second of all, a total of 27 interviews were conducted with representatives from organisations within the critical infrastructure sectors. Of those, 24 were conducted in person and three were conducted by telephone. The selection of interviewee candidates took place based on the list of critical infrastructure sectors as described in 1.2.

The research team sent a draft list of candidate organisations to the Steering Committee prior to the kick-off meeting and the list was discussed during the meeting. Based on the suggestions of the Steering Committee, the list was adjusted and extended. The final list of interviewee candidates was selected based on a number of criteria. The aim was to interview at least two parties per sector. This was successful for every sector, except for drinking water and food. The drinking water sector in its entirety declined to participate and only one representative was interviewed from the food sector. For other sectors, three or four interviews were conducted. Besides a sectoral mix, a certain balance between public and private organisations was also sought. Furthermore, the focus was placed on prominent players. For this the author did not define a specific criterion, since she subsequently devoted attention to finding the appropriate balance between public and private organisations, and was also limited by the availability of interview candidates and their contact details. For the private sector, Small and Medium Enterprises (SMEs) were excluded from the list of organisations to be interviewed. This decision reflects the number of different roles played by big firms in society in contrast to SMEs, and the respective means available to both groups. Moreover, the visibility of big players influences their threat profiles and the necessity to take action.\(^2\)

The underlying reasoning was that by placing the focus on large organisations and companies, sharper conclusions could be drawn and unequal comparisons could – to the extent possible – be avoided.

The research team reached out to the identified organisations both in writing and by telephone with the request to be placed in contact with their Chief Information Officer (CIO) or Chief Information Security Officer (CISO).

The members of the Steering Committee were also asked to provide the contact details of additional relevant individuals from their networks. The interview protocol (see Annex A) was shared with the respondents via email prior to the interview, for preparation purposes.

Considering the confidentiality and sensitivity of the requested information, it was decided – in consultation with the Steering Committee – not to refer to organisations by name, not even in a separate

\(^2\) This was confirmed by a number of interviewees from large companies in different sectors.
list without attribution of individual contributions. This last point was a conscious decision to as far as possible guarantee the anonymity of interviewees, considering the limited number of organisations interviewed per sector. A list of organisations in the annexes with, for example, references aggregated by sector, could still have compromised the anonymity of the organisations.

Reports were written of all the interviews and shared with the interviewees for validation purposes. Ten interviewees in total responded to the reports with additional remarks or corrections. This allowed interviewees to correct potential factual errors and to provide additional remarks before the interviews were analysed in the preparation of the research report. In addition to the 27 interviews with representatives from the critical infrastructure sectors, 3 individuals from the insurance industry were also interviewed to answer question 5.

1.6. Limitations

This research has a number of limitations. First of all, organisations within the critical infrastructure sectors are diverse, which means that interviewed organisations cannot be representative of their entire sector. This is an important limitation because at times references are made to organisations within specific sectors. References to sectors are solely being made to map differences between organisations whenever possible. In consideration of the anonymity of the interviewees, the references to sectors are a compromise to provide at least some information about their organisation. The generalisability of the findings is also limited due to the limited number of organisations interviewed.

The exclusion of SMEs is also a limitation of the research. Because of this, the report cannot provide an insight into the way in which SMEs approach cybersecurity and to what extent their experiences coincide with those of larger organisations, or what unique challenges they face with their cybersecurity approach.

Finally, the selection of organisations is also subject to limitations, because the research was entirely dependent on the willingness of organisations to participate and on representatives whose contact details were accessible. This means that organisations that were not reachable, as well as organisations that did not want to take part in the research, are left out of the study, even though their experiences may have provided different insights.

---

3 Unless explicitly stated otherwise, this report uses the term organisation for both public organisations as well as private companies.
By now cybersecurity has become a frequently used term in our daily vocabulary, both in the Netherlands and abroad. According to Hathaway and Klimburg (2012), the term cybersecurity was broadly adopted at the start of the new millennium, after the clean-up of the millennium bug. Hansen and Nissenbaum (2009, 5), however, recognise a longer history of the term cybersecurity:

The history of cyber security as a securitizing concept begins with the disciplines of Computer and Information Science. One, if not the first usage of cyber security was in the Computer Science and Telecommunications Board’s (CSTB) report from 1991, Computers at Risk: Safe Computing in the Information Age which defined ‘security’ as the ‘protection against unwanted disclosure, modification, or destruction of data in a system and also [to] the safeguarding of systems themselves’.

Just as with other societal challenges, the definition of the problem is part of the discussion. Despite the frequent use of the term cybersecurity, a single definition of the concept is absent and partially because of that do different stakeholders use the term in different ways (ENISA 2012).

As Choucri et al. (2012, 2) explain:

Trivial as it might appear on the surface, there is no agreed upon understanding of the issue, no formal definition, and not even a consensus on the mere spelling of the terms – so that efforts to develop policies and postures, or capture relevant knowledge are seriously hampered.

The absence of a single definition is enhanced due to the absence of a unified way of spelling the term, as indicated by Choucri et al. (2012). In both national as well as international policy and academic discussions, the term cybersecurity is spelled three different ways. One can speak of cybersecurity, cyber security and sometimes even cyber-security. Even the Dutch government appears to find it difficult to make a choice in this area. The first ‘National Cyber Security Strategy’ speaks of ‘cyber security’, and although the second National Cybersecurity Strategy carries ‘cybersecurity’ in the title, there remains a

---

4 As indicated on the website of the Cooperative Cyber Defence Centre of Excellence (CCDCOE) of the North Atlantic Treaty Organisation (NATO): ‘There are no common definitions for Cyber terms – they are understood to mean different things by different nations/organisations, despite prevalence in mainstream media and in national and international organisational statements.’ See: https://ccdcoe.org/cyber-definitions.html
National Cyber Security Centre (NCSC). These apparently trivial differences in spelling do lead to potential problems when trying to gather all the relevant knowledge within the domain (Choucri et al. 2012).

The relationships between the term cybersecurity and related concepts such as information security or I(C)T-security also lead to potential confusion and cloudiness about the answer to the question: what exactly do we mean with cybersecurity? This chapter shall first provide a short reflection on that question before moving on to discuss other aspects of the state of the art, including information about threats and developments in the area of cybersecurity.

2.1. From information security to cybersecurity

This chapter begins with the definitions as introduced in the two Dutch National Cyber Security Strategies. In the first ‘National Cyber Security Strategy’ (Rijksoverheid 2011, 3) cybersecurity is defined as follows:

Cyber security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information.

In the second ‘National Cyber Security Strategy’ (Rijksoverheid 2013, 7) cybersecurity is defined as follows:

Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems.

Both definitions demonstrate a connection between the concept of cybersecurity and the principles of confidentiality, integrity and availability (CIA) that form the core values of the concept of information security. However, that is where the similarities between the two definitions end.

The important difference is that the first focuses on an output commitment, whereas the second focuses on an effort commitment. The phrase ‘to be free of’, in particular, seems geared towards a state of absolute security, while the ‘efforts to prevent’ in the second definition suggests an attitude of risk acceptance (see also 5.1).

The introduction of the term ‘cybersecurity’, particularly for insiders who have been involved in the field for a long time, seems akin to old wine in new bottles. As Felten (2008) writes in response to a speech by United States (US) President Barack Obama:

\[5\]

According to one of the members of the Steering committee, the distinction is quite clear. With regard to names, the government uses Cyber Security and in running text the term is written as a single word: cybersecurity.
It’s now becoming standard Washington parlance to say ‘cyber’ as a shorthand for what many of us would call ‘information security’. I won’t fault Obama for using the terminology spoken by the usual Washington experts. Still, it’s interesting to consider how Washington has developed its own terminology, and what that terminology reveals about the inside-the-beltway view of the information security problem.

While Felten (2008) speaks specifically about Washington, his remarks have a broader reach. As a concept, ‘cybersecurity’ appears to be primarily used by, for example, policymakers, while the more technically-minded community continue to use the term ‘information security’.

2.2. Cybersecurity as part of national security

According to Zimmer (2013), it is predominantly due to a military thought process that cyber has been transformed from a prefix to a noun.\(^6\) Cyberspace is, after all, now considered to be the fifth domain of warfare, after air, water, space and land. Other authors also emphasise the militarisation of cyberspace (see O’Connell 2012; WRR 2015). This leads to concerns about cybersecurity being exclusively approached as a topic of national security. In a report about cybersecurity policy development, the OECD (2012, 32) writes:

> Another concern is that the lack of specificity of the term ‘cybersecurity’ in conjunction with the emergence of sovereignty considerations in cybersecurity policy making may lead to re-couch all cybersecurity issues into the language of ‘national security’ and warfare, preventing balanced policy making and fostering the adoption of drastic solutions such as network monitoring instead of other practical solutions more respectful of citizens’ rights. Discussions related to the protection of critical information infrastructures might influence broader cybersecurity debates towards national security thereby justifying sweeping unaccountable powers.

As early as 2005, Nissenbaum identified two perspectives in the area of computer security. The first perspective finds its roots in the technical approach of computer security, while the second perspective approaches computer security from a national security perspective. The dissection of different approaches to the terminology is important to understand how the formulation of the topic – popularly known as framing of the issue – can influence proposed policy options. As described in the report ‘The Public Core of the Internet’ by the Netherlands Scientific Council for Government Policy (WRR) (2015), over the years cybersecurity has increasingly entered the domain of national security. The WRR reflects, for example, on the state of affairs half a decade ago, when internet policy was primarily the concern of the Ministry of Economic Affairs, with a focus on aspects such as e-commerce and telecommunications. In the current era, the emphasis has been placed on cybersecurity’s role in conjunction with national security, which is why the Ministry of Security and Justice – especially the National Coordinator for

\(^6\) On LinkedIn there is even a group against the usage of cyber as a noun. The name of the action group is ‘detecting wrong use of cyber.’
Security and Counterterrorism (NCTV) – plays the leading role. This focus has certain negative consequences. As the WRR (2015, 11) explains, the engineers’ approach, exercised by Computer Emergency Response Teams (CERTs) (aimed at ‘keeping the network healthy’), and international cooperation within it, are inconvenienced by actors focused on national security, such as intelligence and military cyber units. This mixture of conceptions of security is undesirable because the partial interests of national security clash with the collective interest in the security of the network as a whole.

2.3. Cybersecurity: more than information security?

Cybersecurity is broader than national security – and national security is simultaneously also broader than cybersecurity – but how does the term cybersecurity relate to information security? Considering both terms are used interchangeably, and that they also share core values, the question must be asked: what is the difference between information security and cybersecurity?

Van den Berg indicated in an interview that he considers the usage of the CIA-principle in the context of cybersecurity as archaic (Ridderbeekx 2013). In his opinion, CIA is driven too much by technology and is too abstract for cyberspace. Von Solms and Van Niekerk (2013) argue that cybersecurity is broader than information security and identify the following examples to demonstrate the areas in which cybersecurity goes beyond information security: cyberbullying, home automation, digital media and cyberterrorism. Gartner also reflects on the term in its publication Definition: Cyber Security (qtd. in Franscella 2013):

Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries.

For Gartner, the inclusion of information technology’s offensive capacities is the dimension by which cybersecurity is considered to be broader than information security, as well as the grounds on which the connection with national security is (partially) established. Conversations about the use of offensive capacities take place, primarily, in regard to challenges in the area of defence. Hathaway and Klimburg (2012) also describe how the use of the term cybersecurity, usually speaking, reaches further than information security and ICT-security.

Cybersecurity is, in a sense, both broader and narrower than information security. It is broader because it also relates to, for example, network security. It is interesting to note in this discussion the European Commission’s use of the term ‘Network and Information Security’, and its indication that information security is a part of the ‘whole.’ Simultaneously, cybersecurity is also a smaller field than information security when a clear distinction is made between ‘physical information security’ and ‘digital information

---

7 The authors specifically write (2015, 83): ‘Five years ago, internet policy was basically a matter for the Ministry of Economic Affairs and was about e-commerce and the frameworks for telecommunications and the Internet. Anno 2014, the focus shifted to the topic of cyber security which falls under the Ministry of Security and Justice, to be precise, the National Coordinator for Counterterrorism and Security (NCTV). The Ministry of Defense is a close second with an operational Cyber Command and official authority to carry out defensive and offensive military operations on the internet.’
security.’ These are both part of information security, but in a narrow sense physical information security would not be considered a part of cybersecurity.

The above gives at least some insight into the different opinions about how to define the concept of cybersecurity. As indicated, besides its definition, the use of the word cybersecurity, including its spelling, is also a topic for discussion.

2.4. Threats come together in a fragmented overview

The importance of a single definition is also emphasised during the development of threat analyses. These threat analyses form an essential part of the way in which organisations treat cybersecurity and the measures they take. Different organisations – both public as well as private – develop threat overviews or trend analyses.\(^8\)

Gehem et al. (2015) have identified and studied a total of 70 reports in the cybersecurity threat analysis sphere. In their meta-analysis, they observe that the reports develop a rather fragmented overview. According to the authors, this has multiple causes. First of all, some reports focus on all potential threats in the area of cybersecurity, whereas other reports are more specifically focused on particular types of threats. Secondly, the focus of reports ranges from global, including all sectors, to others where the focus is limited to a select number of countries or sectors. The third observation is that the methodology used by existing reports differs and sometimes lacks transparency. This makes comparisons between results difficult and also influences the quality of the data. Gehem et al. (2015, p. 9) summarise the problem as follows:

> One of the main observations of our study is that the range of estimates in the examined investigations is so wide, even experts find it difficult to separate the wheat from the chaff.

Because of this, the authors conclude that, while there is certainly no lack of reports available in the area of risk analyses and threats, there is a lack of well-defined and comparable threat overviews and risk analyses. Gehem et al. (2015) are certainly not unique in their conclusion, although their meta-analysis based on 70 reports does grant their conclusion more weight. ENISA (2015, 79) identifies a similar problem in its ‘Threat Landscape’:

> The ‘publicity’ of threat information in related media is quite high. Threat landscape reports are important elements in the cyber-security community. Information on cyber-threats are [sic] quickly taken up by media. The number of publications has significantly increased in the reporting period. In the future it will be necessary to establish cooperation (consolidate efforts) among various players in the field to avoid duplication of work and increase quality of assessments.

---

Based on research (on a smaller number of sources) for this study, the same conclusion can be drawn. In particular, the lack of a broadly accepted taxonomy of threats leads to inequalities in the reports available. A clear distinction between a vulnerability, a threat, an attack and an instrument to exploit the vulnerability is frequently absent. This observation, combined with the variation in methodological approaches, means that existing threat analyses must be approached with a necessary level of reservation.

Through the Cyber Security Assessment Netherlands (CSAN), the Ministry of Security and Justice has tried to establish – at least for different targets in the Netherlands – an overview of threats since 2011. In the first CSAN a division was made which will be used for the purposes of this report. This categorisation of threats was also used during the interviews with representatives from organisations within the critical infrastructure sectors.

2.5. Classification of threats

Threats play an essential role in the debate surrounding cybersecurity, for organisations in both the public and private sectors. The threats that organisations are confronted with influence the way in which they treat cybersecurity and subsequently how much they are willing to invest in security measures. This part of the report, therefore, will briefly reflect on the different threats organisations are confronted with. A generally accepted categorisation of threats within cybersecurity at an international level is absent. The NCSC, previously known as GOVCERT.NL, in cooperation with other public and private parties, has published the CSAN since 2011. This report reflects on the previous period with the intent to use incidents and trends as a basis for the development of a threat overview for the future. The first CSAN identifies three categories of threats. These are information-related threats, system-related threats and indirect threats (GOVCERT.NL 2011). During the interviews, the focus was limited to information-related threats and system-related threats, although respondents voluntarily mentioned indirect threats.

2.5.1. Information-related threats

During the interviews, representatives of organisations within the critical infrastructure sectors were asked what they perceived as the largest threats to both their organisations as well as the whole sector. Considering the sensitive nature of this information, not every interviewee was willing to identify and describe the largest threats. Within the category of information related-threats, different types of information were discussed.

Personal data
A potential data breach – involving personal data – was a potential doom scenario for interviewees in different sectors. This was the case, for example, for organisations within the health sector, the finance sector, public administration and public order and safety. As such, a potential data breach can have consequences for the personal data of customers, business relations, patients or employees. The potential compromise of personal data of employees is a particular source of concern for organisations within all sectors. The NCSC (2014, 98) explains how the protection of privacy and the potential reputation damage caused by personal data breaches leads to an increased level of attention to the security of client
and personal data in all sectors. The potential reputation damage that accompanies the ‘loss’ of personal data appears to be the largest threat for organisations, as such an incident could seriously affect the level of trust that clients, employees and patients have in the organisation.

**Financial data**

The Global Information Security Survey 2014 developed by Ernst and Young indicates how surveyed organisations prioritise threats for their organisations. At the top of the list are cyberattacks with the intent of acquiring financial data such as credit card numbers and bank information. Kaspersky Lab (2014) indicates that organisations perceive the loss of client information (22%) and the loss of financial information (20%) as the worst possible data losses. Financial information seems particularly sensitive, considering that 7% perceive the loss of payment data and 5% perceive the loss of log-in credentials as the worst possible losses. Based on this, Kaspersky Lab (2014) concludes that in total 32% of organisations consider the worst data losses to pertain to financial data. This is perhaps understandable given the events of 2014, better known as the year of the Megabreach. In January 2014, American retailer Target announced how hackers had been able to compromise a total of 110 million accounts. In August 2014, a media report emerged announcing that the large financial services provider JP Morgan had fallen victim to a cyberattack which led to the compromise of 83 million accounts. The following month large Do-It-Yourself (DIY) store Home Depot announced that its payment systems were compromised, which provided perpetrators access to 56 million accounts. These three cyber incidents are considered – especially in the US – as the biggest incidents of 2014 (Tobias 2014).

The financial sector is often called the ‘testing ground’ for attacks. The Dutch Central Bank (De Nederlandsche Bank – DNB) (2014) speaks of systemic risks with respect to cyber-related threats and indicates how targeted attacks, in particular, may undermine the integrity and confidentiality of the information systems. With one eye on the future, this is an important observation.

**Intellectual property**

‘Theft’ of intellectual property is also mentioned as a potential threat for organisations. Organisations that are involved in scientific research, as well as organisations in the private sector which have sensitive information about their services, processes and products in development, explained how potential infiltration of their systems could lead to serious consequences. The financial consequences of theft of intellectual property are difficult to map, especially since, as one interviewee indicated, intellectual property damage could be very significant, but is difficult to make plausible. The actual damage caused by theft of intellectual property is difficult to prove. Nonetheless, it could have a big impact if a competitor went to market with a product, based on the intellectual property stolen, for a lower price and at an earlier date. The whole research pipeline of the organisation with the original idea becomes worthless. The challenge to demonstrate the damage caused by intellectual property theft is also discussed in the literature (see for example Cabinet Office 2015; Libicki et al. 2015). Libicki et al. (2015), for example, explain that the importance of intellectual property varies and depends on the mission statement of the organisation.
For organisations within the critical infrastructure sectors, system-related threats are perhaps even more worthy of attention. Potential manipulation of processes can lead to a state of physical insecurity. This is especially the case for organisations in the transport, surface water management, and public order and safety sectors, and the energy, chemical and nuclear industries. None of the interviewees indicated that such incidents had taken place as of yet, but they did speak of experiences with DDoS-attacks, which attempt to sabotage the business operations of organisations. In particular, the DDoS-attacks targeting the Dutch banks in the spring of 2013 were mentioned by several interviewees as a motivation to take action or to at least think about the necessity to take action (see 3.3). Even if websites are only providing information and do not offer any other functionality— as was the case with many organisations—DDoS attacks can still be a reason to take action, since such an attack can lead to reputation damage.

2.5.3. Indirect threats

Although not directly asked about indirect threats, interviewees did speak about such threats without a prompt from the interviewer. An example of an indirect threat—defined as an untargeted threat—is ransomware. Ransomware is a type of malicious software that limits access to a computer system by infecting the system and subsequently taking it hostage. To liberate the system, the owner or user is asked for money (a ransom) in exchange for the perpetrator that placed the ransomware removing it. Ransomware is also known as the police virus, because it pretends, or at least pretended, to be the police, the Federal Bureau of Investigation (FBI), or a representative from the movie and music industry, claiming that the user had carried out an illegal activity for which a fine had to be paid. The difficulty of ransomware—as indicated by a representative of an organisation within the finance sector—is that the victim of the ransomware ‘voluntarily’ transfers the money. There is no instance of fraud, which means the victim is responsible for the financial damage. Moreover, ransomware does not only implicate individual victims. Organisations can also be implicated when employees are ‘taken hostage’ by the malware. The Municipality of Lochem in the Netherlands, for example, was hit by ransomware (Beveiligingnieuws.nl 2015). In March 2015, Data Recovery Nederland (DRN) reported that just as many ransomware complaints had been received in the first quarter of the year as during the whole of 2014.

2.5.4. Reputation damage as the largest threat

During the interviews, multiple respondents mentioned reputation damage as the largest threat. This is not a threat in the more traditional sense, since it is more a consequence of an incident. As such, it is a secondary threat, because it accompanies incidents that occur as a result of information-related, system-related or indirect threats. Nonetheless, reputation damage appears to instil more fear than the direct damage caused by incidents. This is confirmed by Libicki et al. (2015, 19) when they write:

The effect of a cyberattack on reputation worried CISOs most, rather than more-direct costs. What actual intellectual property or data might be affected did not matter as much as the fact that any intellectual property or data were at risk. Two-thirds of all respondents specifically mentioned loss of reputation as the greatest possible fallout from cyberattack.
The fear of reputation damage appears exacerbated by the impact of incidents on organisations in the past. This is the case both in the Netherlands and abroad. In the Netherlands, the consequences for DigiNotar were irreversible and the organisation ultimately had to declare bankruptcy. The consequences for the corporate leaders of Sony and Target also indicate how incidents can damage organisations and their board members through reputation damage. In the next chapter the fear of reputation damage returns, as it influences the way in which organisations approach cybersecurity (see 3.3).

2.6. Developments introduce new challenges and opportunities

A discussion about threats would not be complete without a brief look ahead to the future. The digitalisation of society shows no sign of slowing down and new applications lead to new opportunities as well as new challenges. One of the developments that is often discussed is the Internet of Things (IoT). According to some experts, in the future, attacks on the IoT will transform from proof-of-concept to a regular risk (see, for example, Pescatore 2014). As of yet – as far as is publicly known – this has remained limited. Lyne (2015, 2) writes: ‘Perhaps the reason the Internet of Things has been less exploited so far is cyber criminals have yet to find a business model that enables them to make money.’ Nonetheless, the expectations are that this will change in the near future and that the IoT will introduce a new attack vector.

According to Trend Micro (2014), in the future, targeted attacks will occur more frequently than untargeted cybercrime. This prediction is based on a number of successful high profile attacks, which have led to the impression that targeted attacks via digital espionage can be an effective way to gather intelligence. Together with targeted attacks, Trend Micro (2014) suggests that social media, in particular, will be used as an attack vector.

In addition, cloud computing continues to be a recurring topic that will also be of importance in the future. As Friedman (2015) argues, cloud computing will be a big challenge for cybersecurity because it provides multiple entry points to data, which leads to an increased vulnerability for data breaches. Simultaneously, however, future developments also introduce new opportunities to enhance cybersecurity. Big data analytics, for example, is mentioned as an instrument to improve detection of fraud and security incidents. According to Gartner (2014), in 2016 a total of 25% of large companies will use big data analytics to detect at least one fraud or security incident. This is the case because big data provides companies with faster access to their data and demonstrates correlations between the different types of data. Gartner (2014) writes specifically that: ‘big data analytics enables enterprises to combine and correlate external and internal information to see a bigger picture of threats against their enterprises. It is applicable in many security and fraud use cases such as detection of advanced threats, insider threats and account takeover.’ The improvement of detection possibilities is of particular importance and will feature further in this report (see 5.1).
Prior to developing an insight into the nature and size of investments in cybersecurity, it is important to map which drivers exist for organisations to take cybersecurity measures within the critical infrastructure sectors. This chapter will first provide a short reflection on the theoretical approaches to cybersecurity investments before discussing a number of drivers. These drivers are identified based on the literature and the client, and were subsequently confirmed by the interviews.

3.1. Theoretical approaches to investing in cybersecurity are difficult to apply in practice

Relatively speaking, the literature devotes a lot of attention to the development of models to determine the optimal level of cybersecurity investments for organisations. Gordon and Loeb introduced their economic model for the optimal investment in information security in 2002. Their model is built on the assumption that organisations can exert influence on vulnerabilities by investing in information security, but that they cannot influence the reduction of threats. To come to an optimal investment level, an organisation needs to make a comparison between the expected benefits of the investment and the associated costs. The investment increases when the vulnerability increases. The second assumption states that organisations can, however, reach a point at which information\(^9\) becomes so vulnerable that the highest level of security can no longer be justified from an economic point of view. As Bisogni et al. (2011) indicate, Gordon and Loeb’s model (2002) assumes that all necessary information with respect to vulnerabilities, threats and impact of attacks is available. This is rarely the case, however, for cybersecurity in practice. Methods of attack change continuously and, on top of that, there is a reluctance to publicly share information about attacks and the associated costs for organisations (Bisogni et al. 2011). The lack of information leads to a situation where organisations may underestimate the risks of cyberattacks and thus engage in suboptimal investments.

Bisogni et al. (2011) describe how organisations lack the motivation to share information due to the characteristics of the market, even though sharing information can lead to organisations investing more in cybersecurity. The sharing of information by organisations is thus of essential importance for an optimal level of investment in the area of cybersecurity to be reached. Obstacles with regard to the exchange of

---

\(^9\) Gordon and Loeb (2002) specifically speak about information, because their model is focused on information security. For cybersecurity, network and system security can be added to the model.
information have been widely acknowledged in the literature (see for example Baker & Schneck-Teplinsky 2010).

According to Gallaher et al. (2006), there are two barriers to reaching an optimal level of cybersecurity investment. The first barrier, as also indicated by Bisogni et al. (2011), is an absence of complete information. The second barrier concerns the negative externalities of a cyberattack, which mean that the organisation that can influence the prevention or the reduction of the damage does not experience the damage, or at least the full damage, itself (Anderson et al. 2009; Kox & Straathof 2014). Because of these negative externalities, organisations invest less than the optimal level, according to Gallaher et al. (2006). Due to the existence of externalities and the nature of cybersecurity as a public good, every investment made by an organisation, especially in proactive measures, leads to more social than private benefits (Gallaher et al. 2006). As a result, organisations are inclined to invest less. As Moore and Anderson (2011, 1) write: ‘An economic perspective has yielded invaluable insights into the analysis and design of information security mechanisms. Systems often fail because the organisations that defend them do not bear the full costs of failure.’

Rue et al. (2007) provide an overview of the broad scale of the models available that focus on decisionmaking processes in the area of investment in cybersecurity. They indicate that several uncertainties exist about the best way for organisations to invest in cybersecurity. There are uncertainties about:

- Threats and vulnerabilities
- The consequences and impact of (successful) attacks
- The effectiveness of measures
- The shifting use of information technology
- The changing nature of threats related to cybersecurity
- The increase in attack methods and attack vectors
- The motives of attackers.

According to Rue et al. (2007) no single model alone can answer the question about an optimal level of investment for cybersecurity. In addition, there is also a lack of clarity about how these models operate in practice, when real as opposed to theoretical data is used to come to corporate decisions. As such, they indicate that a model has little value without reliable information. Rue et al. (2007) therefore propose that in some cases it is necessary to simplify and adjust the model according to the missing data instead of further expanding on the model without reliable and available data. Garvey and Patel (2014) make a similar argument when they argue that analytical methods used for cybersecurity economics have to be flexible depending on the information requirements. As they write:

Some investment decisions may necessitate methods that use in-depth knowledge about a mission’s information systems and networks, vulnerabilities, and adversary abilities to exploit weaknesses. Other investment decisions may necessitate methods that use only a high-level understanding of these dimensions. The sophistication of methods to conduct economic-benefit tradeoffs of mission assuring investments must calibrate to the range of knowledge environments present within an organization.
As described in a report by the World Economic Forum (WEF) (2013), the lack of a definition and understanding of cyber risks is one of the foremost challenges in their treatment. The quantification of the damage of an attack, the motives of the different threat actors and the determination of the probability that an incident will take place, remain difficult to establish. Without these basic instruments in the area of risk analysis, the WEF (2013) indicates that it is potentially attractive for decisionmakers to exclusively devote attention to, or invest resources in, aspects which they are certain about. This can lead to certain vulnerabilities being left unaccounted for.

In response to the question of whether companies and consumers invest sufficiently in cybersecurity, Romanosky (2013) states that the assumption is that companies invest insufficiently because cyberattacks and incidents are still taking place. This implicitly assumes that sufficient investment or optimal investment will lead to the complete elimination of incidents. In that sense, as Romanosky (2013) writes, an appropriate level of protection becomes the equivalent of an absolute level of protection. There is, however, a general consensus that a 100 per cent level of security does not exist (see also van Eeten 2010). The number of security incidents, therefore, is not a reliable indicator to determine whether the investments that have been made are optimal (Romanosky 2013). Ultimately, the ambition of finding the optimal level of investment is a difficult one to achieve. Libicki et al. (2015, 7) write: ‘While the optimal cybersecurity program is one that minimizes the total cost of cyberinsecurity (expressed as the sum of the resources spent on cybersecurity and the costs incurred because organizations are less than fully secure), no one really knows what that point is or how to get to it. And best practice is not necessarily optimal practice.’ The achievement of an optimal level of investment appears, therefore, to be primarily a theoretical exercise that is difficult to translate into practice. There are other ways, however, in which organisations decide which measures to take or what to invest in with respect to cybersecurity. These will not answer the question of what an optimal level of investment is for organisations, but they will provide more insight into what drivers incentivise them to take measures and how the dynamic between drivers, regulatory instruments and ultimate measures functions.

3.2. Regulation causes incentive for action

Regulation plays a leading role in the analysis of Gallaher et al. (2006). According to the researchers, regulation in the United States (US), especially the Gramm-Leach-Bliley Act (GLBA) and the Sarbanes-Oxley Act (SOX), has led to a significant increase in the cybersecurity budgets of financial service providers. Through such regulation, board members have had to devote more attention to the topic of cybersecurity. Closely related is the influence of notification requirements on the investments in cybersecurity (Gallaher et al. 2006). Other sources confirm this (see Kovacs 2014):

Over the past three years, organizations in the United States have increased cybersecurity spending partly due to regulatory pressure. Data protection laws that have already been introduced and ones that will be implemented over the upcoming period in Europe and the Asia-Pacific region are expected to accelerate spending on IT security solutions in these parts of the world as well.

Sales (2013) argues that companies do not invest enough in cybersecurity due to negative and positive externalities, free riding and the challenges associated with the protection of a public good. According to
Sales (2013), these are general challenges of administrative law. He links the cybersecurity problem to environmental law, anti-trust law, liability law and health law. Through the inclusion of these legal fields, the cybersecurity problem can be approached from a broader analytical framework, which will allow the answers to its challenges to be of a more generally applicable nature. Gordon et al. (2014, 29) also write:

Since most firms in the private sector look only at their private costs of security breaches, it is rational to expect them to under invest in cyber security activities relative to the social optimal. Accordingly, in order to move towards socially optimal levels of cyber security investments, there is a compelling argument for governments (or some other entity focusing on increasing social welfare) to explore a variety of regulations and/or incentives that are designed to get private sector firms to increase their cyber security investments.

Even so, during the interviews regulation was not mentioned by the respondents as a primary driver. In fact, one interviewee indicated that internal security requirements are much higher than regulation requirements. The same organisation amends its internal policy four times a year depending on developments in the area of, for example, threats and incidents. Policy has to function like a wiki: a living instrument which is easily amended based on new developments. This flexibility is necessary considering the changes in threat assessments based on the identification of new vulnerabilities, exploits and incidents. Regulation is usually behind, as it follows after the facts, and is therefore inherently less adaptive, because its development process requires more time. Another interviewee stated that even if regulatory frameworks are absent, measures still have to be taken due to the societal relevancy of safety and security of critical infrastructure objects.

Nonetheless, organisations are evidently preoccupied with upcoming regulation, especially at the European level, such as the European Union (EU) General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) Directive. Through the NIS Directive, the European Commission (EC) is trying to generate an incentive to ensure a high communal level of network and information security. The EC wants to improve the security of the internet and of private networks and information systems by obliging member states to improve their readiness and improve cooperation, and by obliging critical infrastructure providers to take sufficient measures and to have serious incidents reported to national competent authorities. These government measures enhance the pressure on organisations to take measures, but sometimes primarily because of the lack of clarity about how organisations can fulfil the requirements. Terms such as ‘appropriate measures’ are being used, but organisations do not have sufficient clarity of what that means, as became evident during the interviews.

Presently, organisations primarily use ISO27001, a specific standard in the area of information security, which was updated in September 2013 and came into existence through a cooperative effort between the International Standardisation Organization (ISO) and the International Electrotechnical Commission (IEC). This applies to both the public and the private sectors. For organisations within the national government, the primary instrument to function as a framework for information security is the ‘Baseline Informatiebeveiliging Rijksdienst’ (BIR). The BIR is entirely structured according to ISO27001 and ISO27002. Government actors are obliged to comply with both standards. The BIR replaces five other standards. These are the ‘Haagse Ring, Rijksweb’, for mobile data carriers, ‘Departementaal Vertrouwelijke webapplicaties’ and ‘Digitale Werkomgeving Rijk’ (DWR). As indicated in the
introduction of the BIR (Rijksoverheid 2012, 4), ‘These five sets of standards differ in structure, partially overlap one another and are therefore difficult to manage and implement. In addition, the ministries and implementing organisations each have their own baseline for information security. So many different sets of standards is confusing and impedes controlled security and the implementing and managing of the standards.’

Through the introduction of the ‘Taskforce Bestuur Informatieveiligheid en Dienstverlening’ (BID), organisations within the Dutch national government have received a boost through the development of a specific baseline. For the Water Boards (waterschappen), for instance, the Association of Water Boards introduced the Information Security Baseline for Water Boards (Baseline Informatiebeveiliging Waterschappen, BIWA). In addition, the municipalities – through the Baseline Informatiebeveiliging Gemeenten (BIG) – as well as the provinces – through the Interprovinciale Baseline Informatiebeveiliging (IBI) – have developed their own baselines. Taskforce BID places the emphasis on self-regulation, or basically the requirement for organisations to take responsibility for themselves.

Moreover, the former Minister of Security and Justice announced in 2013 the introduction of a notification requirement for ICT-intrusions. This notification requirement was submitted as a legislative proposal titled ‘Data processing and notification requirement cybersecurity’ in January 2015. As indicated in the explanatory memorandum, the proposal introduces ‘A duty to report any breach of security or loss of integrity of electronic information systems (hereafter: IT breaches) and lays down rules on the processing of data for the duties of the Minister of Security and Justice in the field of cyber security.’

The notification requirement exclusively applies to ‘Providers of products or services of which the availability and reliability is critical for Dutch society, and only if the infringement has resulted or could result in the significant interruption or potential of interruption of the availability or reliability of such products or services.’ Once implemented the notification requirement will require increased efforts that are certainly not welcomed by all organisations within the critical infrastructure sectors. One interviewee indicated that – based on the existing cooperative relationship with the National Coordinator for Counterterrorism and Security (NCTV) – he did not perceive the notification requirement as an obligation, while another interviewee perceived the idea of an obligation as undesirable precisely because of existing cooperative relationships and argued that there was a preference for continuing to report incidents on a voluntary basis. The introduction of a legislative proposal for a notification requirement in case of an ICT-intrusion owes a large debt to the digital crisis that occurred as a result of the DigiNotar incident (see 1.1).

During the interviews, some respondents spoke about other potential measures which could be either introduced or stimulated by the government to generate the necessary incentives. An example is to oblige organisations to a minimum number of basic requirements in the area of cybersecurity. The United Kingdom (UK) has already started this through the introduction of ‘Cyber Essentials’ (Department for Business, Innovation and Skills and Cabinet Office 2014). One interviewee referenced the often-made comparison with the manufacturing of cars with seatbelts, which is obligatory as a result of government regulation. If companies do not take responsibility for themselves, several interviewees suggested, regulation will have to fill that void. Another interviewee gave the impression that the pressure on
companies should be increased and that certain requirements ought to be imposed in the area of usage and availability.

3.3. Incidents lead to evaluation and measures

While the literature predominantly emphasises regulation, during the interviews the role of incidents surfaced as the primary incentive. The level of attention paid to cybersecurity, especially in the boardroom, appears to be determined in large part based on incidents. As Rossi (2014) explains: ‘without a cyber-attack occurring or anything going wrong, cybersecurity can be seen as an unnecessary expense, a burdensome cost on the enterprise, leaving many to question whether the amount spent on security was investment best placed. Fear is far too often employed in order to drive uptake, either through crises that have happened in the past, or hypothetical events that could occur in the future.’

Cybersecurity incidents enjoy a lot of attention, especially from the media, which means that the focus turns to the organisation (where the incident took place) with potential reputation damage and, for example, loss of customers as a result. The media attention, in particular, appears to be a primary driver for organisations to introduce (additional) measures. As one interviewee indicated, board members become nervous about potential reports in the media. An incident about a pumping station in Veere that occurred in February 2012 was extensively discussed in the media and was mentioned by two interviewees. The incident had a clear impact on the way in which organisations approach cybersecurity. Along with some other factors, this incident led to much attention for the relevant management. In a television broadcasting of EenVandaag, the editors of the news programme suggested that it was ‘child’s play’ for people to be able to remotely control sluices, pumping stations and sewage pumps from their homes through the internet (Bloem & Blokzijl 2012). The incident led to parliamentary questions. Other examples confirm this observation. During the interviews, several respondents referred to the Distributed Denial of Service (DDoS-)attacks on the banks in April 2013. Due to the DDoS-attacks, clients of different Dutch banks could not pay through iDEAL for several hours. In addition, clients experienced problems with internet banking and mobile banking (NOS 2013). These attacks were the topic of discussion during a high-level meeting between the Minister of Security and Justice and the Minister of Finance. For organisations both inside as well as outside of the financial services sector, this was a reason to take action, or to at least reflect on the possibility that a similar incident could also take place within their organisations. Incidents play a crucial role in drawing attention to the topic. This attention can be translated into bigger or different investments in cybersecurity at the respective organisation or organisations within the sector. One interviewee specifically indicated how incidents lead to increases in budget. His organisation received an additional budget of 600,000 euros as a result of DigiNotar. Risk management appears to be primarily based on the tangibility of the risk, as indicated by an interviewee. ‘Otherwise’, he added, ‘the willingness to invest in cybersecurity will never emerge.’ Another interviewee indicated that without the political urgency he never would have received money. The political urgency was generated as a result of questions asked in the Lower House of the Dutch Parliament based on incidents which had received media attention. Every time something else happened, the interviewee returned to the board to ask for more money. He used incidents to enhance their awareness.
Another interviewee described the situation as follows: incidents lead to evaluation and that can lead to improved measures. Libicki et al. (2015, 11) summarise the situation as follows: ‘Cybersecurity is a hard sell, especially to chief executives (unless they or someone they depend on has been breached).’ According to them, the topic does not receive attention from boardroom members until they are forced to pay attention when an incident takes place within their organisation.

3.3.1. Regulation forces stimulus of incidents through notification obligation

Based on the factors described above, an important connection can be made between the role of regulation and the role of incidents. The introduction of a notification requirement in California led to organisations having to notify their clients when their data has been compromised. This has led to a culture of transparency with regard to incidents, which has raised the pressure on organisations to take action. The focus primarily rests on taking measures to increase the level of cybersecurity as a means to prevent future incidents or reduce the damage in case they do occur.

Another type of measure is the adoption of a cyber-insurance policy (see 3.4), which (partially) transfers the risk and can at least reduce the damage or costs associated with incidents. In the US in particular, there is the possibility of legal action, which might lead to high costs.

3.3.2. Media attention for incidents can also be counterproductive

Incidents, and in particular the way in which the media represents such events, can also have potential negative effects or be counterproductive. As one interviewee indicated, the media’s treatment of incidents lacks nuance, which means reputation damage can have a significant impact. This is also described in the literature (Guinchard 2011):

> The discourse on cyber threats tends to be dominated by excessive publicity given to some threats to the detriment of others, and by exaggerated claims about the frequency and scale of the attacks. This narrative distorts the public perception of the threats and masks the need for better detection tools and information-sharing strategies.

The media attention devoted to an incident predominantly has an impact because of the pressure it places on an organisation to take additional measures. These additional measures predominantly have as their purpose to prevent further reputation damage, which is recognised by organisations as the greatest threat (see 2.5.3). Not all authors agree, however, about the impact that media attention has. Berninger (2014) cites several studies in arguing that negative media attention as a result of cyberattacks can lead to a reduction in the stock value of an organisation. Hovav and D’Arcy (2004), on the other hand, conclude, based on their analysis, that publicly announcing an attack has occurred has no impact on victimised companies.

3.3.3. Real damage of incidents is difficult to determine

According to Dean (2015) the damage that companies suffer as a result of an incident is relatively limited. Based on his analysis of data breaches and attacks that have been extensively discussed in the media, such as those on Target, Sony and Home Depot (see 2.5.1 Error! Reference source not found.), Dean notices
how the total damage is less than 1% of the annual revenue of these companies. After reimbursements from insurance policies as well as tax deductions, the damage is even lower. Dean (2015) describes how the original estimate of the damage for Sony was around 100 million dollars, but that ultimately the incident cost Sony rather ‘little.’ According to their quarterly statement, the incident cost Sony 15 million dollars in incident response and recovery measures. And the expectation is that the company will not suffer long term costs associated with the incident. Dean (2015) also discussed how much the large scale data breach at Target cost the retailer. Based on the most recent financial statements of the company, the total gross damage was 252 million dollars. Of that amount 90 million dollars has been reimbursed through insurance policies and 57 million dollars of the damage is tax deductible, which means that the ultimate damage for the company comes to 105 million dollars. This is the equivalent of 0.1% of the revenue generated by Target in 2014.

For Home Depot, another company that fell victim to a large scale data breach – in which a total of 56 million credit and debit card numbers and 53 million email addresses were compromised – the ultimate cost of the damage was 28 million dollars. This was after the company received 15 million dollars from its insurance policy. Based on these cases, Dean (2015) argues that there is a market failure due to the existence of information asymmetry. The comparison made by Dean (2015), however, does not take into account the overarching costs of an incident or a data breach. With a data breach of credit card and debit card data, other parties, such as card issuers, payment processors and other retailers where fraudulent transactions subsequently take place, are also involved and implicated (Weiss and Miller 2015). Then there is always the argument of reputation damage, which can only be mapped through indirect indicators, since reputation damage itself does not have a price tag. During one interview, a respondent from the insurance industry argued that the resignation of the Chief Executive Officer (CEO) of Target in May 2014 and the resignation of the Sony Pictures Entertainment co-chairman in February 2015 will certainly have consequences for those companies. Both resignations are – at least in the media – directly connected to the cyberattacks the companies suffered. Nevertheless, based on his findings, Dean (2015) concludes that there are limited financial incentives for companies to invest in better information security practices, and suggests that perhaps government regulation is necessary to improve the situation.

According to the Ponemon Institute (2014b), which carries out an annual study into the costs associated with data breaches, the average costs suffered by a company after a data breach increased from 5.4 million dollars to 5.9 million dollars. 10 This calculation is based on the amount of 'lost' data, or records. This, according to Jacobs (2014), is too simplistic a reflection of reality. Besides the financial damage, the Ponemon Institute also writes that companies that suffered a data breach also lost more customers than they previously did. Kaspersky Lab (2014) indicate that, based on their research, the average damage caused by a cyber-incident is 720,000 dollars, but can potentially escalate up to 2.54 million dollars. American intelligence and security agencies estimate that American companies suffer an average loss of 250 billion dollars annually in damages (Gertz 2014). 'Most of that theft,' writes Gertz, ‘is related to high-technology development and innovative developments that represent a key strategic economic advantage

---

10 The Ponemon model used to come to this calculation has been criticised. See for example: http://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/
Investing in Cybersecurity

for the United States over other nations.’ All of these estimates have to be placed into perspective, because the reliability of the data is difficult to determine.

Anderson et al. (2012) have carried out a systematic study based on available studies of the costs of cybercrime. As indicated by the authors at the start of their article, the study was carried out in response to a request made by the British Ministry of Defence as a result of its scepticism about available data, which potentially overestimated the problem. Anderson et al. (2012, 23) summarise the problem of damage indicators clearly when they write: ‘Previous studies of cybercrime have tended to study quite different things and were often written by organisations (such as vendors, police agencies or music industry lawyers) with an obvious “agenda”.’ Because of this, the gathering of reliable data is difficult and previous statements about the damage caused must be approached with hesitation. According to Libicki et al. (2015), the problem is predominantly the result of the focus on the threat as opposed to a focus on the risk. Libicki et al. (2015) claim that risk, as opposed to threat, should receive more attention.

### Box 1 Damage within the financial services sector

Since 2010, the Dutch Banking Association (NVB) has made figures about the damage caused by internet banking fraud publicly available. In March 2015, the NVB reported that the damage caused by fraud in online banking was reduced to less than half, from 9.6 million in 2013 to 4.7 million in 2014. As a result of the way in which Dutch banks continuously improve the automated detection of fraud attempts and thereby prevent damage, the cost of malware-related attacks has been reduced to less than 500,000 euros. The rest of the damage, 3.9 million euros, is caused by phishing. These figures stand in sharp contrast to the headlines in the New York Times in February 2015, which stated ‘Bank Hackers Steal Millions via Malware’ (Sanger & Perlroth 2015). The headline is based on a report by Kaspersky Lab in which the company describes how there is evidence that there is damage of at least 300 million US dollars due to malware related fraud in banks. Kaspersky Lab even indicates an expectation that it could be as much as three times the stated amount, causing other media headlines to indicate how one could potentially speak of a loss of 1 billion US dollars (BBC 2015b). However, the calculation of these figures is not included in the report by Kaspersky. The only indication of the calculation is to be found in Kaspersky’s reference to the fact that at least one bank has suffered a loss of 10 million US dollars and that the same could be true of 100 banks.

3.4. Insurance companies can potentially stimulate organisations to improve their cybersecurity practices

3.4.1. The emergence of cyber-insurance

The market for cyber-insurance policies emerged during the late nineties when companies that sold security software, such as antivirus software, initiated partnerships with insurance companies (LeLarge & Bolot 2009). According to LeLarge and Bolot (2009), the combination of security software and insurance was used as evidence to demonstrate the high quality of the security software. According to Guy Carpenter (2014), cyber-insurance policies appeared on the market in the US in 1996. The demand took off in 2002, after California became the first state to introduce a notification requirement, forcing companies to notify their customers in case of a data breach. This notification requirement opened the door to potential lawsuits, from which companies wanted to protect themselves through insurance.
policies. This process comprises two related steps. First, there is the introduction of the notification requirement, which allows liability to play a role in forcing companies to internalise externalities, subsequently leading to societal benefits. The second step is the subsequent introduction of insurance policies to transfer the risk. Presently in the UK – based on an estimate made by one of the interviewees – 90% of the cyber-insurance market is connected to American companies, where the notification requirement has been an important stimulant for the insurance industry in this area.

3.4.2. The cyber-insurance market is growing

The market in the US has grown to 60 insurance companies and an annual revenue of 1 billion dollars (Guy Carpenter 2014). Besides the US, the UK, especially England, and more specifically London, has grown into a large market in the area of cyber-insurance with 160 million pounds of insurance policies specifically devoted to cybersecurity. A large part of that goes to cover American data protection, or rather to execute the notification requirement in case of data breaches. Cyber is the fastest growing sector within the insurance industry (Cabinet Office 2015). Based on estimates from the Cabinet Office, the global premium income for independent cyber policies has increased by 50% in 2014 compared to the previous year. Presently, the global premium income is worth between 1.5 and 2 billion pounds, which is approximately 0.1% of the global property and casualty insurance premium pool.

According to the Ponemon Institute (2014a), in 2013 only 10% of respondents had a cyber-insurance policy. The number had increased to 26% in 2014. Baker and Schneck-Teplinsky (2010) explain that the uncertainty about the actual risk that an organisation faces means companies are less inclined to invest in cyber-insurance policies. Second of all, cyber-insurance policies are relatively expensive, which makes them less attractive. The availability of data about and from the cyber security insurance market is presently still limited (Romanosky 2013) and the available academic literature is predominantly theoretical in nature. Based on Romanosky’s (2013) personal correspondence, he states that the average insurance policy costs between 10 and 25 thousand dollars. Other sources cite rates between 10 and 25 million dollars, and even as high as 50 million dollars (Romanosky 2013), without providing the supplementary data, such as size of organisation and annual revenue. Moreover, based on interviews with Chief Information Security Officers (CISOs) in the US, Libicki et al. (2015) indicate how current insurance policies are frequently perceived as more hassle than they are worth. The CISOs perceived cyber-insurance policies to only be useful in specific cases and anticipated little benefit from having one. None of the interviewees for this research project had a specific cyber-insurance policy. All interviewees indicated that cyber-insurance did not play a role in their cybersecurity approach. Even though Libicki et al. (2015) report that approximately one third of their respondents (about six representatives) did have an insurance policy, they confirm the impression that cybersecurity insurance policies do not play a role in organisations’ approach to cybersecurity. As they explain: ‘Strikingly, in no case was insurance central to the process of improving cybersecurity (in contradiction to how fire insurance practices promote fire safety); it was a matter handled by corporate finance people with, at best, some input from the cybersecurity department.’

28
3.4.3. Expectations about cyber-insurance as an incentive for measures

Despite the doubts about the added value of cybersecurity insurance policies, cyber-insurance is still perceived as a powerful instrument to influence incentives for cybersecurity and to enhance the level of self-protection (LeLarge & Bolot 2009; Majuca et al. 2006; Cabinet Office 2015). In addition, Kesan et al. (2005) argue that cyber-insurance will lead to higher investments in cybersecurity, which would improve the overall level of cybersecurity. Moreover, cyber-insurance standards will facilitate best practices for organisations. Baker and Schneck-Teplinsky (2010) also suggest that the requirements from insurers could potentially become the standard for cybersecurity within a particular sector, with companies being stimulated to meet the insurer’s standard. A last benefit indicated by Kesan et al. (2005) is that the overall societal well-being could be improved through a growing insurance market in the area of cybersecurity. According to Baker and Schneck-Teplinsky (2010), the insurance market is potentially one of the most important instruments for the government to influence the private sector without direct regulation. By requiring a certain level of security, they argue, insurers can stimulate companies to invest in cybersecurity. The Cabinet Office published a report in March 2015 about the role of cyber-insurance policies in managing and reducing cyber-risks. In the report, the Cabinet Office also indicated how cyber-insurance policies can make an important contribution to the field of cybersecurity. The first reason for this is that the insurance rate that organisations pay to insurance companies proportionally decreases based on the measures they take in the area of cybersecurity. This supports the expectation described by Baker and Schneck-Teplinsky (2010) about the role of insurers in being able to determine the standard of security requirements. According to the Cabinet Office (2015) insurance policies go hand-in-hand with loss prevention, because insurance companies can use their insights based on their experiences with other clients. Moreover, insurance companies can apply their broader insights and experiences in the area of risk management to cybersecurity. Insurers themselves have mixed feelings about this. As one interviewee from the cyber-insurance industry in London indicated, insurance companies do not want to do the government’s dirty work. This is why, despite efforts by the UK government to convince insurers to introduce certain requirements, a number of insurers only endorsed Cyber Essentials (see 3.4.5).

3.4.4. ‘Moral hazard’ as potential downside

While some authors believe insurers can play an important role in the improvement of cybersecurity, Shetty et al. (2010) argue the opposite. They argue that the presence of cyber-insurers could actually work counterproductively. To actually use cyber-insurance policies as an effective instrument, two problems need to be resolved, according to Shetty et al. (2010). Firstly, to ensure enforcement of best practices in the area of cybersecurity, the traditional information asymmetry needs to be resolved. Secondly, free riding is also a problem with respect to cyber-insurers. Free riding can be prevented by obliging organisations to comply with certain security requirements. According to Hunker (2007)\footnote{Hunker (2007, 18) states ‘As a condition of receiving cyber security insurance in other instances, underwriters insist on the policy holder implementing a number of security enhancing measures.’}, insurance companies do already do this; yet this was not noticeable in the interviews carried out for this project (see...
3.4.5). In fact, not one single interviewee from the insurance market confirmed Hunker’s statement. Even so, the literature speaks a lot about information asymmetry and the presence of moral hazards. As Bailey (2014, 4) writes:

if the level of security infrastructure needed to price risk is lower than the level of infrastructure needed to adequately secure consumer data, firms with insufficient information-security possess an incentive to invest in infrastructure only up to the level that is required to purchase insurance coverage rather than investing to the level that is adequate for consumer protection.

The Cabinet Office (2015) notes that cyber-threat is presently ill-defined, leading to confusion about definitions based on different causes and consequences. Because of the growing demand based on American regulation, specifically the notification requirement, insurers frequently reduce cybersecurity to coverage for data breaches. The Cabinet Office (2015), however, identifies eleven types of potential damage as a result of a cyberattack, suggesting that cyber deserves a broader treatment than an exclusive focus on data breaches. The eleven types of potential damage are:

- Theft of intellectual property
- Business disruption
- Data and software loss
- Cyber exploitation
- Cybercrime and cyber fraud
- Privacy violation
- Liability to network failures
- Reputation damage
- Loss of physical goods
- Death and injury
- Incident investigations and response costs.

These categories partially overlap, and have largely been discussed in 2.5. Besides, they have clearly been developed from a bottom-up perspective, because they are difficult to place within a conceptual framework. This demonstrates the lack of maturity of the field of cybersecurity, especially in connection to cyber-insurance policies and threat analyses (see also 2.4). Nevertheless, the ability to determine the types of potential damage is essential to map what insurance companies need to compensate their clients for. One interviewee, a representative from the insurance market in the Netherlands, indicated that the average insurance policy in the area of cybersecurity covers the following costs:

- Notification – information obligation to customers
- Reconstruction of data
- Profit loss
- Legal advice
- Civil law penalties.
3.4.5. General criteria for cyber-insurance policies are absent, but in development

To genuinely provide a positive stimulant to organisations to improve their cybersecurity practices, insurance companies have to maintain certain security requirements or criteria for future clients. To identify these criteria, three interviews were held with representatives from the insurance market. The cyber-insurance market is still in its infancy in the Netherlands; therefore, two of the three interviews were conducted with companies in London. Based on those interviews, the conclusion can be drawn that companies in the US, in particular, take out cyber-insurance policies to receive coverage against potential costs associated with data breaches. This is especially the case with respect to the notification requirement in the US, which applies to the majority of states and certain sectors. Through the interviews with insurers in London, some insight can be developed about the criteria used by insurance companies before they issue a cyber-insurance policy. Presently, there is a group of insurers within the London market that is developing a general application form to streamline the information that is being requested from clients, and to perhaps work towards a set of basic security requirements. As indicated by two interviewees, at the moment companies still work with different application forms and there is no basic set of criteria or requirements dictated by insurance companies for future clients. The British government has tried to use insurance companies to make organisations adopt a basic set of security requirements, as one interviewee indicated. The report that the Cabinet Office published in March 2015 is the result of that effort. Insurers have, with a certain sense of reluctance, consented to require Small and Medium Enterprises (SMEs) to at least comply with the requirements as described in ‘Cyber Essentials’. Libicki et al. (2015, 17) describe the situation in the US as follows: ‘There was little evidence that any cybersecurity standards were being imposed by insurers (perhaps because they dealt with the financial side of the house rather than the operational side), nor was there much indication that such standards made a difference in how companies secured themselves.’

Looking ahead, it is difficult to say with any level of certainty whether the role cyber-insurance can play in theory will be put into practice. While at the moment it is certain that cyber-insurance does not play a role in demanding or stimulating minimum security requirements before organisations can obtain an insurance policy, the expectation that insurance companies will play an important role in the future must be approached with some scepticism. Based on the interviews with insurance companies in London, it becomes evident that they will not allow themselves to be used by the government for the purposes of setting standards to determine the minimum level of cybersecurity. However, an increase in regulation (such as the NIS Directive and the EU GDPR, see 3.2), and the related increase in obligations, may potentially lead to an increase in the adoption of cyber-insurance policies. The notification requirement in different states of the US has, after all, already had that effect on the insurance market.
This chapter describes the findings from both the literature and the interviews about the nature and size of investments in cybersecurity. The first part provides an overview of findings based on the literature review, while the second part discusses the findings from the interviews. During the interviews, the majority of organisations did not provide insight into the size of their cybersecurity investments. According to many, being able to map the size of investments in cybersecurity by organisations within the critical infrastructure sectors is a challenge and in some cases not possible at all. As a result, the second part of this chapter predominantly focuses on the underlying reasons that interviewees have shared to explain why mapping the nature and size of investments in cybersecurity is difficult. Moreover, in the last part this chapter describes the reactions of interviewees to the question of whether introducing a target number for investments in cybersecurity is desirable and feasible.

4.1. Available data about investments in cybersecurity is fragmented and difficult to compare

According to PwC (2014), organisations are starting to invest more in cybersecurity technologies and products as a result of incidents and regulation. According to the Ponemon Institute, 2014 was the year of the megabreach and 61% of the surveyed organisations decided to increase their cybersecurity budget by an average of 34% (Peters 2015). Nevertheless, 67% indicated that they had insufficient funds to defend their organisations against cyberattacks. Some 43% of respondents to the Global Information Security Survey 2014, published by Ernst and Young, indicated that their cybersecurity budget would remain the same, while 5% indicated that their budget would be decreased. Gartner has predicted that global IT-security spending will increase by 8.2% in 2015, which will make the total spending 76.9 billion dollars (Gartner 2014b). This estimate has led capital investment firms to invest massively in cybersecurity start-ups. According to Allied Business Intelligence (ABI) research (2014), in 2020 a total of 100 billion dollars will be spent on cybersecurity globally. Following the attacks on JP Morgan (see 2.5.1), the bank indicated in a letter to its shareholders that its cybersecurity budget would be increased by 250 million dollars over the next five years. This would amount to twice its current budget, but what percentage of their total revenue this figure would represent was not listed. JP Morgan is not the only financial services provider that decided to increase its spending after an attack (Huang et al. 2014). Sales (2013) describes how the general impression is that companies generally do not invest enough in cybersecurity. While empirical data about cybersecurity investments is absent, anecdotal evidence appears to support this statement.
The CyberEdge Group (2014) describes how one out of four surveyed employees doubts that their organisation invests sufficiently in cybersecurity. This percentage, however, provides a distorted image, when one digs deeper into the underlying methodology on which the conclusion is based. The CyberEdge Group asked employees to what extent they agreed with the following statement: my employer invests in an adequate manner in cybersecurity. Of the 522 surveyed employees, only 2% strongly disagreed with the statement, while 13% disagreed a little and 10% did not have an opinion.

Sales (2013) indicates how certain companies within the critical infrastructure, such as utility companies, have little competition, which means the threat of customer loss after an attack will have little impact on them. The absence of such market forces means, according to Sales (2013), that utility companies will not even implement costless security measures. Based on his analysis, strategically important companies, such as those within the critical infrastructure, would invest even less in cybersecurity than those outside. This reasoning was rejected by organisations during the interviews, with precisely the opposite opinion – that these organisations, due to their critical function, actually take (extra) measures in the area of cybersecurity (see also 3.2). For example, organisations in the energy, transport, public administration, surface water management, and public order and safety sectors, emphasised that their critical function is precisely the reason to treat security as a priority. For the implementation of the European Commission’s (EC) Network and Security (NIS) Directive, the United Kingdom (UK) carried out an impact assessment (Department for Business, Innovation and Skills (BIS) 2013). Within the assessment, an estimate was made that 1.98 billion pounds is spent on cybersecurity on an annual basis. The financial services sector and the public administration sector spent the most on cybersecurity: 706.3 million and 869.5 million pounds, respectively. The majority of this sum is spent by large organisations, approximately 1.45 billion pounds, while Small and Medium Enterprises (SMEs) collectively spend about 533 million pounds on cybersecurity. The average amount per large organisation is 540,000 pounds, while the average per SME is 26,000 pounds. What must be noted, however, is that the average per sector varies (Department BIS 2013).

The United States (US) Department of Justice has freed a budget of 722.4 million dollars for cybersecurity in 2015 (US Department of Justice 2015). This is an increase of 7.6 million dollars in comparison to 2014. These additional investments are reserved for the Criminal division and the Cybercrime and Intellectual Property Enforcement Program. The budget for the entire federal government has, however, been reduced from 1.44 billion dollars to 1.41 billion dollars (Elbarasse 2014). Certain domains have received a larger budget, while other domains witnessed their investments being reduced. Elbarasse (2014) writes:

Areas seeing increased levels of funding include threat and vulnerability management, data integrity and privacy management, access control and data recovery. But other areas would see a decrease in funding, include [sic] continuity of operations, continuous monitoring, and identification and authentication.

During his State of the Union speech, Obama pleaded for an increase of 14 billion dollars (Kerr 2015). The available data about investments – or, more broadly speaking, spending – in cybersecurity is largely
fragmented. Data comes from different sources, but primarily from the large consultancy offices such as Ernst and Young, PwC and Deloitte. According to Pierre Audoin Consultants (PAC) (2015), organisations in the Netherlands spend less on cybersecurity than their competitors in Finland and Sweden, but just as much as countries like France, Germany and the UK. This is calculated by PAC (2015) on the basis of the percentage of GDP. PAC does not mention real amounts in relation to cybersecurity budgets.

4.2. A lack of a unified way of counting leads to a lack of clarity and uncertainty

The absence of a single definition of cybersecurity and the different perspectives on what the term means have been discussed in chapter two based on the literature review. During the interviews, the topic of the absence of a single definition returned. The absence of a unifying and single way of defining which costs belong to the overarching field of cybersecurity, in particular, represents an obstacle to generating comparable data and to subsequently draw conclusions.

Which costs constitute cybersecurity is presently still difficult to establish because the term itself is still relatively new, meaning that organisations generally speak of IT- or ICT-security, or information security. This overlap between the terms leads to confusion and a lack of unity. Organisations therefore come across as uncertain or insecure about what actually should be counted to answer the question ‘how much does your organisation or your department invest in cybersecurity?’ In addition, interviewees indicated that measures (can) serve multiple purposes, which means the manner of classification can have an influence on the size of cybersecurity investments. Caution must be exercised to prevent the potential comparison of apples and oranges. Every organisation is constructed differently, which means the terminology is dissimilar, and that can lead to incomparable units. As such, it is unclear what costs can be attributed to cybersecurity. Interviewees expressed doubts about whether, for example, antivirus software, identity and access management, and redundancy should be counted. The answer to these doubts strongly depends on the meaning of the term cybersecurity. An organisation in the financial services sector had begun to develop a cost collection model in cooperation with partner organisations abroad. Unity at the sector level therefore appears to be the most appropriate first step to overcome this challenge.

4.3. Intermezzo: types of investments in cybersecurity

While answering the question on the quantitative aspect of cybersecurity investments, organisations also described the complications involved in answering questions about the qualitative aspect of cybersecurity, or rather the type of measures they invest in. Prior to the interviews, similar studies and relevant documents were analysed to make an inventory of available conceptual frameworks to categorise the types of measures. Commissioned by the Department of BIS in the UK, PwC (2013) has conducted a study into the investments in cybersecurity by organisations. In doing so, it used the following categories to classify the different types of investments:

- People aspects of cyber security
- Purchasing security products
This categorisation has been used for the interview protocol. To develop further insights into the ways by which cybersecurity spending can be categorised, and with regard to the importance of approaching cybersecurity holistically (see 5.1), interviewees were also presented with the following categorisation. The National Institute of Standards and Technology (NIST) has introduced five categories of activities that together embody the security lifecycle. These are:

- Identify
- Protect
- Detect
- Respond
- Recover.

For the interview protocol, a variation of these five categories was used, because the first phase, identify, was more geared towards recognition of the problem. These are:

- Prevention
- Detection
- Response
- Recovery

The division is not taxonomically justified. For example, a detection system prevents an intrusion from successfully taking place, so it can theoretically be classified as a preventive measure, but it can also be classified as a detective measure. This categorisation of measures was familiar and useful for some interviewees, whereas others hardly recognised it, or not at all.

In the area of prevention, a lot of attention is devoted to public awareness activities focused on employees. This includes training, campaigns and sometimes also conversations with departments or groups of employees. In addition, audits can also have a preventive effect because they identify vulnerabilities and notify organisations of those vulnerabilities. Moreover, organisations also work with penetration testing and ethical hackers.

In the area of detection, interviewees specifically spoke about Security Operations Centres (SOCs). According to Zimmerman (2014, 3) SOCs are the ‘focal point for security operations and computer network defense (CND) in the large enterprise.’ As Zimmerman indicates, SOCs come in different types and sizes. The size of the SOC is, of course, of influence on the capabilities the centre has. Zimmerman indicates that the activities and the mandate of the SOC can be broad. He provides the following list of (potential) responsibilities:

1. Prevention of cybersecurity incidents through proactive:
   - A. Continuous threat analysis
   - B. Network and host scanning for vulnerabilities
   - C. Countermeasure deployment coordination
   - D. Security policy and architecture consulting.
2. Monitoring, detection, and analysis of potential intrusions in real time and through historical trending on security-relevant data sources
3. Response to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures
4. Providing situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behaviour to appropriate organizations
5. Engineering and operating CND technologies such as IDSes and data collection/analysis systems.

Of these, the digesting and analysing of data is most time consuming for SOCs. This primarily focuses on detection of potential security incidents.

Security Intelligence and Event Management (SIEM) was another measure mentioned by interviewees, together with external monitoring. Interviewees explained that these measures in particular provided them with insight into what sort of attempts were being made to infiltrate their organisation.

In the area of response, SOCs are also applicable, since they play a role in the response when incidents occur.

Only the recovery category received little input from the interviewees. As one interviewee indicated, recovery is a luxury.

As indicated by PAC (2015), the conventional approach is to build a wall around the organisation to keep malicious actors outside. This approach is no longer sufficient, because organisations must look ahead to what happens once an incident takes place. According to PAC (2015), companies invest 85% of their budget on preventive measures and only 15% on detection and response. There appears to be a trend, however, in which spending is moving from prevention to detection and response (see chapter 5). Very little can be convincingly added on this topic based on the findings of the interviews, since only two interviewees provided a division of their budget according to the security lifecycle. One interviewee indicated that his budget was divided along the following lines:

- Prevention 60%
- Detection 20%
- Response 10%
- Recovery 10%

While the other interviewee had a very different division:

- Prevention 15%
- Detection 45%
- Response 40%
- Recovery 0%

This latter breakdown was provided by the interviewee who indicated that recovery was a luxury.
4.4. Cybersecurity is (too) interwoven in projects and processes

The second reason that multiple interviewees cited to justify why they did not provide insight into the data about their investments in cybersecurity, was the integration of cybersecurity in existing projects and processes within the organisation. As indicated by multiple interviewees, cybersecurity is not a separate unit cost. Cybersecurity features as a topic within decision-making processes, but in terms of the investment is integrated with other projects and processes. Because of that, isolation of the cybersecurity budget of a project or a process is a challenging, if not impossible, task. According to one respondent, (cyber)security is a quality aspect, which means it cannot be viewed as a separate aspect of products. Another respondent described how, when purchasing, for example, Supervisory Control and Data Acquisition (SCADA) systems, the security measures are already embedded in the system, which means they are part of the broader investment. This was confirmed at a broader level when another respondent stated that cybersecurity is implicitly included in every budget and that to attach a price tag to it is very difficult. The exceptions to this limitation include the projects and programmes that are specifically developed to enhance the level of cybersecurity. Within public sector organisations, there are a couple of examples where specific programmes and projects have been introduced in the area of cybersecurity and have subsequently received a separate budget.

4.5. Cybersecurity: quality over quantity

The third reason why mapping data on the size of cybersecurity investments is complicated is the qualitative approach to cybersecurity measures. During the interviews, respondents emphasised that cybersecurity is not approached from a cost perspective. The approach with respect to what measures need to be taken is primarily qualitative. The needs of an organisation in the area of cybersecurity are analysed based on a risk analysis. To develop a plan of action, different types and sources of information are used. This depends on the organisation, although certain connections became apparent between organisations and between sectors. Multiple interviewees mentioned using the information generated through the National Cyber Security Centre (NCSC) as an ingredient for their plan of action. Organisations also used the results of internal or external audits, and incidents from the past. Information originating from cooperative platforms such as the Information Sharing and Analysis Centres (ISACs) and comparable platforms were also mentioned as important input for the development of a plan of action. The measures that are mentioned in the plan of action are subsequently translated to a cost perspective. At that point, cybersecurity has to compete with other areas that require money in order to be executed, although this is certainly not the case everywhere. In some organisations, cost hardly plays a role. One respondent indicated that his board even asked him whether he needed more money. Reasoning logically, it can be assumed that a risk analysis is developed and translated to a cost perspective, and that the cost perspective then functions as input to answer the question of how much an organisation spends on cybersecurity. The persuasiveness of this argument, however, is disputable. Nonetheless, it must be considered that interviewees may not have been directly involved in the quantitative translation of their qualitative plans.
4.6. Critical reflection on the research question and the focus

4.6.1. Focus on investments is too limited

Even if an overview could be generated about investments in cybersecurity based on the cost perspective associated with the risk analysis and the plan of action, a challenge remains with respect to the scope of this research project. During the interviews, multiple interviewees indicated that the focus on investments was too limited. As indicated by multiple interviewees, exploitation costs are not included, which means an answer to the question – even if available – would only tell half the story. To come to the most comprehensive overview possible, a distinction has to be made between running the business and changing the business.

4.6.2. The added value of insight into the size of investments is a topic of discussion

The arguments that different interviewees provided to indicate why they did not provide insight into the nature and size of their investments are primarily focused on challenges related to effort. Words such as 'difficult' and 'complicated' were often used during the interviews. The lack of a unifying way to map investments, the absence of a single definition, the limiting focus on investments and the way cybersecurity is administered, are all reasons why gaining an insight into the nature and size of investments is a challenging task. This means that more work is required than organisations participating in studies such as this one are prepared to do. This simultaneously introduces the question – in part due to the response of certain interviewees – whether sufficient value is offered by having insight into the size of investments in cybersecurity. In particular, the last reason why gaining an insight into the size of investments is difficult to map (see 4.5), that is the observation that cybersecurity is primarily approached from a qualitative perspective, provides a prelude for a critical reflection on the research question.

By coming to a consensus about a cost collection model and a definition, the administrative challenges can be overcome, but a qualitative approach to cybersecurity also appears to have its advantages. Cybersecurity is primarily about taking effective measures. This is why in the current climate more mature organisations divide their attention across preventive, detective and reactive measures. Moreover, the interwoven nature of cybersecurity with regard to projects and processes is an advantage because cybersecurity should not be an afterthought or a separate attachment, but a part of the greater whole. Multiple interviews therefore indicated that the focus of the research should be more on the qualitative approach, which focuses on what type of measures organisations have introduced. These measures could indicate a certain level of maturity and preparation in the area of cybersecurity. This would be more meaningful than solely a number or a percentage.

4.7. The available data is too limited to draw conclusions

Some organisations did provide insight into the nature and the size of their investments in cybersecurity. From the chemical sector, two interviewees provided insight into their investments. For the energy,
telecom, transport, surface water management and public administration sectors, only one interviewee per sector provided insight, while the other organisation(s) did not provide such insight.\textsuperscript{12} For the organisations that provided (detailed) insight into their cybersecurity and IT-spending, an average of 3% of the IT-budget was spent on cybersecurity.

Despite the limited available data provided by organisations, some relevant – albeit non-representative – observations will be shared here. One interviewee indicated that at the moment the budget for information security for his organisation, including the staff, is three million euros. Three years ago it was approximately one million euros. This is an organisation where the total Information Technology (IT)-budget is approximately 70–80 million euros. The same organisation has indicated to the board that additional support is needed for cybersecurity. However, the interviewee indicated that three million was only a partial expression of the real budget, since all sorts of other costs are involved in the total budget for cybersecurity. This was confirmed by other interviewees, while a couple interviewees felt confident they had provided a comprehensive overview of the investments made by their organisations.

There are exceptions to the previously mentioned arguments about the complexity of giving insight into investments in cybersecurity. These are specific cybersecurity costs that are independent and as such automatically isolated. Examples are services that have been outsourced, such as external audits, external monitoring and penetration testing or ethical hackers. These measures comprise the core of Chief Information Security Officer (CISO) budgets in many organisations, while in other organisations – especially multinationals – the CISO-budget is a lot broader. With respect to the outsourced services, such as audits, penetration testing and ethical hackers, multiple organisations could provide an indication, but those amounts are hardly representative of the overall investment made in the area of cybersecurity. As one interviewee indicated, the directly traceable expenditures are marginal. Examples of such directly traceable costs or specific investments include awareness campaigns in the area of cybersecurity, which are only a small fraction of the overall package of measures.

4.8. Why did some organisations provide insight?

Due to the fact that some organisations – albeit a minority – did provide insight into their investments in cybersecurity, the question as to how this discrepancy can be explained was introduced during the interviews and during meetings with the Steering Committee. One potential explanation is the level of maturity of the organisation. The competence of being able to give insight into the nature and size of cybersecurity investments can be a potential indicator of the maturity of the organisation’s approach to cybersecurity.

This hypothesis – which can be tested in follow-up research – is, however, called into question when a more focused look is taken at the organisations that did provide insight. Roughly speaking, this includes two types of organisations. The first includes organisations – especially in the public sector – that have to ‘catch-up’, based on observations facilitated by external pressure that the cybersecurity situation within

\textsuperscript{12} As indicated in chapter 1, the number of interviews varied per sector between 2 and 4.

40
their organisation is in need of attention. These organisations have a specific programme or project focused on cybersecurity and can therefore provide a clear insight into their budget, because it is directly and exclusively connected to the project or the programme dedicated to cybersecurity. Some organisations are a step further behind and are currently exploring what they should be doing. In a repetition of this research, more organisations might be able to provide insight because they have specific programmes or projects devoted to the topic with the intention of catching up.

The second group of organisations that provided insight do indeed come across as more mature. They could potentially confirm the hypothesis. To do this, however, more research needs to be conducted, as previously indicated, and more information about the organisations needs to be included in the analysis.

Based on the findings of this research project, it is essential to emphasise that the ability solely to provide insight into cybersecurity investments is too limited as an indicator to determine the maturity of an organisation in the area of cybersecurity. More (qualitative) context is needed for that. One of the interviewees explained that a lot of measures have been taken because the organisation has been part of the critical infrastructure for ages. Within certain sectors there has always been attention for physical and whole system security, and cybersecurity can theoretically be seamlessly woven into that.

Nevertheless, it is potentially useful to reflect on the organisations that did easily provide insight into the size of their cybersecurity investments. This does, however, demand a more thorough analysis of other factors within the organisations to isolate why they are able to provide insight into their cybersecurity expenditures.

4.9. Introduction of a target number is undesirable and infeasible

During the interviews, representatives of organisations – as per the client’s request – were also asked whether the introduction of a target number was a desirable and feasible idea. A target number is an instrument to stimulate and advance a particular change. It is formulated as a number or an amount that a particular party – for example the government – wants to achieve. As indicated by Heemskerk and Fennema (2013, 399), since the start of 2013, the Netherlands introduced, by law, target numbers for a more equal division of high-level positions in the business world between men and women. Despite the legal nature of these target numbers, there are no sanctions or other consequences associated with failing to meet the target. Other examples include the target number used to ‘activate clients’ by the Netherlands Authority for the Financial Markets (AFM). The target number has to be implemented to stimulate banks and insurance companies to activate a certain number of clients to get rid of their unit-linked products (woekerpolis). While target numbers are frequently used for a variety of policy areas – from women at the top to minimising greenhouse effects – there appears to be hardly any literature available about the underlying theory or the reasons for the usage of such an instrument. It appears to primarily be a means to stimulate organisations or countries to take action. During the interviews respondents were asked whether the usage of a target number in the case of cybersecurity was a desirable and feasible idea. The first reaction of interviewees was often that they considered it a difficult or complicated issue. The majority of the interviewees subsequently indicated that they considered it both undesirable and infeasible.
Some interviewees showed enthusiasm. A target number could, for example, have value as a benchmark for the organisation. Based on the benchmark, an organisation could determine how it compares to the target number. If an organisation, for example, spends less than the target number, then that could be a motivation to subsequently look into the underlying reasons for that state of affairs. Another interviewee indicated that it would be pleasant to have a target number and that it could help to raise awareness in the case of resistance from the board. Simultaneously, however, the same interviewee also indicated that a qualitative checklist would be more valuable.

Two interviewees indicated that it would be possible to maintain a target number if clear conditions were introduced, and if the numbers were aggregated at the sector level. According to another interviewee, such a number would potentially be possible if it were defined in SMART (Specific, Measurable, Acceptable, Realistic and Timely) terms. Moreover, it would have to be clearly indicated whether the number applies to investments or exploitation costs. That would, however, be difficult to define in SMART terms, according to the interviewee. If the focus is exclusively on investments, then existing measures would be overlooked. The limited positive reactions were accompanied by conditions that such a target number would have to comply with in order to have some form of added value.

Arguments against the introduction of a target number, however, were extensively discussed during the interviews. First of all, a target number would lead to a misplaced focus on a particular percentage or amount. The added value of a number is absent if there are no further considerations about what the money is spent on and why particular choices are made. Several interviewees indicated that the role of cybersecurity must first be more clearly thought out, as well as the way through which cybersecurity will take place.

The necessity of a risk analysis, in particular, was emphasised during multiple interviews. leading to the conclusion that the diversity of risk profiles, even within sectors, could complicate the introduction of a target number and even make it undesirable. If cybersecurity is approached from a risk analysis perspective, then there is a conscious choice about the risk tolerance. Besides, every organisation – even within the same sector – has a different risk profile.

Furthermore, there were doubts about the added value of a target number because it does not in principle lead organisations to spend more on the field in question. Instead, one interviewee anticipated a larger administrative burden. The biggest risk associated with the introduction of a target number is the creation of a state of ‘pretend security’. Numbers can be easily manipulated, which means that creative accounting can be used to comply with the target number, according to one interviewee.

The introduction of a target number can also have potential negative consequences, because of the connection to finances. This refers back to the current approach to cybersecurity which is primarily qualitative rather than quantitative. In addition, the idea of a target number met with resistance because it would approach cybersecurity as an isolated, rather than an integrated, part of the organisation and its spending. It is precisely the intertwinelement of cybersecurity in the daily business operations of organisations that make it undesirable to start looking separately at how much is spent on the topic.

Instead of a target number, there was a desire – expressed by one interviewee – for knowing how much organisations spend on cybersecurity – which is the primary purpose of this research.
In case the idea of a target number is introduced, there was a clear preference for doing so through self-regulation within the sector. As an interviewee from the private sector indicated, a target number is definitely not something which can be forced through with government regulation. Another interviewee also expressed a preference for self-regulation and considered a transfer to government regulation only acceptable in the case that self-regulation had failed.

A target number does appear desirable for certain other parties. Rhett Oudkerk Pool, board member of the industry organisation Nederland ICT and CEO of Kahuna, for example, indicated in April 2015 that, in his opinion, organisations in the Netherlands should be spending 10% of their Information Communication Technology (ICT)-budgets on cybersecurity. In addition, Oudkerk Pool points out that Dutch companies spend more money on coffee machines than on securing their digital infrastructure. The awareness of the importance of a good approach and the right expertise in the area of cybersecurity must be increased at the boardroom level in companies, he argues. The problematic nature of such statements is that they are based on assumptions, since there is presently no reliable data available that can confirm this statement. Considering the challenges associated with mapping the expenditures in the area of cybersecurity, precaution must be exercised when making statements that lack nuance, both about the measures that have been taken as well as the introduction of a target number, without an appropriate basis for doing so. Furthermore such statements must be placed in perspective, considering the potential motives of those who make them.
Besides mapping the nature and size of investments in cybersecurity, this research also aims to contribute to the improvement of the level of cybersecurity in organisations in critical infrastructure sectors, both in the Netherlands and abroad. During the research, interviewees were asked for best practices. A number of these best practices are related to other trends that emerged during the interviews, as well as in the literature. This chapter has as its primary goal to indicate how organisations which are seemingly more mature in the area of cybersecurity approach the topic, by exploring a number of these trends. To this end, the best practices have been generalised, so as to be more broadly applicable.\(^{13}\)

5. From good to better

5.1. Risk acceptance as vehicle for a more holistic approach

The first step towards an improvement in the area of cybersecurity is the acceptance of the risk that an incident can take place. As one interviewee indicated, ‘we invest a lot, but I am under no illusion that we cannot be hacked.’ This realisation has also been internalised by other organisations, which appears to have introduced a trend of acceptance by organisations that successful attacks can take place. This has made the question of whether an incident will take place obsolete and has replaced it with when a successful attack will take place. In addition, this has shifted the focus to the issue of how quickly a successful attack can be detected. The emphasis has therefore become focused on the minimisation of damage and expediting the detection of attacks (Rubens 2015). The acceptance that a successful attack can and will take place also creates the environment necessary for cybersecurity to be approached from a more holistic perspective, and for the emphasis to be transferred from an exclusive focus on prevention to a broader focus on all phases of the security lifecycle. Although some interviewees did not demonstrate much of an affinity with this classification, others recognised it. Multiple interviewees indicated that they are investing more in detection and response. There is also talk of companies that are consciously investing less in prevention precisely to see what (attempted) infiltrations take place, as a means to learn from such incidents. As one interviewee indicated, being able to identify the reconnaissance phase is essential. The moment that malicious actors begin their reconnaissance, provides the organisations with a perspective on how to respond. Monitoring offers time and space to prevent an attack from being successful.

\(^{13}\) RAND Europe prefers the term good or promising practice because the evidence base needed for the use of the term best practice is higher than the answers offered by interviewees based on their experience. A best practice should be empirically tested before it can be regarded as such.
Another interviewee also indicated that – although at the moment attention is primarily being devoted to prevention, and less so to detection, response and recovery – the organisation’s board is recognising that further steps are needed. Although awareness was generally described by interviewees as an essential part of the cybersecurity approach, another interviewee indicated that within the Information Security Forum (ISF) the focus has transferred to behaviour based programmes. Awareness itself, the interviewee argued, is not enough. This opinion is also evident in the second ‘National Cyber Security Strategy of the Netherlands’, as demonstrated by the title ‘From Awareness to Capability’, and is also emphasised in the literature (see van der Meulen 2011a and 2011b). The magic word in the industry, according to another interviewee, is resilience. This has led to a tendency to invest more in resilience as opposed to prevention. The Dutch Central Bank (DNB) (2014) supports this assertion in its ‘Overview of Financial Stability’, when it writes:

> The scope must not only encompass prevention, but also detection and recovery procedures. As complete security can never be guaranteed, attention must also be devoted to monitoring and detecting cyber-attacks, with a view to identifying attacks at an early stage and taking the appropriate action.

The next phase of maturity is already being adopted by organisations within certain sectors. Based on the interviews, organisations in the private sector primarily appear to be investing in detection and response, whereas organisations in the public sector still appear to primarily focus on prevention. The missing factor, as indicated by one interviewee, is predictive measures. These could replace, or perhaps complement, recovery measures. Through the scanning of underground forums, for example, organisations could potentially anticipate certain attacks.

**External monitoring**

External monitoring was indicated by a number of interviewees as an important service for organisations to adopt. The 24/7 character of external monitoring, as well as the professional approach of external organisations, were aspects which respondents specifically mentioned as benefits of the adoption of such a service. As one interviewee indicated, the eyes of an outsider have a coercive effect. Besides, external monitoring also offers organisations an opportunity to ‘keep pace with’ the security levels maintained by the external providers. Although the service of external monitoring is already available on the market, one interviewee hoped that it would become a more accessible and mainstream service, through an increase in organisations offering the service, for example.

### 5.2. From organisation to integration of the supply chain

The second dimension for a holistic approach is the involvement of the whole supply chain or sector. This is more feasible for some sectors than for others. The airspace sector is an example where cooperation between different stakeholders has led to positive results, and is recognised to be of essential value, especially in the area of cybersecurity. As van Oudheusden (2015) writes, this interdependence and interrelatedness of all components within the aviation sector is felt particularly strongly in the case of cybersecurity. In the future, moreover, all systems and services will become even more intertwined with
Malicious actors are inclined to attack different organisations within a particular sector, or to approach the weakest link, which, due to intra-sector dependencies can have consequences for the rest of the sector. This has been recognised, for example, by the financial, retail and energy sectors. Integration of the supply chain has multiple advantages. First of all, through the exchange of information, organisations can potentially anticipate attacks. As indicated by the explanatory memorandum (Rijksoverheid 2015, 2) of the legislative proposal data processing and the cybersecurity breach notification: what is important about the notification obligation contained in the bill, is that it seeks to create a culture in which joint contributions to security are a central focus. The aviation sector, for example, has extensive experience with this practice in its efforts to establish a ‘just culture.’

Secondly, it is clear to the partners what impact potential attacks could have not only on the individual organisations, but more importantly on the supply chain. Thirdly, integration within the supply chain or the sector can lead to cooperation with regard to the introduction of measures on different levels. An example is the development of a Security Operations Centre (SOC), which from a cost perspective might be difficult to implement for a single organisation and might be more effective if it can be carried out by multiple partners within a specific sector. Besides, a SOC at sector level can also play a larger role, because it receives information from across the sector. This is, of course, only possible for a limited number of sectors.

5.3. Using existing crisis structures

For multiple interviewees, being part of the critical infrastructure is a core characteristic of their existence. Because of this, certain organisations already have an emergency structure in place when a crisis occurs. One of the suggestions offered by an interviewee was to use existing emergency structures for potential cybersecurity incidents. That this commando-like structure is of importance during a cybersecurity incident was also recognised by a representative of another organisation where such an emergency structure was absent. Cyber exercises exist precisely to train organisations to respond as effectively as possible during a cyber-crisis situation. Considering the probability that a cyberattack will be successful, every organisation should have such a commando-like structure in case a crisis occurs, and also practice its implementation, to identify which aspects of the structure require further attention.

5.4. Inconvenient is preferable to insecure

During the interviews, one interviewee indicated that it was best that certain critical systems were not connected to the internet. Since the integration of systems and processes with the external world leads to large risks, and subsequently reduces the control organisations have with respect to those risks, sometimes the best solution – especially for critical systems – is to leave them disconnected from the internet. This pragmatic measure was complimented by another interviewee, who was familiar with this practice at the organisation of the former interviewee. This process, better known as air-gapping – or the isolation of systems from the network – also features in the conclusions of Libicki et al. (2015), who describe it as a
useful option. They explain that air-gapping is especially used by organisations that possess intellectual property.

5.5. Information exchange is important

The sharing of information in the area of cybersecurity incidents and threats is a recurring topic within the domain. By sharing information between different organisations, a more comprehensive overview can be generated about the modus operandi of attackers, and the existence of vulnerabilities and threats in the area of cybersecurity. The sharing of information was also a recurring topic during the interviews. Cooperative platforms within the different sectors were considered valuable, because they provided insight into challenges which went beyond the individual organisation. In particular, the Information Sharing and Analysis Centres (ISACs) were mentioned. The importance of information sharing is also highlighted in other countries. As such, sharing information is a central theme in the ‘European Cyber Security Strategy’ that was published in 2013 (European Commission 2013). In February 2015, President Obama signed an executive order – ‘Promoting Private Sector Cybersecurity Information Sharing’ – to encourage and advance the sharing of information, especially threat information, within the private sector and between the private and the public sector in the United States (US) (Office of the Press Secretary 2015).

The sharing of information outside of the sector, however, remains a challenge, because trust is a fundamental issue for organisations. Libicki et al. (2015) therefore speak of a ‘web of trust’. The sharing of information can, after all, have negative consequences in the case that the information ends up in the wrong hands or gets misused, or, for example, ends up in the public domain, leading to reputation damage for an organisation. Furthermore, the impression is also often given that governments primarily want to receive information, but rarely want to share information with parties in the private sector. The European Cyber Security Group (ECSG) is a cooperation of four European ICT-companies, including the Dutch Fox-IT. The companies that are part of the ECSG use their cooperation to, among other things, introduce changes at the European level, so that more reciprocity starts to exist with respect to the sharing of information with governments (Schoenmaker 2013). Gordon et al. (2014) also suggest that sharing information has societal benefits in the area of cybersecurity. Simultaneously, however, they indicate that there are potential pitfalls, which prevent these benefits from being realised if economic incentives to share information are absent. Information sharing is difficult, for example, because of the potential policy implications. The legislative proposal in the US with the name ‘Cyber Security Information Sharing Act’ is particularly problematic for organisations such as the Electronic Frontier Foundation (EFF), because it requires companies to share threat information – including personal correspondence from their users – with American authorities without a court order. In light of the Snowden affair, some organisations argue, such a development is undesirable.
5.6. Active dissemination

The sharing of examples of good practices is the rule rather than the exception in the area of cybersecurity. Within different sectors, reports are frequently published which include examples of good practices, and good practices are shared and discussed during meetings. Multiple interviewees observed that there is a lot of information. What is subsequently done with the information, however, is a side of the story which remains neglected in light of discussions on the topic of good practices. As one interviewee argued, it is necessary not only to actively gather this information, but to subsequently draw attention to it. Therefore, it is important to draw attention to where these good practices are available. Merely having the information is one thing, but to subsequently disseminate it successfully is another thing. In the Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID), for example, a government portal has been developed which contains about fifty guidelines that have been written and made available to civil servants. This is with the intention of expediting the implementation of the Baseline Informatiebeveiliging Rijksdienst (BIR). Good practices, as far as they can be shared within the broader community, should be registered in a product catalogue. It is, according to one interviewee, a lot of work to map and to keep up-to-date, but it could be a valuable task for the National Cyber Security Centre (NCSC) to carry out.

A lot of good practices are already available and accessible, so the idea of developing a product catalogue could be further investigated. Examples of broadly available good practices include all documents produced and posted by Surfnet on its website as well as the Informatiebeveiligingsdienst voor Gemeenten (IBD). In addition, the ISF is also a source of good practices for its members. According to one interviewee, the ISF receives information about good practices from different sectors, but they are translated in a pragmatic way, making them more broadly applicable. This is specifically the case for ISO-standards and the proposed Network and Information Security (NIS) directive, for example.
6. Concluding remarks

The main research question at the start of this research project was:

**On what basis, in what way and to what extent do private companies and public organisations in the critical infrastructure sectors invest in cyber security?**

This made the primary focus of this study the mapping of the underlying reasons as to why organisations invest in cybersecurity, what they invest in and how much they invest. The first part of the question drew some useful insights from the interviews, because the responses clearly indicate the crucial role played by incidents in enhancing the urgency for cybersecurity, and also in stimulating the introduction of (additional) measures within organisations. This urgency is primarily brought to life through the fear of reputation damage, which is potentially enhanced through regulation, such as breach notifications which force organisations to become more transparent about their incidents. The potential aftermath, such as lawsuits with respect to liability, can be limited through the adoption of a cybersecurity insurance policy. At the moment, this is primarily the case in the United States (US), and to a lesser extent in the United Kingdom (UK), while in the Netherlands the cybersecurity insurance market is still in its infancy.

Moreover, the cybersecurity insurance market could play a role in stimulating organisations to take measures in the area of cybersecurity by maintaining certain criteria. This, however, is not yet the case. The dynamic introduced through the fear of reputation damage, the obligation to report incidents and the measures subsequently introduced to prevent or reduce future incidents, is clearly of influence on the ways by which organisations approach cybersecurity. Incidents are the largest incentive for action, and regulation, such as breach notifications, can make this incentive even more powerful. Nevertheless, an overemphasis on incidents also carries disadvantages due to the introduction of unrealistic expectations or the continued existence of such expectations. Incidents will always take place. The necessity is to reduce incidents as much as possible and, in particular, to reduce the damage caused by incidents through early detection, which allows for a timely and appropriate response.

While conducting the 27 interviews, it became apparent that the second and third parts of the research question, focused on the nature and size of cybersecurity investments, are difficult to answer, and also may have had a misplaced focus. Nevertheless, answers to those questions have led to useful insights and reflections. The gathering of data about the nature and size of cybersecurity investments is very difficult, for the following reasons:

- There is no single definition of cybersecurity
- There is no cost collection model about which investments should be counted
- Cybersecurity is too interwoven in products, processes and projects
- Cybersecurity is primarily approached from a qualitative perspective
Moreover, the emphasis on the collection of quantitative data was called into question during the interviews. This doubt also became apparent through questions about the desirability and feasibility of the introduction of a target number. This was, according to the majority of interviewees, both undesirable as well as infeasible.

Based on the interviews, it can be concluded that more emphasis should be placed on the nature of the measures that organisations have taken. This also becomes evident based on the good practices available and the identified trends. It is not so much about how much, but more about in what ways organisations invest. The qualitative part of the interviews did not provide a complete overview of the measures taken by organisations. Nevertheless, they did indicate that a holistic approach to cybersecurity, where risks are accepted, and detective and responsive measures are subsequently taken, would be advantageous to the cybersecurity level of organisations. This is also indicated by the literature. Incidents will take place, so the focus should be on early detection of incidents and a subsequent speedy and appropriate response to limit the damage as much as possible. As previously indicated, the largest threat perceived by organisations, both in the Netherlands and abroad, appears to be reputation damage. Both the media and politicians play an important role in this because they have the capacity to exaggerate the threat, which leads to a lingering emphasis on prevention, potentially hampering the speed of information exchange, a trend which can actually be counterproductive for the limitation of damage and the consequences of incidents. Society’s task, therefore, is to focus primarily on realistic scenarios and to relinquish its unrealistic expectations about total prevention.


Bloem, Willem Jan & Joost Blokzijl. 2012. ‘Sluizen, gemalen en bruggen slecht beveiligd.’ EenVanDaag, 14 February. As of 14 September 2015:
http://20jaareenvandaag.eenvandaag.nl/hoogtepunten/39770/sluizen_gemalen_en_bruggen_slecht_beveiligd


ENISA. 2013. ‘ENISA Threat Landscape 2013: Overview of current and emerging cyber threats.’ *ENISA*. As of 14 September 2015:


Gartner. 2014a. ‘By 2016, 25 Percent of Large Global Companies will have adopted Big Data Analytics for at least one Security or Fraud detection use case.’ Gartner, 6 February. As of 14 September 2015: http://www.gartner.com/newsroom/id/2663015


Kaspersky Lab. 2014b. 'Kaspersky Lab Presented Cyber Security Trends and Threat Landscape in Europe.' *Kaspersky Lab*, 3 December. As of 14 September 2015:
Investing in Cybersecurity


Oudkerk Pool, Rhett. 2015. ‘Organisaties moeten meer investeren in cyber security.’ *Nederland ICT*, 16 April. As of 14 September 2015: http://www.nederlandict.nl/?id=13844


Pool, Rhett Oudkerk. 2015. ‘Organisaties moeten meer investeren in cyber security.’ *Nederland ICT*, 16 April. As of 14 September 2015: http://www.nederlandict.nl/?id=13844


Rijksoverheid. 2012. ‘Baseline Informatiebeveiliging Rijksdienst - Tactisch Normenkader (TNK).’
Rijksoverheid. As of 14 September 2015:
http://www.earonline.nl/images/earpub/6/6f/BIR_TNK_1_0_definitief.pdf


Rijksoverheid. 2015. ‘Memorie van Toelichting (MvT).’ Rijksoverheid. As of 14 September 2015:
https://www.internetconsultatie.nl/cybersecurity/document/1464


Schoenmaker, Rene. 2013. ‘Fox-IT start Europese lobbygroep voor delen informatie.’ Webwereld, 23 April. As of 14 September 2015:
http://webwereld.nl/beveiliging/77502-fox-it-start-europese-lobbygroep-voor-delen-informatie


Wetsvoorstel melding inbreuken elektronische informatiesystemen. As of 14 September 2015: https://www.internetconsultatie.nl/cybersecurity


Appendix A Interview protocol

Category 0: Governance

1. What is your position?
2. What is the function of your department?
3. Where is your department located within your organisation?
4. How many employees does your department have?
5. Are you responsible for a budget?
6. If so, what is your annual budget?

Category 1: Nature and size of investments

7. What share of your budget is reserved for cybersecurity?
8. What percentage is this of your department’s budget?
9. What percentage is this of your overall organisation’s IT budget?
10. What percentage of your cybersecurity budget do you devote to:
    - People (staff, training, awareness)
    - Organisational measures (policy development, execution, implementation)
    - Products (anti-virus software, IDS, firewalls)
    - Services (consultancy, external audits, insurance)?
11. With regard to the above categories, what part of your investment do you devote to:
    - Preventive measures
    - Detective measures
    - Reactive measures
    - Recovery measures?
12. What other cybersecurity investments exist within your organisation outside of your department?

Category 2: Underlying rationale for the determination of your budget

13. How is the cybersecurity share of your budget determined?
14. What security requirements or industrial standards do you (have to) comply with?
15. What role do these play in your determination about how much and in what to invest in terms of cybersecurity?
16. What role do incidents play in your investment strategy?
17. What do you see as the biggest threats in the area of cybersecurity for your organisation and/or for your sector?
18. How does this influence your investment strategy looking forward?
19. What other factors influence your investment strategy?

Category 3: Best practices

20. Based on your experience and expertise, which measures, either from an organisational or a technical perspective, should be identified as best practices?
21. To what extent are these measures present in your organisation?
22. How should or could these best practices be (more) widely adopted and implemented?

Category 4: Development of target numbers for cyber security investments

23. Is the development of a target number (i.e. a percentage of IT budget) for the investment in cyber security desirable?
24. If so, why? If not, why not?
25. Is the development of a target number for the investment in cybersecurity feasible?
26. If so, why? If not, why not?
27. In case such a target number is both desirable and feasible, how should it be implemented? Through self-regulation or government regulation, or via some other form of governance?

Closing questions:

28. Do you have additional questions or comments which can help us with our research?
29. May we approach you if we have additional questions?

Thank you for your participation in this interview.