CPB Netherlands Bureau for Economic Policy Analysis

CPB Communication | 2016, July 6

Cyber Security Risk Assessment for the Economy

Conducted together with the Dutch National Cyber Security Centre (NCSC)

Centraal Planbureau

Centraal Planbureau
Van Stolkweg 14
Postbus 80510
2508 GM Den Haag

T (070)3383 380
I www.cpb.nl

Contactpersoon
Bastiaan Overvest
Tatiana Kiseleva
Bas Straathof

Aan: NCTV/Cyber Security
Datum: 6 July 2016 (Dutch version)
Betreft: Cyber Security Risk Assessment for the Economy

1 Introduction

CPB Netherlands Bureau for Economic Policy Analysis has conducted this risk assessment, together with the Dutch National Cyber Security Centre (NCSC) which is part of the National Coordinator for Security and Counterterrorism (NCTV), about ICT-related risks to the economy. This Cyber Security Risk Assessment (CSRA) discusses the economic problem areas around cyber security and the resulting risks to Dutch companies and consumers. The assessment was partly funded by the Dutch Ministry of Security and Justice.[1]

1.1 Main findings

Information and communications technology (ICT) has penetrated all layers of society and the economy. Cyber security, therefore, has become increasingly important, and so has combating cybercrime. Cybercrimes differ from traditional crimes, because perpetrators are more difficult to track, economies of scale are larger and it is easier for cyber criminals to operate on an international scale. This involves various risks to Dutch companies and consumers.[2]

1. Financially motivated cybercrime, such as ransomware, is on the increase. For internet-related crimes, the chances of being caught are small, while the internet is becoming more significant for the economy. Technologies such as DDoS attacks and ransomware are offered as services, which is why also criminals without any technological knowledge are able to cheat and commit blackmail and fraud. Bitcoin is the digital currency that facilitates financial transactions between criminals and between them and their victims. Cybercrimes may become easier to combat by enabling the digital reporting of crimes, as well as by increasing the

[1] This document was authored by Tatiana Kiseleva, Bastiaan Overvest and Bas Straathof (all CPB), with contribution by Remco Mocking, Ali Palali and Robin Zoutenbier (all CPB). In addition, advice was obtained from a sounding board group consisting of Kees den Breeijen (Tele2), Bert ten Brinke (SIDN), Kas Clark (NCTV/NCSC), Michel van Eeten (TU Delft), Bas de Groot (CBS), Jan Kortekaas (NCTV), Erik Leertouwer (WODC), Michel van Leeuwen (NCTV/NCSC), Ronald van der Luit (EZ), Mireille Reiners (Capgemini) and Remco Ruiter (Betaalvereniging Nederland). Our thanks also go to Alex de Joode (Nederland ICT), Simon van de Geer (Ministry of Security and Justice), Ben Vollaard (Tilburg University) and other experts, for their ideas. The responsibility for the analysis and its conclusions lies solely with CPB.
[2] See Table B in the Appendix for an extensive summary

knowledge on the subject among police, and to bring current fines more in line with the size of criminal profits. (Sections 2.1 and 3.1 and Chapter 4)
2. Providers offering cyber security solutions often only operate on national or regional levels, because their customers mostly prefer large or well-known providers. Therefore, new security solutions may receive less attention. The government could offer greater possibilities to start-up companies through Small Business Innovation Research (SBIR) contracts and business certifications. In addition, re-consideration of international agreements on export licences may improve access to foreign knowledge. (Section 2.2)
3. Unsecure software and unsecure digital services continue to create opportunities for criminals. Vendors of software and digital services are provided with insufficient incentive to compete on product security and, therefore, assume only limited liability for product reliability. A legally required minimum product liability may provide vendors with incentive to increase the security of their products. (Sections 2.3 and 2.6)
4. The practice of phishing poses a threat to email reliability. Governments and businesses, therefore, increasingly use secure messaging systems. Government authorities and semi-public organisations could improve the appeal and reliability of email as a reliable way of communicating, if they themselves more often would use existing secure standards for authentication and encryption, such as TLS, DKIM, SPF and DMARC. The 'comply or explain' concept could be enforced more stringently. For the Netherlands, Idensys and iDIN may offer alternative platforms for reliable communication. (Sections 2.4 and 3.2)
5. Advanced, financially motivated attacks may become a threat to key processes within the financial sector. Cyber security could become part of integral supervision in all key sectors, similar to that in the financial sector. (Section 2.5)
6. Economic espionage by state actors may have a negative impact on profits related to commercial research and development investments. (Section 3.3)
7. Large data leaks and DDoS attacks remain likely. In addition to the direct costs for the victims and potential victims, this may limit the use of vulnerable services via the internet. Parties that have the best information and possibilities to ensure sufficient security levels should be awarded more responsibilities. Internet service providers (ISPs), for example, could play a larger role in the prevention and mitigation of DDoS attacks. (Section 3.3 and Chapter 4)

1.2 About this assessment

This cyber security risk assessment (CSRA) in intended to provide insight into the underlying causes, consequences and magnitude of cyber risks; thus, helping policymakers and businesses to understand and prioritise those risks. Where possible, the CSRA also discusses government policy options. It builds on the NCSC's Cyber Security Assessment Netherlands 2015. These annual assessment reports by the NCSC provide an overview of trends in relation to cyber security. The added value

of the CSRA particularly consists of its economic analysis of cyber security, with a focus on market failure limiting cyber security and the ensuing risks to businesses and consumers. The emphasis in the CSRA is on financially motivated cybercrime, whereas the Cyber Security Assessment Netherlands also includes vandalism, activism, terrorism and espionage – all of which can also damage the overall confidence in digital economic communication.

All the data used for this assessment are fully accessible and can be provided by CPB on request. The data sources are provided in the appendix to this report.

1.3 Analytical framework

According to the National Cyber Security Strategy of the Dutch Ministry of Security and Justice and the National Coordinator for Security and Counterterrorism (NCTV), 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.' Cyber security can become compromised – whether intentional, unintentional, or with malicious intent. Cybercrime concerns the last. A formal definition of risk is that of the effect of uncertainty on targets.[3] This report centres around two types of uncertainty: 1) about the scope and consequences of cybercrime, and 2) about the way in which cyber security problems can be solved. The main objective of this assessment is to contribute to achieving the optimal cyber security level, from a societal perspective.

The significance of cyber security for the economy cannot be quantified – and this is also true for the risks described. Not only because of the difficulties in measuring it, but also because, as yet, we simply do not know how to determine the costs and benefits of increased cyber security for the economy. Although some reports provide estimates of economic damage in relation to cybercrime, these studies are usually based on best guesses by experts and/or obscure methodologies. The significance of ICT for the economy in general is also not easy to determine, although statistic research has been conducted into this aspect. In the period between 1995 and 2004, when ICT use increased substantially, the increase in productivity was over one percentage point higher. Any causal relationship, however, has not yet been established.

Figure 1.1 shows the general framework of this report. It primarily distinguishes between market failure, problem areas and threats/manifestations. Market failure occurs when decisions made by businesses and consumers do not lead to the socially desired level of cyber security. Here, five general causes of market failure are distinguished. For example, a transaction between two parties may also have certain consequences for others (i.e. 'external effect'). Furthermore, the market may also fail

[3] ISO 31000 (2009) / ISO Guide 73:2002.

when a monopolist limits production in order to make more of a profit (i.e. 'market power'), or when vendors have more information on a certain product than its potential buyers (i.e. 'asymmetric information'). Systematic flaws in reasoning (i.e. 'irrational behaviour') can also be the cause of market failure. And, lastly, markets may also fail when uncertainties about the future make entering into contracts more difficult (i.e. 'incomplete contracts').

Market failure may lead to either less or more cyber security than would be considered optimal, from a societal perspective. The maximum level of security is typically not optimal, as the benefits to society do not outweigh the costs of achieving that level. Many businesses therefore conduct a quantitative cost-benefit analysis for their investment decisions regarding cyber security. Such analyses for the economy as a whole cannot yet be done. However, a market failure analysis may indicate the areas where cyber security is possibly too weak or too excessive – and what could be done to change the situation.

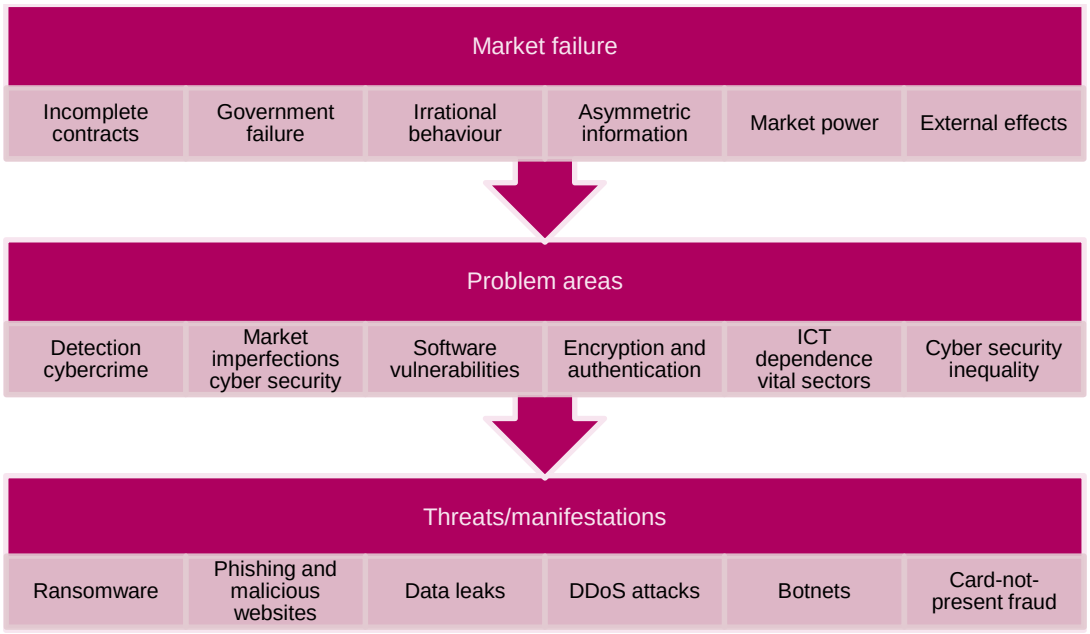
Market failures create various problem areas with respect to cyber security. These problem areas not only relate to cybercrime but also to cyber security in general. Software vulnerabilities or a sub-optimal market for cyber security solutions, for example, may also lead to disruption or failure of ICT systems.

Threats and manifestations are the third element of the analytical framework shown in Figure 1.1. Threats and manifestations, here, refer to the concrete ways in which cyber security is reduced and the means used to achieve this reduction. These particularly concern cybercrimes, activism and espionage; for example, phishing emails, data theft, and DDoS attacks.[4] The difference between a threat and a manifestation is that the former represents a potential disruption and the latter an actual disruption. The way in which threats are made can change. Whenever people have become used to a certain risk or when a technological solution to the threat has been found, the method becomes less effective and cyber criminals will look for new alternatives.

Threats and manifestations of cybercrime are brought about by combinations of problem areas. For example, software vulnerabilities (e.g. 'zero days' and publicly known shortcomings) mean computers can be hacked, and sometimes the detection of cybercrime is rather inefficient. The problem areas of 'ICT dependence of vital sectors' and 'Cyber security inequality' relate to the possible consequences of cybercrime.

[4] See ENISA (2016) for an elaborate taxonomy of threats (link)

Figure 1.1 Analytical framework of the Risk Assessment



1.4 Selection of subjects and reader

Chapter 2 discusses the problem areas we consider important: detection and prosecution of cybercrime (Section 2.1), the market for cyber security (Section 2.2), software vulnerabilities (Section 2.3), encryption and authentication (Section 2.4), ICT dependence of vital sectors (Section 2.5), and inequality in cyber security (Section 2.5).

These problem areas, and combinations thereof, lead to a large number of different types of concrete threats and manifestations. For this study, we selected four subjects, based on the literature[5], topicality[6] and discussions with experts. Chapter 3 provides an analysis of ransomware (Section 3.1), phishing and malicious websites (Section 3.2), and data leaks (Section 3.3). DDoS attacks are discussed separately in Chapter 4. The purpose of that discussion is to illustrate how these problem areas lead to specific threats, and not to estimate future threats to cyber security.

[5] CSBN (2015) and Symantec (2016) mention, for example, ransomware and phishing as important manifestations of cybercrime.
[6] For exampe, in April of 2016 alone, large data leaks occurred: personal data on 50 million Turks were said to have been published online (link), and 2.6 terabytes in financial data on the wealthy were revealed (the so-called Panama Papers) (link).

2 Problem areas

2.1 Detection and prosecution of cybercrime

Introduction

Following an investigation by the Dutch Team High Tech Crime (THTC) in the Coinvault case, police arrested two people from the city of Amersfoort on 14 September 2015. The Coinvault virus was a cryptoware virus that encrypted the files of victims, which was then used to blackmail them. The virus infected at least 2000 computers and led to payments from around 30 victims.[7] The amount obtained by the criminals in this case is unknown, but in comparable cases illegal profits were estimated at hundreds of thousands of euros.[8]

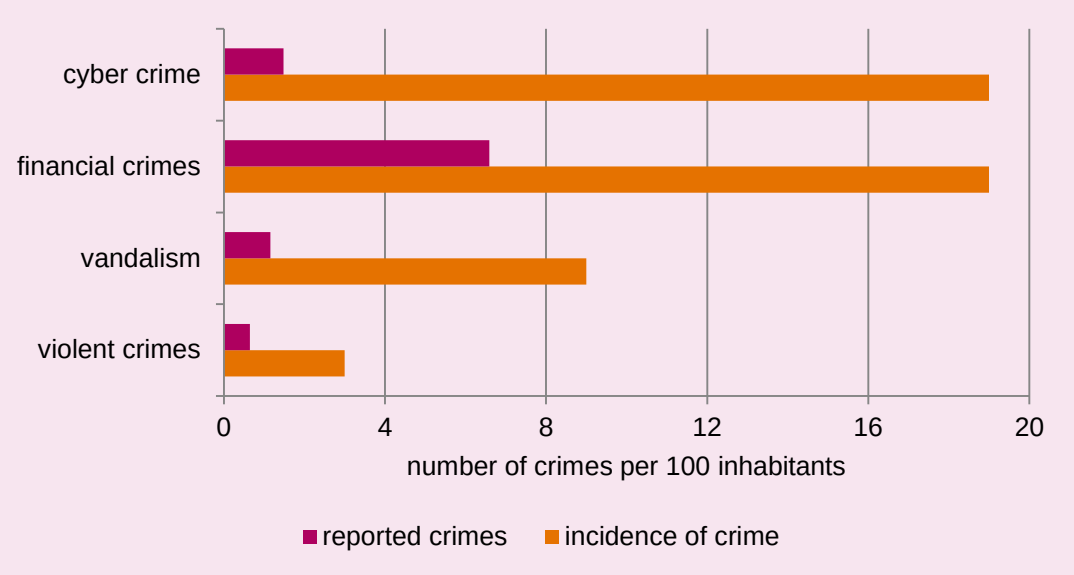
In this particular case, the criminal justice system was able to solve the case but not to prevent it. How effectively is cybercrime being deterred in the Netherlands by policy, the Public Prosecution Service (OM) and the judiciary? What are the possibilities for increased prevention of cybercrime?

Crimes, criminal complaints and penalties

With the rise of ICT within society, cybercrime[9] has become an everyday feature of life. In 2015, 11% of the Dutch population fell victim to cybercrime.[10] In that year, 19 cybercrimes were committed per every 100 inhabitants – indicating that some people were affected multiple times. Figure 2.1 shows the number of incidences and registered criminal complaints in a comparison between cybercrimes and other criminal offences. These days, cybercrime is as common as financial theft.

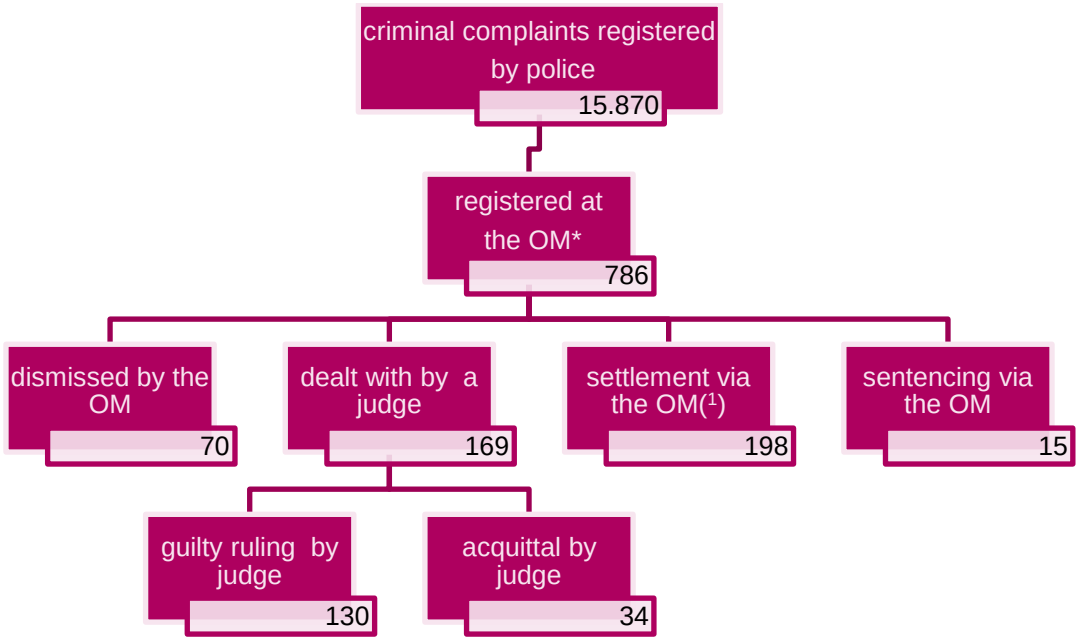
[7] NCSC (2015).
[8] See Section 2.1 and NCSC (2014), Table 6.
[9] Cybercrime involves crimes committed using digital methods. This may refer to traditional crimes, e.g. fraud, swindle and theft, which are committed using new means, but also includes 'hardcore' cybercrime, where ICT is both means and objective.
[10] CBS (2015), Veiligheidsmonitor [Safety monitor]. The forms of cybercrime investigated by the CBS are identity fraud (including phishing), sales fraud (concerning either non-payment or non-delivery of goods and services bought online), hacking (e.g. illegal access to an email account) and cyberbullying.

Figure 2.1 Cybercrime occurs regularly, but is not often reported



Source: CBS Veiligheidsmonitor 2015. Sample size: 111,252.

Figure 2.2 Hacking and the criminal justice system (2005–2014)



* OM = Dutch Public Prosecution Service
Source: CBS, *Tabellen criminaliteit en rechtshandhaving 2014* [Tables on crime and the judicial system 2014]. *Computervredebreukzaken 2005 – 2014* [Incidence of hacking 2005–2014]. ([1]) Settlement cases refer to cases settled via the Public Prosecution Service (OM) by which suspects avoid prosecution.
Note: CBS data represent yearly registered cases. In addition to hacking, also other forms of cybercrime are also punishable by law, such as the wilful destruction of data. See De Cuyper and Weijters (2016), for an overview of juridical aspects of cybercrime.

The figure notably indicates that relatively few cybercrimes are being reported. The percentage of registered criminal complaints is: 8% for cybercrimes, whereas for violent and financial crimes this is 21% and 35%, respectively. The low percentage of reported cybercrimes may be due to the victims' low expectations of perpetrators being caught by policy, the limited damage they suffered, or feelings of embarrassment.

According to law enforcement data, there were nearly 16,000 registered criminal complaints of hacking, over the 2005–2014 period[11] (Figure 2.2). During the same period, the Public Prosecution Service (OM) processed 786 complaints. In 343 cases of hacking, the crime was either punished (130 guilty verdicts) or settled (213 settlements).[12]

For hacking, the chances of being caught appear slim, as the number of filed complaints is much higher than the number of guilty verdicts. In order to serve as a deterrent, in addition to the chances of being caught, the type of penalty is also important. In cases of hacking, judges may impose a prison sentence of up to four years, depending on the type and severity of the crime, or impose a fine of up to 20,250 euros (in the fourth category). The courts may also order compensation payments to victims. Table 2.1 shows that, over the last 5 years, on average, judges imposed fines or ordered compensation payments in cybercrime cases of over 7,000 euros and prison sentences of one year.

Table 2.1 Overview of judicial rulings on cybercrime

Year of ruling	Average penalty or fine (euros)	Prison term (years)	
		average	highest
2011	1,812	0.8	3
2012	500	1.2	2
2013	8,969	1.2	3.3
2014	582	0.5	1.1
2015	11,227	1.2	3.3
total	7,362	1.1	3.3

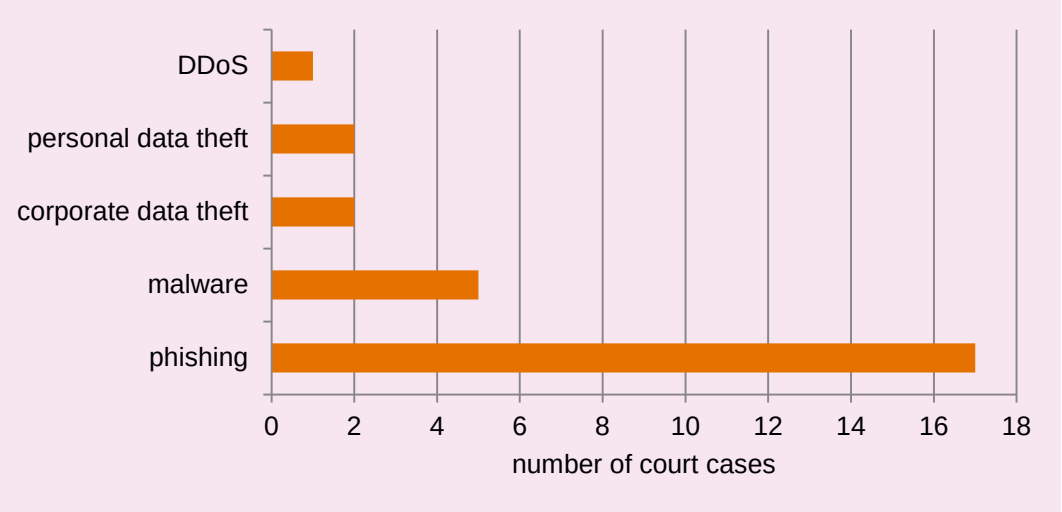
Source: rechtspraak.nl. Note: information on court cases was obtained by CPB by searching the database on the key words: 'computervredebreuk', hacking, DDoS, malware, viruses and phishing. Crimes in which cybercrime was not the main object, such as child pornography, were not included in the analysis. Penalties, fines and prison terms were calculated on the basis of 'guilty verdicts'. Not al court cases are published on rechtspraak.nl. The table, therefore, only contains a selection of all cybercrime cases in the Netherlands.

[11] Hacking (Dutch: 'computervredebreuk') is the term used for gaining unauthorised access to a computer or network. Examples of cybercrime involving hacking include phishing, the construction of mala fide websites and the distribution of malware.
[12] Note that affected companies may contain multiple victims, which is why multiple criminal complaints may lead to a single court case.

An average fine of 7,000 euros may seem high, but is in fact rather low, compared to the profits made by some cyber criminals. Ransomware, for example, may yield between 2,770 and 83,000 euros per day.[13]

Because both the penalties and the chances of being caught are relatively low for cybercrime and ICT's increasing economic significance for society, financially motivated cybercrime may be expected to increase. This can be seen from the large share of phishing crimes in court cases on cybercrimes of the last two years (Figure 2.3).

Figure 2.3 Number of court cases per type of cybercrime (2014–2015)



Source: rechtspraak.nl.
Note: information on court cases was obtained by CPB by searching the database on the key words: hacking, DDoS, malware, viruses and phishing. Crimes in which cybercrime was not the main object, such as child pornography, were not included in the analysis. Penalties, fines and prison terms were calculated on the basis of 'guilty verdicts'. Not al court cases are published on rechtspraak.nl. The table, therefore, only contains a selection of all cybercrime cases in the Netherlands.

In addition to the detection of criminals, the police is also actively involved in the obstruction of criminal acts. This occurs often in collaboration with banks and ISPs.[14] If the chance of catching criminals is slim, obstruction can be an effective measure to reduce criminal profits and, thus, increase the level of security.

Economic insights into detection

Cybercrimes often work according to the same mechanisms as those of more traditional crimes. Similar to during physical incidences of burglary, cyber criminals also invade the domain of their victims to either destroy or steal property. Therefore, existing economic insights into crime also apply to cybercrime. Like other criminals, cyber criminals – either consciously or subconsciously – also consider the costs and

[13] See Section 2.1 and NCSC (2014), Table 6.
[14] Examples of obstruction of crime are addressing the (unknowlingly) facilitation of cybercrime by hosting firms (link) and the stopping by the policy of 'money mules' – individuals who were recruited by criminals to facilitate money laundering (link).

benefits of a particular crime. All criminals will only commit a crime if the expected benefits outweigh the expected costs.[15] Those costs are usually the direct costs of the crime, the chance of being caught times the severity of the penalty and the thus missed alternative income.

Precautionary measures (e.g. anti-burglary windows[16] or using a strong password) may increase a criminal's direct costs. A wide application of precautionary measures may lead to an across-the-board reduction in crime; if the level of security is improved for most homes and vehicles in a certain district or city, local criminals will be less inclined to burglarise them.[17] Improved security of much-used ICT applications, such as operating systems, will therefore also lead to less cybercrime. This requires a well-functioning cyber security market (Section 2.2), secure software (Section 2.3), internet users being able to identify each other and being able to protect their data (Section 2.4).

In addition to these similarities, there are also differences between traditional crime and cybercrime. To begin with, perpetrators usually are more difficult to detect within the cyber domain. New technologies make it easier to commit cybercrimes while remaining anonymous and practically untraceable. For other types of crime, there is often physical evidence (in cases of burglary, fencing and violence) that helps to identify the perpetrators. Internet criminals, on the other hand, may demand payment in bitcoin, conceal their IP address and encrypt their data. Such masking technologies do not exist for traditional crimes.

In second place, cybercrime has larger economies of scale. Malware, which uses software vulnerabilities, or a smartly drafted phishing email can make many victims within a short period of time. This can be very lucrative for cyber criminals. For detection, the large scale on which this occurs implies that there may be many more victims than those that have filed a criminal complaint. Multiple complaints may also be traced back to a single perpetrator. Another source of economies of scale is the emergence of 'cybercrime as a service', where cyber criminals hire out botnets to other hackers or develop and resell malware techniques.[18] These things make cybercrimes cheaper and easier to commit.

The third important difference between cybercrimes and traditional crimes is the fact that it is much easier for cyber criminals to operate on an international scale. After all, geographic distances are not a factor in the cyber domain. Dutch police detectives, therefore, also depend on their foreign colleagues, and the effort and time involved in

[15] See for instance Becker (1968).
[16] See Vollaard and Van Ours (2011) for an empirical study on the impact of anti-burglary windows on the incidence of burglary.
[17] Ayres and Levitt (1998) show that the availability of Lojack systems (a piece of equipment that helps to trace stolen vehicles) has led to a sharp decrease in the number of car thefts.
[18] See, for example, Samani (2013) and NCSC (2015).

the harmonisation between the various police forces make it more difficult to investigate international cybercrime.

And, finally, there is a difference in insurance. Damage caused by traditional crime against property can usually be fully insured, but in cases of cybercrimes, insurance is still in its infancy. For example, close to 97% of Dutch households has property insurance, which covers any damage resulting from burglary.[19] A possible explanation for the difficulty of insurance against cybercrime is the moral danger. Because of the digital character of such a crime, victims may find it hard to prove their computers were hacked. Digital traces of hacking are difficult to find. In addition, such damage is also more difficult to quantify. The market value of a stolen physical good can be determined relatively easily, but cybercrimes often involve personal data or intellectual property – the value of which is much harder to determine.

Policy options

The low direct costs of cybercrime, the slim chances of being caught, the relatively low penalties and the high incidental profits make financially motivated cybercrime more attractive. If these three factors do not change, then neither will the threats from cybercrime. One of the focal points of the Dutch security strategy (Veiligheidsagenda 2015–2018) is that of countering cybercrime. The police, for example, has set the target of addressing 360 cybercrime cases in 2018 and to also involve regional forces in these efforts. An advantage of this objective is that the police is targeting cybercrime in a way that is both steadfast and measurable. Disadvantage of such quantitative objectives is that, if the focus is on the number of crimes, this may affect the quality of police work.[20] Moreover, changing regional circumstances call for flexibility (Vollaard, 2003).[21]

The Dutch Cabinet, furthermore, has recently submitted two legislative bills to the House of Representatives – the Cybercrime Act III ('Wet computercriminaliteit III') and the Data Processing and Compulsory Reporting Cyber Security Act (Wet gegevensverwerking en meldplicht cybersecurity). The bills increase police authorisation in the detection of serious crimes and they oblige key organisations to report serious ICT hacks.

The percentage of registered criminal complaints related to cybercrime may increase if criminal complaints could be filed digitally, for the most prevalent types of cybercrimes – after all, the internet is the 'crime scene' of cybercrime. Victims, currently, have to physically go to a policy station to file their complaints, where they are dependent on the knowledge of the individual officer who registers the complaint. If such a complaint goes unrecognised as being a punishable crime, or if the officer

[19] Dutch Association of Insurers (2016), p. 14.
[20] Also see Goodhart's law: "Once a measure becomes a target, it ceases to be a good measure."
[21] Alternative performance systems are discussed in Vollaard (2003).

does not describe the crime correctly in the dossier, the chances of expert detectives being put on the case are slim. For this reason, the Dutch national registration office for reporting internet fraud (Landelijk Meldpunt Internet Oplichting) conducted an experiment with digital filing of criminal complaints of online sales fraud and, over the last years, guide books were written in order to increase the knowledge among duty officers.

Public-private partnerships may help to provide detection services with more insight into the latest threats to companies. Furthermore, countries could increase their collaborations on combating cybercrimes, seeing the international character of cybercrime. A first step in this direction could be a European register of cases of cybercrime and/or criminal complaints.

The effectiveness of an increased chance of catching cyber criminals could be enhanced by raising the fines and by more serious other penalties. The maximum fine could be determined on the basis of the expected illegal profits from the particular crime, as is currently already applied in competition law. When the chances of catching criminals are slim, the obstruction of criminal behaviour can be an effective method in the fight against cybercrime. And the policy may also use economies of scale in obstructing large-scale crime.[22]

Finally, the saying 'opportunity makes the thief' also applies to the cyber domain. Without potential victims, no potential perpetrators. In order to counter cybercrime, it is important that potential victims are aware of the risks and, therefore, able to make a cost-benefit decision about investing in cybercrime prevention. The following sections describe a number of reasons why potential victims are running unnecessary risks.

2.2 Market for cyber security

Introduction

Fox-IT, one of the largest cyber security firms in the Netherlands, was acquired by UK cyber security consultancy NCC Group, in late 2015. Fox-IT provides a wide variety of security services to government authorities, financial institutions and other vital companies. Reason for the takeover, according to Fox-IT, was the opportunity for international expansion through the NCC Group.[23] This begs the question of whether the Netherlands is becoming too dependent on other countries for its cyber security? And, if so, how much of a problem would that be?

A well-functioning cyber security market also requires a well-functioning demand side. There are indications of the government not properly performing its role of

[22] See, for example, footnote 14.
[23] See this Fox-IT press release.

purchaser[24], and SMEs and consumers often also seem more interested in the price of cyber security than in the security level this would achieve.

The market for cyber security

Cyber security products and services contribute to safe (and more) ICT use in the economy and society.[25] Examples of such products are antivirus software, firewalls, encryption, identification systems and big data technologies for pattern recognition. Examples of services include security consulting (advice on preventative measures), testing the security of ICT systems (penetration testing), and diagnosis and emergency measures in cases of cyber security incidents.

The supply of cyber security products and services is increasingly incorporated into other ICT services (e.g. software) and non-ICT services (e.g. consultation), because cyber security is increasingly already taken into account during the design and development phases of digital systems and technologies, rather than later on. For example, VKA/SEO (2016) shows that 10% of Dutch ICT companies also offer cyber security services. This combining of cyber security with other products and services makes it difficult to distinguish a separate market for cyber security.

Table 2.2 Widely varying estimations on the size of the cyber security market

Source	Method	Economy	Size (turnover)	Derived size of the Dutch market
European Commission[26]	unknown	EU (2013)	11.2 billion USD	0.4 billion euros
VKA/SEO (2016)	survey	Netherlands (2014)	7.5 billion euros	7.5 billion euros
Pierre Audoin Consultants (2013)[27]	bottom-up	United Kingdom (2013)	3.3 billion euros	0.9 billion euros
Pierre Audoin Consultants (2012)[28]	survey	France (2011)	5.0 billion euros	1.8 billion euros
Bundesministerium für Wirtschaft und Technologie (2013)[29]	administrative (VAT) data	Germany (2012)	6.2 billion euros	1.4 billion euros

Note: The size of the Dutch cyber security market was derived by multiplying the estimated market size with the ratio between Dutch GDP and the GDP of the economy in question.

Table 2.3 shows that the estimations of the size of the cyber security market (converted for the Netherlands) vary between 0.4 and 7.5 billion euros. This variation may be due to the use of differing market definitions and research

[24] See the report by the temporary ICT committee (Tijdelijke Commissie ICT) (2015). (link (in Dutch))
[25] See Pierre Audoin Consultants (2013) for a comparable definition.
[26] link to the source.
[27] (link) to the source.
[28] See link.
[29] See link.

methodologies, or because the various national cyber security markets are in differing developmental phases.

Most cyber security firms are nationally oriented, but there is a small group of international companies who operate within most European countries.[30] Examples are Symantec (software), IBM (security services) and Cisco (hardware security). In the Netherlands, in 2008[31], the five largest providers together had a market share of 19%.[32] These global providers generally compete with a large number of smaller European companies, such as Fox-IT in the Netherlands and Sophos in the United Kingdom. European providers mostly operate only on national or regional levels. The average, combined 20% market share of the top five providers is not large compared to many other ICT and non-ICT markets. If the market share is assumed to be a good indicator of market power and demand substitution, the supply side of the market does not appear to have a problem of oligopoly.

On the demand side of the cyber security market, a distinction can be made between government, large enterprises and retail (consumers plus SMEs). The segment for the government is estimated at 33%, for large enterprises this is 48% and retail covers 19%.[33]

Barriers to an effective market

One of the barriers to an effective market is the fact that the European market for cyber security services seems fragmented; small to medium-sized European companies often cannot expand beyond national borders to thus achieve economies of scale. This could be because customers, such as government authorities and consumers, prefer either national or global players. The preference for well-known brands is not necessarily a bad thing, as the large players often have a reputation to uphold and are able to offer a more extensive package of services and products.

Another barrier for international service provision results from the fact that knowledge about cyber security can also be applied offensively. Knowledge about an unknown (zero-day) software vulnerability can be used not only in security but also in cyber attacks. Therefore, exporting such services may require an export permit. Agreements about this subject have been made, internationally, in the so-called *Wassenaar Arrangement*. Further investigation may reveal whether these restrictions strike the right balance between protection against and proliferation of cyber weapons.

[30] Source: European Commission (2015) and IDC EMEA (2009).
[31] More recent data on market shares were not yet available at the time of this publication. The European Commission is currently working on a market study on the cyber security sector, which will be published in the course of 2016. (link)
[32] IDC EMEA (2009).
[33] PAC (2013).

A possible barrier to positive market results is that of government failure. The government, with a share of around 30%, is one of the largest users of cyber security services. It, for example, purchases knowledge for defence and intelligence services, and for the security of government data and government communications. A number of very innovative European companies still are largely dependent on government demand. Because of its key position, it is crucial that the government makes such purchases in a responsible and secure way.

Government authorities, both foreign and domestic, in their role of purchasers sometimes fall short of the mark on the cyber security market.[34] For example, because smaller providers appear to be limited in their opportunities to participate in public tenders.[35] This seems to be the case, not only with regard to cyber security for defence and intelligence services, but also in education and local government.

The government could act more professionally in their role of client; for example, by becoming better informed about the technological possibilities and impossibilities of ICT and its security aspects.[36] When awarding assignments, the government appears to place the emphasis on price and desired application possibilities, at the expense of quality.[37] Moreover, following the initial tendering processes, government bodies may also be locked in to a specific provider in a contract that cannot be terminated before its end date, even if new, better products enter the market.

External effects are another bottleneck for the market. If organisations are insufficiently secure, this may have a negative impact on others. For example, a server that – without its owner knowing – is part of a botnet may be used in a DDoS attack.[38] External effects occur when possible negative impacts on others are not included in cyber security investment decisions.

These effects are generally believed to lead to underinvestment in cyber security.[39] Consumers would for example spend more money on antivirus software if they would also weigh in the adverse effects of botnets on others.[40] However, external effects may also lead to overinvestment. If threats are able to jump from one party to another (irrespective of whether this be a fire from an adjacent building, a flu virus or a computer virus), the low security levels of one party may be reason for another to choose a rather high level of security.[41] A sizeable investment that creates only a small barrier against criminals may be of great benefit to an individual person, while

[34] For a description of the Dutch case, see for example the report by the temporary ICT committee (Tijdelijke Commissie ICT (2015)). OFT (2014) names the shortcomings of the UK Government with respect to ICT.
[35] See PAC (2013) and OFT (2014). The UK Government is believed to lack sufficient commercial and technological knowledge, and to set requirements in contracting that are too high for tendering companies.
[36] Tijdelijke Commissie ICT (2015).
[37] Tijdelijke Commissie ICT (2015).
[38] See Chapter 4.
[39] Anderson and Moore (2006).
[40] Shapiro and Varian (1998).
[41] Acemoglu et al. (2013).

the benefits to society are only limited. This may lead to a security race with negligible effects on aggregate cyber security. It is therefore uncertain if too much or too little is being invested in cyber security, from a societal perspective.

A final bottleneck for the market is that of asymmetric information. Many buyers of cyber security services and products often have no insight into cyber security threats, the consequences of actual manifestations, or into the for them most suitable solution.[42] This is not only a problem at the government, but also in the retail segment. If customers are unable to assess the quality of a particular product, and if performance agreements are difficult to make with product providers, customers tend to either focus on price or decide against purchasing any security product at all.

Because of their limited insight into the quality and necessity of cyber security solutions, consumers and SMEs increasingly opt for free software or for products that are offered in conjunction with laptops, tablets or smartphones. For example, only 21% of small companies (10 to 20 employees) have an ICT security policy, whereas for very large enterprises (more than 500 employees) this is 75%.[43]

Consequences for the cyber security of the economy

Imperfections on the cyber security market lead to a suboptimal security level. If the government has insufficient eye for cyber-related risks, this may disrupt public services and cause digital data to be misused or stolen. Asymmetric information means that often consumers and SMEs are insufficiently protected against cybercrime and, therefore, susceptible to direct hacks and ransomware, among other things.

Policy options

The government, being one of the main parties on the demand side of the cyber security market, could make more use of procurement processes via Small Business Innovation Research (SBIR).[44] This is a form of procurement that suits innovative projects, where the procurer has insight particularly into the objective of the project, rather than into the type of solution. SBIR challenges the market to develop various possible solutions to a certain problem, instead of aiming for the cheapest possible solution to meet the procurer's demands on functionality.

A second option could be to certify cyber security providers. A Dutch or European certification would reduce the uncertainty felt by commercial users and, thus, enhance the reputation of small and medium-sized providers. This would give them more opportunities for international expansion. The risks related to such certification would be the fact that they create an additional barrier for new providers or that they lead to a false sense of security – for example, due to the creation of a 'check list' culture.

[42] PAC (2013) and OFT (2014).
[43] Source: CBS.
[44] See CPB (2016).

2.3 Software vulnerabilities

Introduction

On 7 April 2014, cyber security experts sounded the alarm after the discovery of a programming error (i.e. bug) in the open-source software library, OpenSSL.[45] This bug has since become known as 'Heartbleed'. OpenSSL is commonly used by a large number of webshops, websites and internet routers; therefore, Heartbleed meant that over half a million websites could have been hacked, providing access to credit card information and passwords. All around the world, internet users were urged to change their passwords.[46]

Cyber criminals often make use of software vulnerabilities and bugs. Mistakes by software programmers lead to weak spots in the software, and ignorance or the costs of correcting them cause unnecessary prolonged exposure to cyber attacks.

How unsecure is software?

Software vulnerabilities are quite common. As early as in 2015, 147 vulnerabilities were discovered in the Windows 7 operating system, which at the time was used on over half of all desktop computers around the world.[47] [48] Of those 147, 49 were deemed 'critical', which meant that, due to those vulnerabilities, hackers could install malicious software (malware) on PCs without the knowledge of the owners.

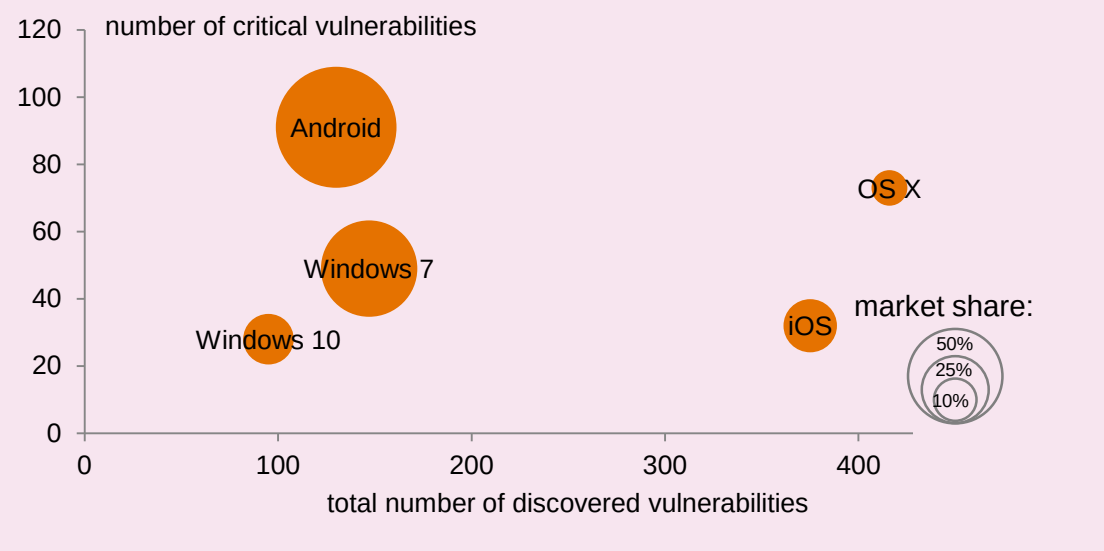
There are differences between the four main operating systems for PCs, tablets and smartphones regarding the total number of software bugs discovered, but the number of critical vulnerabilities differs less strongly – see Figure 2.4. Over the last years, more vulnerabilities were discovered for the Apple (OS X) operating system, but the number of critical vulnerabilities was comparable with those of Android and Windows 7.

The incentive to look for and misuse software vulnerabilities can be related to the market share in two ways. First, the amount of effort and time spent by both hackers and security experts to detect any vulnerabilities increases with the number of users of a particular software package. This may lead to a positive correlation between market share and the number of software vulnerabilities. Second, more secure software is more attractive to consumers, which causes the market share of software with few vulnerabilities to become larger than that of less secure software.

[45] Bruce Schneier, a renowned cryptography expert, described the problem as: 'Catastrophic is the right word; on the scale of 1 to 10, this is an 11'. (link)
[46] For example, see this BBC news report.
[47] Source: www.netmarketshare.com.
[48] Source: www.cvedetails.com.

Publishing vulnerabilities increasingly coincides with the availability of their solution (patch). In 2009, a patch became available for half of all vulnerabilities on the same day they were identified; in 2014 this number increased to over 80%.[49]

Figure 2.4 Software vulnerabilities in operating systems (2015)



Source software vulnerabilities: www.cvedetails.com; market shares: www.statistica.com.
Note: the size of the circle represents the average market share (worldwide) of the operating system in 2015. For Android and iOS, the market shares for operating systems of smartphones were used.

Consequences for cyber security and the economy

Software vulnerabilities render users vulnerable to various manifestations and/or threats of cybercrime, such as ransomware (Section 3.1) and data theft (Section 3.3), limit the reliability of encryption (Section 2.4) and may be used to amplify DDoS attacks (Chapter 4). Software bugs also reduce the reliability and user-friendliness of ICT applications – an operating system that regularly crashes is awkward to work with on a desktop, but may be disastrous in a self-driving vehicle.

Direct economic costs of software vulnerability concern, for example, those related to repair; if users on a global scale need to change their passwords, this requires time that they could otherwise have spent more productively.

Open-source and closed-source software

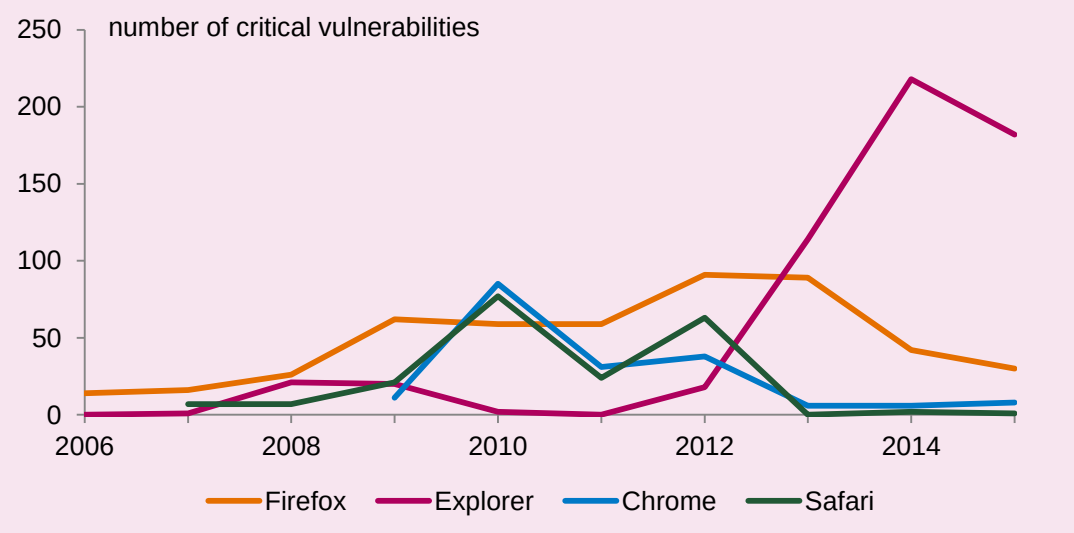
A regularly recurring discussion is one about the question of whether open-source software is more secure than closed-source software. Open-source software basically is software for which the users have free access to its source code, are allowed to alter the software, and can distribute it – either free of charge or at a fee. Examples of open-source(-like) software are Android, Linux, Firefox and Python. Users have no access to the source code of closed-source software, such as Apple's iOS and Microsoft's Windows.

[49] Source: Secunia (2015).

An advantage of open-source over closed-source software is that many more people are allowed to look at and alter the code, which means bugs are discovered and repaired much sooner. In addition, open-source software users are able to develop modules or versions themselves, whereas in closed-source software users are not able to check the source code for vulnerabilities, nor can they repair bugs themselves. On the other hand, the disadvantage of open-source software may be that it is unclear who is responsible for the development of patches to solve any software vulnerabilities, and the variety of versions may also require various patches to solve the same vulnerability problem.

Ultimately, whether open-source software is less or more secure than closed-source software is an empirical question. Here, a complicating factor is that it is partly arbitrary which software packages can be compared. To provide an indication, Figure 2.5 shows the number of critical vulnerabilities discovered, over time, for the four most popular internet browsers. For this figure, comparable programs with comparable functionalities were chosen. The only fully open-source browser is Mozilla Firefox. Chrome was developed by Google and uses open-source software. The other two browsers are by Apple and Microsoft and are closed-source. The figure does not reveal any systemic differences between the open-source(-like) and closed-source browsers.

Figure 2.5 Trend in critical vulnerabilities of internet browsers (2006–2015)



Source: cvedetails.com.

The economy of software bugs

Why is it that bug-free programming is proving to be so difficult? There are various explanations that are related to the economic incentives and technological possibilities for software providers to invest in the quality of their software.

Reducing programming bugs comes at the expense of other objectives, such as the pace of product development, the level of user-friendliness for end users, and affordability. Completely bug-free software, therefore, is neither technologically feasible, nor is it socially desirable.

The interesting subsequent question is that of whether the current system ensures an optimal investment level in software quality. In theory, software providers and end users could enter into agreements on price and quality. However, the different types of market failure, in practice, do not lead to a quality level that would be optimal from a societal perspective.

The first market failure is that software vulnerabilities lead to external effects. If software contains too many critical vulnerabilities, this affects the users, as they become susceptible to attacks, disruptions and system failure, while there are no direct effects for the providers themselves.

The classic economic example of an external effect is that of environmental pollution: if a factory emits polluting substances, this negatively affects people living in the area. A market solution for this type of problem is to establish property rights (the right to a clean environment, or the right to pollute) and, subsequently, to let parties negotiate them.[50] Within the context of software vulnerabilities, as well as elsewhere, this solution would not be a practical one, because of transaction costs and coordination problems. After all, how could software providers negotiate with each of the thousands or even millions of end users?

A second market failure is that of asymmetric information. Software programmers and developers, often, have more information about the quality of their work than do their immediate bosses. Companies could motivate their programmers to detect software bugs, for example by offering them a financial incentive. A disadvantage of this strategy would be the risk of them deliberately programming such bugs into the software so that they can 'discover' them later.

The information available in the user phase is incomplete; neither users nor providers know how many software vulnerabilities there are, or how critical those would be. It therefore would be difficult to draft an agreement in which price is related to software vulnerabilities. Certain software providers provide a financial incentive to their users (i.e. 'bug bounty programmes') to report bugs in the software, in an effort to reduce the degree of incomplete information. Those incentives vary from hundreds to tens of thousands of US dollars.[51] An advantage of this method is that it encourages users to look for and report bugs, which may improve software

[50] Coase (1960).
[51] For example, see this list of companies that have challenged hackers to find their vulnerabilities.

security. However, a potential disadvantage is that, if companies keep the detected bugs a secret for longer than necessary, this meanwhile leaves users unaware of their exposure to those vulnerabilities.

The final problem is that of coordination failure. The detection of and subsequent solution to vulnerability issues involves multiple actors: software and hardware providers (*original equipment manufacturers*) and users. The complexity of the structure of this chain may slow down the solution process. Users, for example, often have to perform certain tasks, such as change their password, change settings or update to a newer version. Users also sometimes depend on hardware development companies (e.g. Samsung or LG) for timely updates of the software. These and other barriers often leave governments, companies and consumers working with outdated and vulnerable software.

Policy options

Product liability law[52] is a possible solution when markets are unable to solve the problem of external effects.[53] There are roughly three liability models: no supplier (in this case: provider) liability, stringent liability with full financial compensation, and the *negligence rule* according to which providers are only considered liable if they have not taken sufficient precautionary measures. In the first model, there are no incentives for providers to prevent software vulnerabilities; in the second model, there are no incentives for the end users to prevent damage; and the third model encourages both providers and end users to prevent any damage.

Which of the product liability models would be the optimal one depends on various factors; for example, the level of detail in which precautionary measures are described and the degree to which compliance can be objectively monitored and/or determined. Also important is the degree to which both providers and end users are able to take precautionary measures. It is unlikely that only one model would be the optimal one for the entire software market, as software is applied for many different purposes (ranging, for example, from computer games to cars and nuclear power plants). In practice, software providers are legally liable, but this liability is strongly restricted by limitation clauses in the terms of use.[54]

The problem of coordination failure could be addressed more effectively if the parties involved could be stimulated to provide more transparency about the quality of their software products. To this end, the Dutch Government is currently supporting the Dutch Secure Software Foundation (SSF, www.securesoftwarefoundation.org).

[52] See Tjong Tjin Tai et al. (2015) for a discussion on the role and possibilities of product liability law in countering cybercrime in the Netherlands, the United States, Brazil and the Czech Republic.
[53] See Cooter and Ulen (2000) for an introduction to the economy of commercial law. Other generic policy solutions for external effects are criminal law, security regulation and tax incentives.
[54] Tjong Tjin Tai et al. (2015).

2.4 Encryption and authentication

Introduction

In what has become known as the San Bernardino case, the US Federal Bureau of Investigation (FBI) ordered Apple to develop an operating system that would provide access to the iPhone of a certain terrorist perpetrator. Apple refused to comply, because the creation of an unsecure operating system would reduce the security level for all Apple customers.[55] In the end, the FBI rescinded the order when they gained access to that particular smartphone with the use of third-party software.[56]

Information that is encrypted can only be accessed by using the correct access code. Authentication is the process by which someone's identity is confirmed by either a person or a machine. Authentication and encryption are closely connected; the true origin of information can only be determined if its sender has used a unique code to encrypt it.

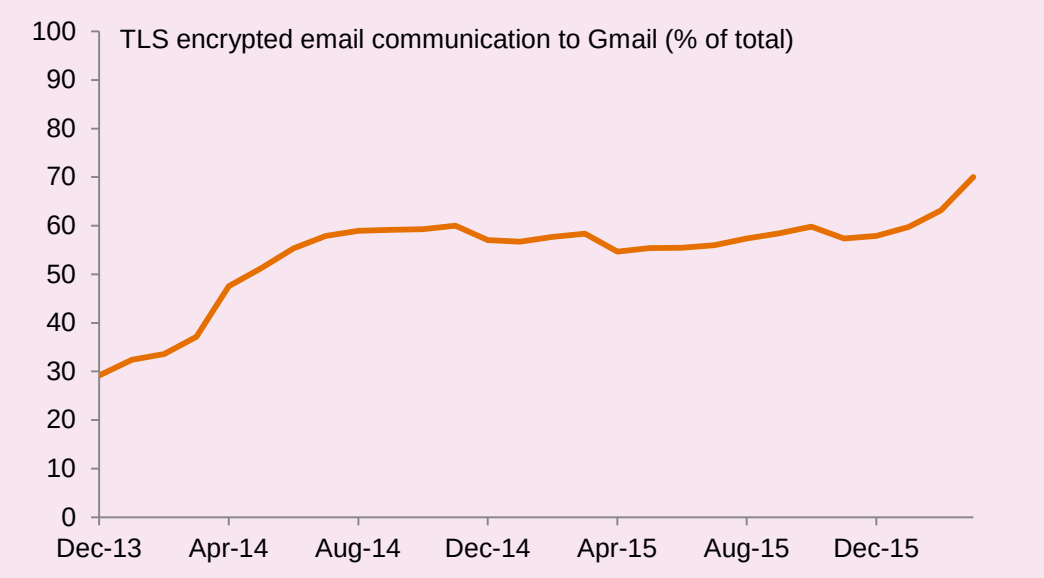
The interests around encrypting information are enormous. Encryption and authentication protect data that is exchanged between and among consumers, businesses and government authorities. Confidence in the secure transmission and receipt of information contributes to the utilisation of all possibilities offered by ICT. In that sense, encryption increases cyber security,[57] although it may also complicate the work of detection services.

Quantitative insights

An example of an often-used encryption protocol is TLS (Transport Layer Security). This protocol secures communications between computer applications, such as email servers and email programs, by encrypting the transmitted data and authenticating the identity of both applications. As emails require both a sending and a receiving party, it is important that TLS (and other security measures) are used by as many email services as possible. However, in many instances, this is not yet the case. Figure 2.6 shows that around 70% of all emails to Gmail addresses[58] use TLS. After an initial rise in the first half of 2014, this percentage has remained stable, to date. For emails with a Dutch domain name, the percentage of TLS-encrypted messages is often higher; for the largest Dutch internet providers it is even close to 100%. NCSC (2015) reports that for '.nl' domain names, TLS often is not optimally configured; only 14% of tested domain names was configured according to the security guidelines of the NCSC.

[55] See the letter by Apple.
[56] According to this article.
[57] Also see the Cabinet standpoint on encryption. (link)
[58] Gmail is a large and globally used email provider. We assumed the number of Gmail emails to be indicative for the total volume of email communication.

Figure 2.6 Share email communication with encryption is stable (worldwide)



Source: Google Transparency Report. (link)

The Netherlands is a frontrunner with respect to the use of DNSSEC, a protocol for checking whether a domain name refers to the correct IP address. NCSC (2015) shows that, in 2015, only 2% of domain names worldwide were using DNSSEC, half of which concerned domain names with the extension '.nl'. This brings the use of DNSSEC within '.nl' to 43%. The percentage among Dutch Government authorities is much lower, with 8%. This was also apparent from a random sample of Dutch municipalities,[59] which showed only 3 in 50 municipalities were applying security standards, such as DNSSEC.

Economic consequences

Encryption and authentication can be applied at various levels and for a wide variety of purposes. They are required, for example, to safely store and transmit personal information and trade secrets. If companies are not able to prevent personal customer information from falling into the hands of criminals, those customers will be less inclined to provide such personal information. It may also be grounds for not purchasing those companies' products.

Furthermore, encryption and authentication also provide protection against infections by malware and phishing. If the origins of software can be determined, it is easier for users to assess whether that software is from a trusted source. The same is true for emails; if the identity of the sender can be determined easily, this makes it simpler to distinguish spam and phishing emails from legitimate messages.

[59] Source: Binnenlands Bestuur. (link).

The importance of reliable authentication is great. This became apparent to the Dutch Government, in 2011, when authorisation certificates by DigiNotar were found to be unsecure. Replacing all certificates was time consuming and, therefore, the government was forced to temporarily continue using the unsecure certificates. The situation could not be fixed immediately; the Dutch Safety Board (Onderzoeksraad voor de Veiligheid) (2012) found that this could have led to 'substantial economic damage and social disruption'. The DigiNotar incident showed the public at large how much the government had become dependent on ICT.

A risk related to existing encryption technologies is that breakthroughs in calculation speeds (e.g. with quantum computing) will create an uneven playing field, with one party being able to break the encryption of others. In the short term, however, a more urgent risk for cyber security is that of the limited use of the existing encryption and authentication techniques.

Supply and demand

Why are existing encryption and authentication techniques so often not being used? In the past, people really had to have the right amount of knowledge in order to use encryption. But, these days, possessing such knowledge is no longer necessary; WhatsApp, for example, changed over to encryption without any effort from the side of its users .

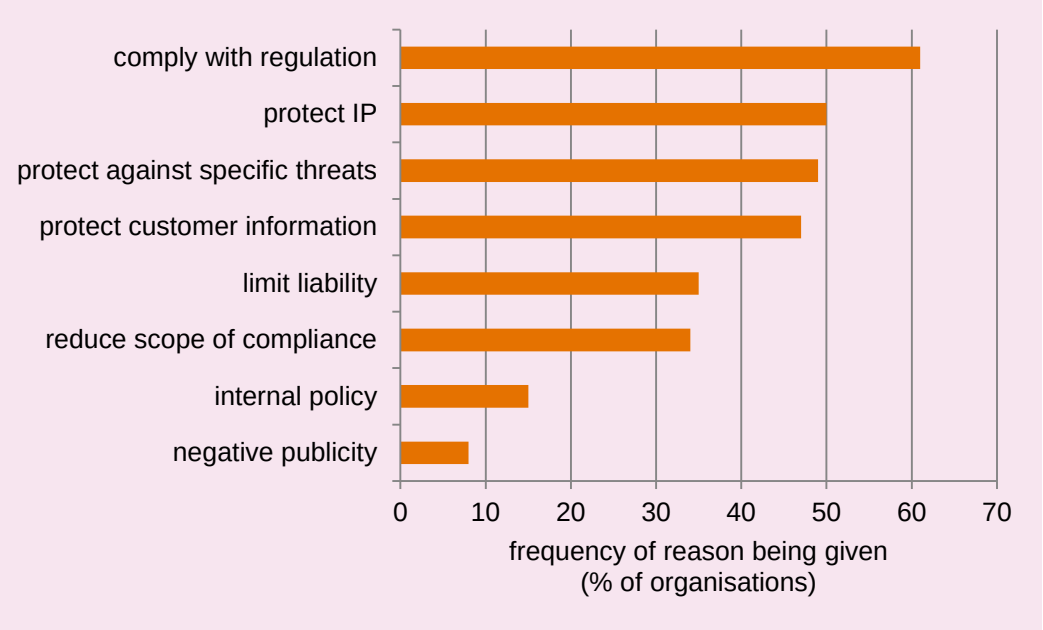
Persuading people, en mass, to use strong authentication technology is much more difficult, as this can only be done at the expense of user-friendliness. For most people, the abstract advantages of better security do not outweigh the concrete bother of having to have a strong password and of applying for log-in codes. Companies such as Apple offer appliances that can be operated with fingerprint identification. This is very user-friendly and is also equivalent to having a very strong password. And in Japan, the government is experimenting with a payment system that uses fingerprints.[60]

Now that using authentication and encryption has become this easy, why is it that so much information is still unsecured? After all, the general application of strong encryption and authentication could greatly reduce issues such as phishing (Section 3.2) and data leaks (Section 3.3). Part of the reason for this is that certain types of encryption are prohibited in a number of countries,[61] because encryption would also prevent governments from intercepting information. Another explanation why encryption is not being used in a number of cases, could have to do with coordination failure. Encryption becomes effective in communication only if a large group of users would adopt the same method. For WhatsApp, it is relatively easy to encrypt all communication within its own network in the same manner. But when individual

[60] See this news message.
[61] See this Wikipedia webpage for an overview.

users within a certain network are able to choose the type of security for themselves, a large number of those users first need to agree on which type of technology to use. Without a dominant user, a network may hold on to old technology. The government could end this type of coordination failure by setting a mandatory standard.

Figure 2.7 Main reasons for using encryption (internationally)



Source: Ponemon 2016 Global Encryption Trends Study. Note: survey among 5000 organisations in 11 countries.

Government regulation appears an important reason for applying encryption. In a survey by Ponemon (2016), companies were asked why they were using encryption. Figure 2.7 shows the most common reasons given. Compliance with regulation was the reason named most often, followed by the protection of intellectual property, protection against specific threats and the protection of client information.

Policy options

The government could minimise coordination failure by becoming 'lead user', by providing a public infrastructure, and/or by encouraging or compelling people to use certain standards. In the Netherlands, a standard online identification system (Idensys) is being developed and provided by the Dutch Government as a public good, and via www.internet.nl the government is encouraging organisations to apply secure standards.[62] Government authorities and semi-public organisations could enhance the appeal of emails as a reliable form of communication by making more use of existing security standards for authentication and encryption themselves, such as

[62] See the Idensys website for more background information (in Dutch).

DNSSEC, TLS, DKIM, SPF and DMARC.[63] The 'comply or explain' rules that apply to these standards could be enforced more diligently.[64]

Private organisations, such as ICT companies and banks, could also offer authentication services. Dutch banks, currently, are working on iDIN (also known as BankID), through which citizens will be able to use existing authentication methods (e.g. Rabo scanner or Digireader) to identify themselves at other institutions.[65]

2.5 ICT dependence of vital sectors

Introduction

On 23 December 2015, hackers succeeded in disrupting the power supply to 230,000 people in the Ukraine, for many hours.[66] The damage to the network took more than two months to repair.[67] Part of the attack was to sabotage the power company's back-up system and to carry out a TDOS attack (i.e. a DDoS attack on telephone numbers); thus, rendering the help desk unreachable. The fact that power grids are vulnerable was already known (Markey and Waxman 2013; NCSC, 2015), but the attack in the Ukraine was the first real-life incident.

The supply of power is one of the vital processes distinguished by the NCSC; other examples are the supply of drinking water, oil, natural gas, telecommunications and basic public information. Disruptions to these key processes may cause substantial damage to both citizens and the business community, within a short period of time.

Economic interests, threats and vulnerabilities

The Dutch National Coordinator for Security and Counterterrorism (NCTV) distinguishes two categories of vital processes, including estimations of the economic consequences of disruptions.[68] Category A includes processes for which disruption could cause more than 50 billion euros in damage. Category B holds processes that would suffer over 5 billion euros in damage. Table 2.3 provides an overview of vital processes per sector. Six fall into Category A. These are the processes around energy distribution, drinking water supply, water management and nuclear energy. No category has yet been determined for processes within the ICT and telecom sector.

[63] SPF (Sender Policy Framework) can be used to indicate which servers are allowed to send emails under a particular domain name; DKIM (DomainKeys Identified Mail Signatures) verifies whether the content of an email message has remained unaltered; and DMARC (Domain-based Message Authentication, Reporting and Conformance) is a standard that indicates how to use SPF and DKIM in a reliable way.
[64] See the Forum Standaardisatie (link).
[65] See this link for more information (in Dutch).
[66] See this article.
[67] Source: ICS-CERT. (link)
[68] See this webpage (in Dutch).

Table 2.3 Vital processes and sectors

Sector	Category	Process
Energy	A	Nationwide electricity transport and distribution
	B	Regional electricity distribution
	A	Natural gas extraction; Nationwide natural gas transport and distribution
	B	Regional natural gas distribution
	A	Oil supply
ICT and	PM	Internet access and data communications
telecommunications	PM	Telephone services (mobile and landline)
	PM	Satellite
	PM	Time and geo-spatial positioning (satellite)
Drinking water	A	Drinking water supply
Water	A	Control and management of large quantities of water
Transport	B	Air traffic control; Aviation (flights and aeroplanes)
	B	Shipping control
Chemicals	B	Large-scale production and processing and/or storage of chemical and petrochemical substances
Nuclear energy	A	Storage, production and processing of nuclear material
Financial communications	B	Retail payments system
	B	Large-scale credit transfers
	B	Interbank payment systems
	B	Securities transactions
Government	B	Communication with and between emergency services via 112 and C2000
	B	Police action
	B	Availability of basic information and data systems

Source: NCTV (link). Category A: more than 50 billion euros in damage, per serious disruption event. Category B: more than 5 billion euros in damage, per serious disruption event. PM: not categorised.

Strict security is obviously important for vital infrastructures. This is the very reason why there are so few incidents in countries such as the Netherlands. Estimations of the economic risks around vital infrastructure, therefore, depend on the approximation by experts.

Table 2.4 provides a summary of the threats/manifestations and vulnerabilities for vital sectors, as estimated by the NCSC, in consultation with the experts.
Spear phishing is a general risk for all vital sectors. In addition, DDoS attacks are also a significant problem for the financial sector, energy sector and national government. Cryptoware (type of ransomware) is also seen, mostly arriving through personal email accounts of staff members.

A type of vulnerability that is identified by experts in both the energy and telecom sector is the emergence of a monoculture, in which all organisations within the sector depend on the same supplier.[69] Problems involving a specific product or service, thus, may affect the entire sector. For the national government and insurance companies, experts point to the vulnerability aspect of those sectors being responsible for the

[69] NCSC (2015, Appendix).

incomes of large groups of people.[70] Securing data files with privacy-sensitive information is identified as a risk for the national government as well as for insurance and health care organisations. Experts in the health care sector indicate that personal information is not always carefully managed. For example, medical specialists manage databases with patient data themselves, and patient data are uploaded via apps from the pharmaceutical industry.

Table 2.4 Threats/manifestations and vulnerabilities of vital sectors

Sector	Threats/manifestations	Vulnerabilities
Drinking water supply	Malware, phishing	Increased use of cloud services
Energy	DDoS, phishing	Monoculture**, remote access equipment
Financial sector	Identity fraud, phishing, DDoS	Availability credit transfer systems
Managed service providers*	Power outages, phishing	Unpublished software vulnerabilities
Nuclear	Malware, phishing	Access control
National government	Cryptoware, DDoS, phishing	Privacy, security of income for citizens, public safety
Telecommunications	Cryptoware, DDoS, phishing, spam	Monoculture**, security of new technologies
Transport	Cryptoware, phishing	Awareness at transport companies
Insurance companies	Cryptoware, DDoS, phishing	Privacy, security of income for citizens
Health care	Cryptoware, phishing	Patient data in third-party databases

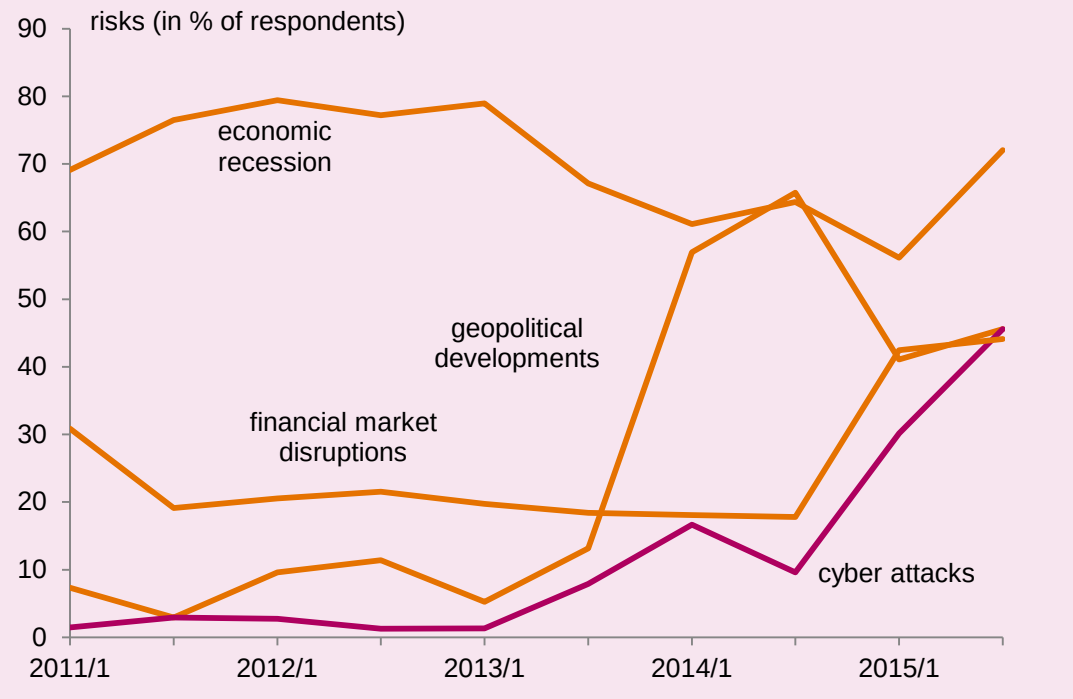
Source: CPB, based on NCSC (2015). *ICT providers who manage operational processes of other organisations, **sector dependent on single supplier

In the financial sector, cyber attacks on payment systems and stocks and bonds systems pose a systemic risk.[71] For example, attacks on Target2 systems could disrupt the financial system. Adequate prevention, detection and response to cyber attacks, therefore, are all important for the financial infrastructure, from a societal perspective.

Financial service providers in the United Kingdom consider the lack of cyber security increasingly as a threat to the stability of the financial sector. This has become apparent from biannual surveys conducted by the Bank of England (2015a) among risk managers at banks, investment companies and insurers.[72] Figure 2.8 shows which developments respondents consider a risk for the UK financial system. A new economic recession is considered the largest risk, followed by cyber attacks, geopolitical developments, and financial market disruptions. Often, these four risks are tied together; financial market disruptions can lead to recession, and geopolitical tensions can lead to cyber attacks.

[70] NCSC (2015, Appendix).
[71] CPB Financial Stability Report 2016, Chapter 2 (in Dutch).
[72] See the publication.

Figure 2.8 The four main risks to the financial system of the United Kingdom



Source: Bank of England, Systemic Risk Survey 2015 H2.

Notably, in 2014, cyber attacks were mentioned by over 10% of respondents, whereas, one year later, nearly half of all respondents considered cyber attacks a risk for the financial system. In its biannual surveys, the Bank of England does not enquire about specific underlying threats, which makes it difficult to explain the increase in perceived cyber threats.[73] Currently (2016), increasing and stress-testing the cyber resistance of financial institutions is high on the agenda of De Nederlandsche Bank (the Dutch central bank).[74]

Advanced financially motivated attacks may become a threat to key processes within the financial sector. An incident in February 2016 made clear that criminals are able to penetrate increasingly further into the critical areas of the financial sector. They hacked the SWIFT[75] client software of the central bank of Bangladesh and transferred 81 million dollar in that way.[76]

Dependence and underinvestment

Within vital sectors, the personal incentive to invest in cyber security may be smaller than the public interest. In other words, there is a positive external effect. This externality, usually, occurs via customers. ISP customers, for example, often are

[73] In its correspondence, the Bank of England has indicated that a number of incidents (e.g. the data leak at ISP TalkTalk) are the basis for the increase in the perceived risk of cyber attacks.
[74] See DNB (2016), Annual Report 2015. (link)
[75] SWIFT (Society for Worldwide Interbank Financial Telecommunication) is the largest provider of communications services to banks and other financial organisations.
[76] Source.

prepared to pay for secure and reliable internet connections, but do so from a personal cost-benefit perspective, only taking into account a disruption's direct effect on themselves.

Large-scale disruptions in vital sectors may have further-reaching consequences than any series of unrelated individual disruptions. There are two reasons for this fact. Firstly, during an individual disruption alternatives are often available. In case of a disruption to hardwired internet access, it is mostly still possible to gain access to the internet via a mobile connection of another provider. The damage of a disruption would be many times greater if there was no other way to access the internet.

Secondly, disruptions to vital sectors are also more serious because they can lead to unexpected effects due to complex interdependence. A local power failure may have consequences for any number of processes in various locations. Such dependence, for example, became apparent from a DDoS attack on a Dutch bank that caused a general disruption to the iDEAL online payment system, and an interruption at a telecom provider suspended the Rotterdam metro service.[77]

Because large-scale disruptions cause more damage than individual ones, the demand for secure and reliable services from the market is smaller than would be desirable, from a societal perspective. This could provide insufficient incentive for companies in vital sectors to invest in cyber security.[78]

Policy options

Secure and reliable service provision costs money. And certainly for companies in vital sectors, their individual customers are not automatically prepared to pay for what society considers the optimal level of security and reliability. Here, there is therefore an obvious role for the government, but exactly what role should that be? Government may contribute to the security in vital sectors, in two ways:

The first is that of integrated supervision. Cyber security is part of the supervision of the sectors. The degree to which sector-specific supervisors currently pay attention to cyber security may vary between sectors. Supervisors should consider stability and security in an integral way, and this also includes cyber security. This is already common practice in the financial sector.

The second is to collect and share information on vulnerabilities and to seek collaboration with businesses. This would help external parties, such as scientists, to point to problems that otherwise perhaps would remain invisible to the supervisor. Sharing information also means that both citizens and businesses would be able to

[77] See the news message (in Dutch).
[78] Section 2.2 provides an overview of the reasons why the market generates insufficient supply and demand for cyber security also from non-vital sectors. These mechanisms are also relevant for vital sectors.

make more informed choices. Public-private collaborations help the government to better serve the public interest.

2.6 Digital divide: asymmetry in security

Introduction

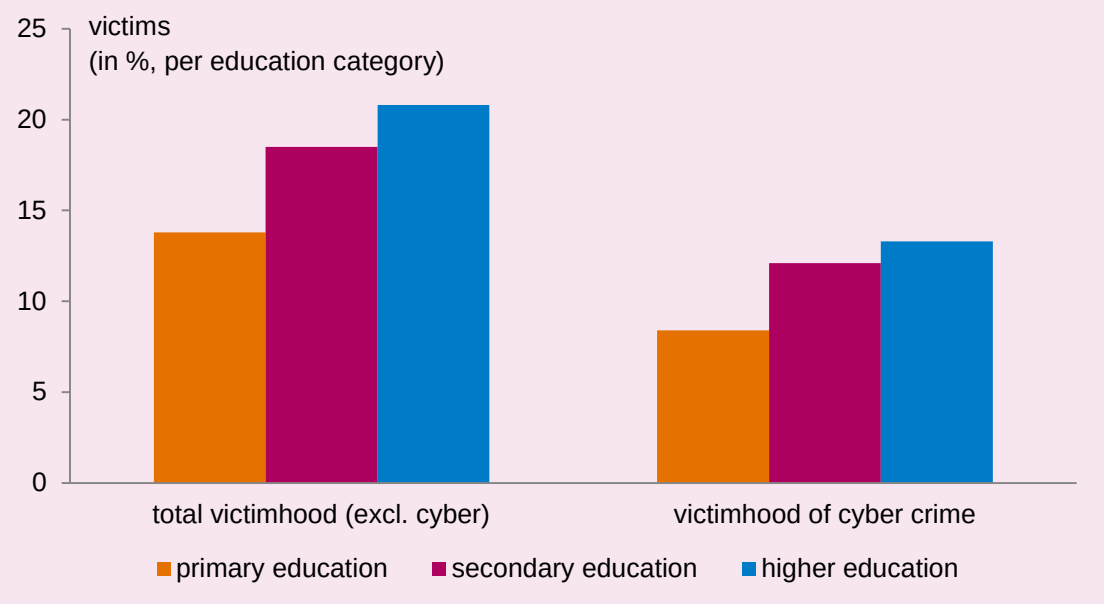
ICT is offering increasingly more possibilities for people who have access to the internet. This may increase the difference in such possibilities between people with and those without access to the internet; thus, resulting in a digital divide. In the Netherlands, nearly all people have access to the internet, but globally this is not the case. In 2015, 35% of the population in developing countries had such access (ITU 2016)[79]. In developed countries, this was 82%. Internet access is increasing, in both developed and developing countries, but so are the differences in access between the two groups of countries. In 2005, 8% of the population in developing countries had access to the internet, against 51% in developed countries – a difference of 43 percentage points. By 2015, this difference had increased to 47 percentage points.[80]

Cybercrime victimhood in the Netherlands

Lower educated people indicate to be the victim of traditional crimes less often than higher educated people.[81] Figure 2.9 shows this also to be the case for cybercrime; 8% of the lower educated become victims of cybercrime, against 13% of those who are higher educated. Possible explanations for this difference could be that people on a lower income are less attractive victims for cyber criminals, and that internet use varies between educational levels.

[79] ITU Key ICT indicators. (link)
[80] Also see the World Development Report (2016) for insights into worldwide ICT access (link)
[81] This section focuses on a possible 'digital divide', in the Netherlands, between educational levels. There are no indications, according to the CBS Veiligheidsmonitor [safety assessment], of any 'digital divide' in relation to age or country of origin.

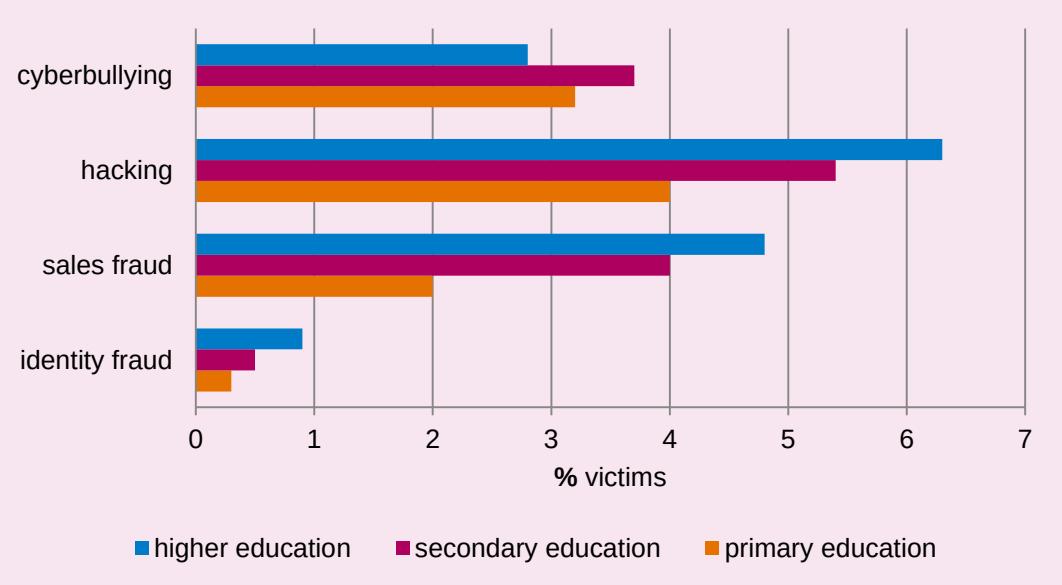
Figure 2.9 Victims of cybercrime, per educational level



Source: CBS Veiligheidsmonitor 2015.

The type of cybercrime differs per education category (Figure 2.10). Hacking is the cybercrime most named for all education categories, followed by sales fraud for secondary and higher educated people, and cyberbullying for those with secondary and primary education. Identity fraud occurs relatively often among higher educated people. These findings are consistent with the hypothesis that the higher educated are considered a more attractive target by criminals.

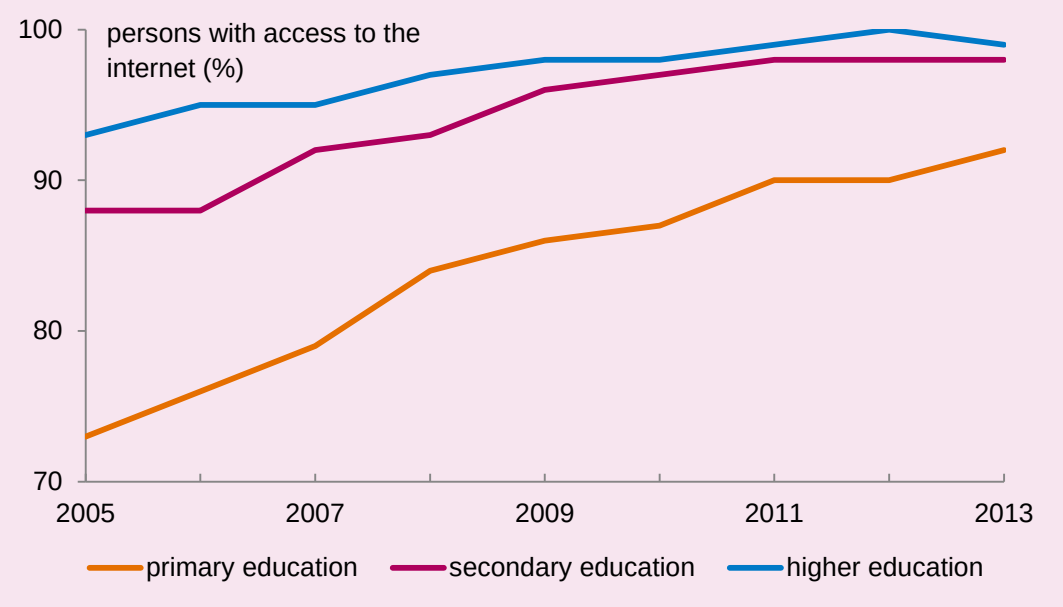
Figure 2.7 Types of cybercrime, per educational level



Source: CBS Veiligheidsmonitor 2015 (Table 4.9.4)

For cyber security, there does not appear to be a 'digital divide', with a relatively more vulnerable group feeling less cyber secure than others, but there is a small group of lower educated people who seem to lag behind, with respect to ICT use. Figure 2. shows the developments in internet access per education category, for the 2005–2013 period.[82] The share of lower educated with internet access has increased substantially, but they still lag behind secondary and higher educated people.

Figure 2.8 Internet access, per educational level



Source: CBS Statline (ICT use, according to personal characteristics).

Economic consequences of asymmetry

In the Netherlands, there are no large groups of people without access to the internet. Those with a lower education usually also have such access, as well as the basic skills needed to use the internet. CBS statistics on victimhood show that lower educated people are in fact less often a victim of cybercrime than those with secondary or higher education. For the Netherlands, a social divide whereby the more vulnerable are lagging behind the rest of Dutch society, therefore, is unlikely.

Policy options

The openness of the internet and the free access to all types of software offer many possibilities, but also mean that government can offer only limited protection against cybercrime. The government, therefore, implicitly or explicitly weighs the possibilities of ICT against its security. The optimal balance between those two is not always the same for every Dutch citizen, and not everyone is equally able to weigh the benefits against the risks.[83] Government, at least for the average consumer, may

[82] Developments in access to a personal computer and to the internet itself are comparable.
[83] An example of a government policy that offers a high level of legal protection is that on the collection, storage and use of personal data. Without protection against cybercrime, the value of the privacy regulation would be limited.

therefore consider setting a minimum liability standard for providers of digital services, or guarantee a minimum level of security.

3 Threats and manifestations

3.1 Ransomware

Introduction

Ransomware is one of the most notable forms of cybercrime of the last years.[84] The NCSC describes ransomware as the 'greatest cyber criminal business model'. This type of malware blocks the access to a computer and, in the case of cryptoware, uses encryption technology to encode it. Then, the hackers demand a ransom for decrypting it again. In contrast to the more traditional ransom methods, ransomware is easy to expand on; it can be scaled up. Cyber criminals only need to invest once in an effective application and, subsequently, release it at very low costs to a large number of potential victims.

Profits and frequency of ransomware

Ransomware is able to infect large numbers of computers and, thus, to inflict considerable financial damage. Table 3.1 gives an overview of six ransomware variants and the number of infections and payments they generated.[85]

Table 3.1 Statistics ransomware cases

Casus	Number of infections	Number of payments	Average payment (euros)	Daily profit (euros)	Total profit (euros)	Share of people who pay
Symantec: Reveton	500,000	15,000	100	83,333	1,500,000	3.0%
Symantec: RansomLock	68,000	1,972	152	7,317	300,000	2.9%
Kafeine: Reveton	25,120	825	85	35,000	70,000	3.3%
Dell/Spagnuolo: Cryptolocker	200,000	771	359	2,770	277,000	0.4%
TorrentLocker	4,180	653	394	7,354	257,393	15.6%
Coinvault	2,081	31				1.5%

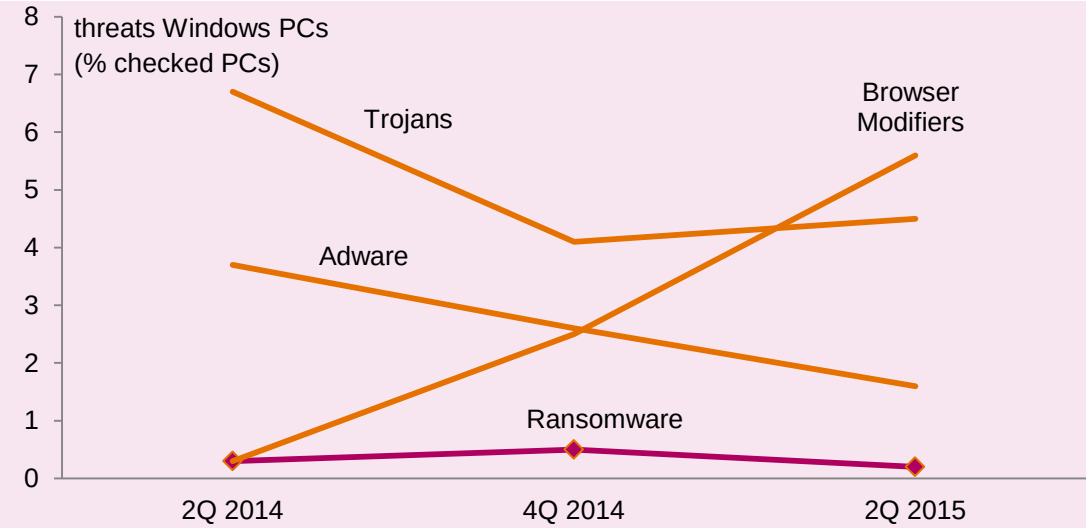
Source: NCSC (2014, 2015), Fox-IT and CPB calculations. Note: the nationalities of victims are unknown.

The numbers of infections vary strongly, from 2,000 to 500,000. Also notable is the substantial number of victims who are unwilling to pay a few hundred euros in

[84] See NCSC (2014) for a general discussion on ransomware and cryptoware.
[85] For these six variants, the financial profits are publicly known. There are many more ransomware manifestations, for example see Symantec (2016), p. 56 for an overview.

ransom, which causes actual profits to be much lower than the potential profits based on the number of infections.

Figure 3.1 Ransomware relatively rare on a global level



Source: Microsoft Security Intelligence Report, editions 17, 18 and 19.

On the basis of the limited number of available sources, ransomware does not yet appear to occur as frequently as other malware (malicious software). Figure 3.1 provides an overview of some of the computer threats for which Microsoft checks PCs, on a global level. In the Netherlands, in 2015, 0.3% of PCs with a Windows operating system were supposedly threatened by ransomware.[86] This is lower than the threat level of, for example, 'browser modifiers', although the impact of a ransomware infection generally is much more serious. A recent survey has shown that, in the last five years, over 1% of internet users in the Netherlands fell victim to extortion.[87] [88] Other investigated forms of cybercrime (identity theft and fraud) were much more widespread.

In the Netherlands, between April 2014 and April 2015, 87 criminal complaints of ransomware infections were filed.[89] This number is relatively low, seeing that the ransomware Coinvault[90] alone was responsible for infecting over a thousand PCs nationwide during that period. The low number of criminal complaints of ransomware is consistent with the equally low numbers of complaints of other forms of cybercrime (Section 2.1). In addition, the chances of being caught are also low, because cyber criminals are using masking techniques. As far as we were able to

[86] Microsoft Security Intelligence Report. (link)
[87] In the survey, this term was explained as: 'Someone extorting money from you to recover access to an account or your computer'. This description is very similar to that of ransomware, which is why the results are indicative of ransomware.
[88] Riek et al. (2016).
[89] Source: NCSC (2015).
[90] Coinvault is a ransomware virus that infected thousands of PCs in 2014/2015. See also Section 2.1.

ascertain from public sources, to date (beginning of 2016) no court cases that centre around ransomware have been decided.[91]

Computer users can reduce the impact of ransomware by making regular back-ups of their most important files. More and more people are doing so; in 2010, only 30% of internet users were making regular back-ups, whereas by 2015 this had increased to 61%.[92]

Economic impact of ransomware

Ransomware has various disrupting effects on the economy. Ransom payments are a socially undesirable redistribution of funds, from victims to perpetrators. As far as known, payments generally come to a few hundred euros per incident. Non-payment also causes damage, as victims are temporarily or even permanently barred from accessing valuable data. As most victims appear to refuse to pay, the main cost to them is time rather than money. Victims will try to remove the ransomware without having to pay. In the survey by Riek et al. (2016), victims of extortion indicated that they had spent an average of 8 hours in their attempt to do so. The threat of ransomware also leads to people taking precautionary measures, such as that of making regular back-ups. Whether the costs of these measures are socially undesirable is unclear, as making back-ups also prevents data loss in case of a computer crash.

In some cases, ransomware infections may threaten the access to and functioning of services. In February 2016, for example, the computer systems of a US hospital were hacked, blocking the access to patient information.[93] In that case, the hospital management opted to pay a ransom of 17,000 dollar.

In the longer term, ransomware negatively affects the general confidence in internet services. If emails and websites that look harmless in fact contain ransomware, this will make internet users more careful and may even cause them to decide against using certain digital services.

The economy of ransomware

Ransomware is different from a physical hostage situation. Compared to people being held hostage, ransomware is much easier to scale up and is far more anonymous. The fact that it can be conducted on a much larger scale means that it is much easier for ransomware to make large numbers of victims, while the anonymity of the data hijackers lowers their chances of being caught. One of the similarities between the physical and the digital crime is that the victims of ransomware mostly have to carry

[91] Source: www.rechtspraak.nl.
[92] Source: CBS (2010), (link) and CBS (2016), 'ict, kennis en economie 2016' [ICT, knowledge and the economy 2016].
[93] See this article.

the costs of the damage themselves. This provides a strong incentive for computer users to take their own precautionary measures.

Ransomware appears a lucrative business, but, to date, it is less widespread that any of the other forms of cybercrime. There are three economic explanations why cyber criminals do not use this method more often. In the first place, the publicised profits from infections are not representative of the profits for most ransomware developers. Designing an effective ransomware campaign costs time and money, and is increasingly complex because of the race against the providers of cyber security services who are working on countering such ransomware. It is, however, possible that there are really successful campaigns that we know nothing about.

In the second place, cyber criminals have a credibility problem. Victims are only likely to pay a ransom if they believe that the hackers will really unlock their device or reverse the encryption and not infect their PC again. The police, therefore, advises against paying in cases of ransomware infection[94] and, as Table 3.1 shows, most victims follow this advice. Normal businesses increase their credibility, for example, by building a reputation or investing in advertising campaigns. These things hardly seem an option for cyber criminals, but it cannot be ruled out that they will not develop a technical solution to this problem, possibly via the use of fixed bitcoin addresses.

The third explanation is that it is difficult for cyber criminals to determine the right price for unlocking the data. Whether victims are prepared to pay the ransom depends also on how important the encrypted data are to them, and whether or not they made a back-up. For example, if all photographs of the first year of a child's life have been encrypted, the victim will be willing to pay much more money for their return than if the files consist of old administrative data. Cyber criminals usually have no idea of what data they are encrypting and, therefore, demand a standard amount of money.

The ransomware developer is in fact a monopolist, because he is the only person with access to the decryption code. Economic theory shows that monopolists could cream off additional profits by price discrimination. Therefore, it would be profitable for cyber criminals to have information on the victims and their level of income when setting the ransom amount. Determining the amount is much easier for directed attacks, such as on hospitals.

Outlook

Ransomware appears to be a financially attractive form of cybercrime. A campaign's total profits can be high and the chances of being caught small due to masking techniques and victims' low willingness to file a criminal complaint. To date, the

[94] See this police explanation.

threat posed by ransomware appears only limited, but this could change if cyber criminals gain access to the content of the personal information they encrypt and are able to define the ransom amount in this way. Ransomware may also become more prevalent if its developers are able to solve the credibility problem.

Policy options

Organisations could counter ransomware by preventing payment to perpetrators, as much as possible. They could do so by stimulating the creation of regular back-ups. This would reduce the need to pay. In some cases, making a back-up is difficult and costly; for example, in the case of utility companies that have to ensure a continuous supply. Another policy option would be to detect the white-washing of illegal ransomware profits.

Ransomware is often distributed through malicious emails and websites – policy options to counter these are described in the following section. Criminals use software vulnerabilities in ransomware infections. Section 2.3 gives suggestions for making software more secure. And, finally, ransomware could be combated by improving the detection and prosecution of cybercrime, see Section 2.1.

3.2 Phishing and malicious websites

Introduction

Phishing is an important threat to the cyber security of many internet providers. In 2015, the Dutch Fraudehelpdesk, for example, registered around 10,000 fake emails per month, and this number has increased substantially in the first months of 2016.

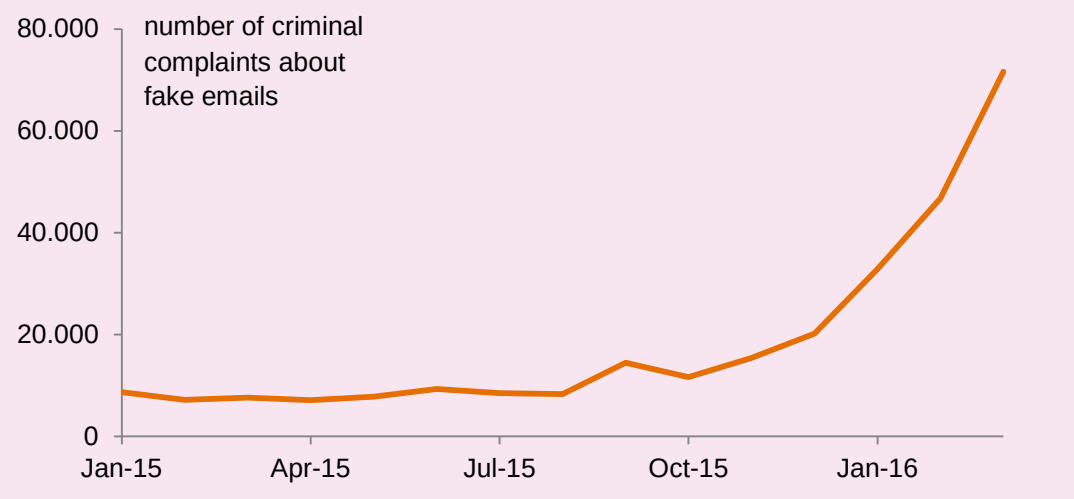
'Phishing email' is the collective term for a variety of fraudulent emails. Senders may, for example, fish for personal data (e.g. PIN numbers or passwords), try to install malware via a link in an email, or to induce payment of phantom invoices. 'Spear phishing' is when cyber criminals send a personalised message to a potential victim.[95] Fake emails sometimes also ask people to visit (malicious) websites. Once on the website, victims are under the impression that they have reached the page of a bank or well-known webshop, and they are subsequently asked to enter some personal data, such as PIN numbers and passwords. These types of malicious websites are called phishing sites. In addition, while victims are visiting the malicious websites, it is also possible that any number of vulnerabilities of their PC system are utilised automatically. These types of websites are so-called malware sites.

[95] An example would be CEO fraud. When an employee receives a message so-called from his highest boss (the CEO), telling him to transfer a large sum of money. In the Netherlands, two companies are believed to have lost around 1.3 million euros in this way. Source: FD. (link)

Magnitude and financial damage

Phishing emails seems to be on the rise. Figure 3.2 shows that the number of phishing emails reported to the Fraudehelpdesk has risen sharply over the first months of 2016.

Figure 3.2 Strong increase in phishing emails in the Netherlands



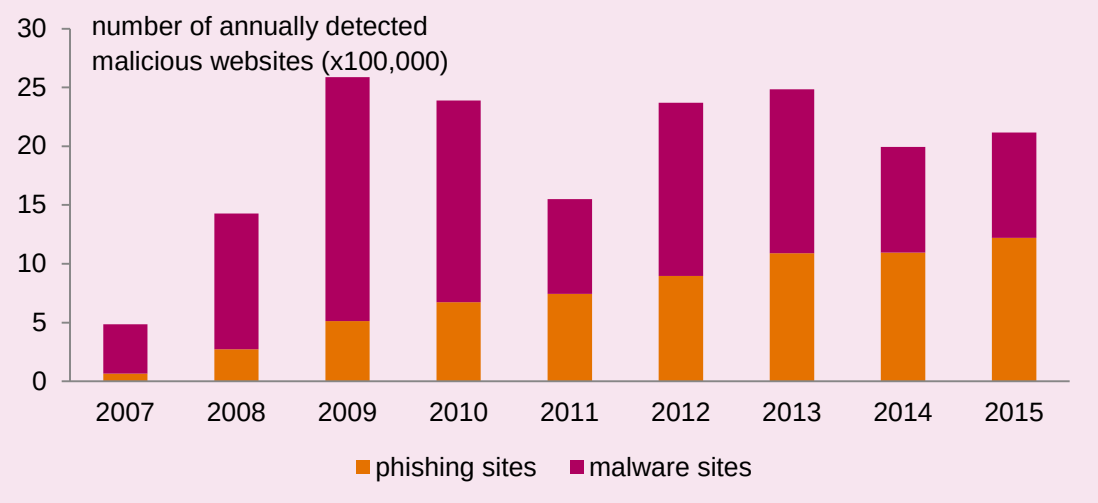
Source: Fraudehelpdesk.

It may very well be that the number of recipients of fake emails is remaining more or less constant, but that victims are informing the Fraudehelpdesk more often. In that case, the rising trend points to an increasing alertness among internet users.

A survey of internet users in the Netherlands has shown that, over the last five years, 2.3% had been the victim of a scam.[96] Such scams are false attempts to persuade someone to transfer money to a fraudulent website. A scam can be seen as the objective of a phishing attempt.

[96] Riek et al. (2016).

Figure 3.3 Increase in globally detected phishing websites

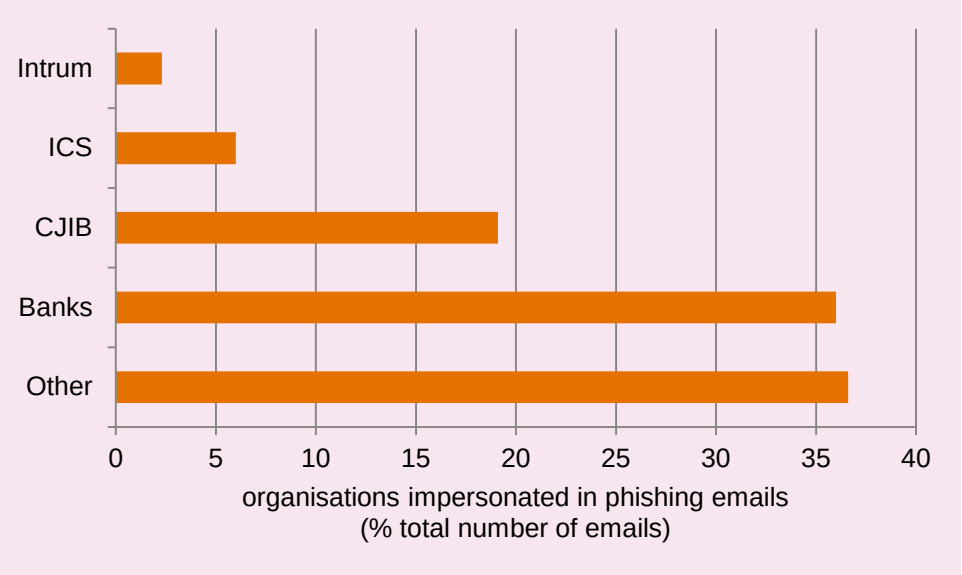


Source: Google Transparency Report. ((link)

There has been a global increase in the threat of phishing websites, see Figure 3.3. In 2008, Google uncovered 5,235 phishing websites per week, whereas in 2015 this number had increased to as much as 23,491 per week – an increase of 349%. The number of malware website has hardly increased; in 2015, Google uncovered 17,190 new such websites per week.

Phishing is a typical form of financially motivated cybercrime. Most attempts are aimed to make money. This is apparent from the types of forged sender addresses. Figure 3.4 shows the organisations under whose name the phishing emails appeared to have been sent; with 36% of phishing emails were impersonating Dutch banks. This is followed by the Centraal Justitieel Incasso Bureau (government debt collection agency), ICS (Visa and MasterCard credit cards) Intrum Justitia (debt collection agency). The fact that a cyber criminal is sending phishing emails under the name of a certain organisation does not automatically mean that the organisation itself is insecure.

Figure 3.4 Mostly impersonation of financial payment organisations



Source: Fraudehelpdesk. Percentages of phishing emails December 2015. Note: 'Banks' represents the total for ABN AMRO, ING and Rabobank.

The total financial damage caused by phishing is unknown, but there are figures that give an impression of the order of magnitude of this damage. For example, internet banking fraud, where phishing is an important mechanism, in 2014, led to 4.7 million euros in damage.[97] The Fraudehelpdesk received 1,303 reports of webshop fraud in 2015, with 977 victims losing a total of 328,000 euros – 335 euros per person. This average amount, individually regarded, is relatively small. Perhaps cyber criminals choose to keep the amount low in order to prevent victims from filing a criminal complaint and themselves – eventually – from being caught. Or potential victims may become more suspicious and less likely to be tricked when the amounts are too high.

Economic consequences

An economic consequence of phishing is that consumers are becoming more careful – and possibly even too careful, if it means they no longer trust legitimate emails and websites. In 2015, 17% of Dutch citizens at one time or another chose not to use internet banking, because of security concerns.[98] Successful phishing attempts often cause financial damage for their victims.[99] The victims also need to spend a considerable amount of time solving the problem and recouping their losses; according to estimations, over 8 hours per incident.[100]

It is becoming increasingly difficult for legitimate entrepreneurs to use digital means in their approach of potential customers; financial institutions and government

[97] Source: NVB.
[98] Source: CBS. (link)
[99] See Riek et al. (2016) for a discussion on the quantitative size. Depending on the method, they arrived at an estimation of between 89 and 353 euros in profit per victim, per scam.
[100] Riek et al. (2016).

authorities, for example, can no longer email their customers and other citizens directly, and they are setting up separate and additional secure email addresses. Apart from the additional costs of this digital infrastructure, it also is more inconvenient for them and the recipients, as they now have to work with multiple email addresses.

Reliable and user-friendly online identification options make it easier for companies and consumers to trust each other, thus enabling an increase in the number of transactions.

The economy of phishing

Phishing and malicious websites take advantage of a number of vulnerabilities. First, there is the limited rationality of people; phishing emails and websites are increasingly very good forgeries and convincingly formulated – recipients then tend to ignore any clues that this may be fraud (i.e. the confirmation bias[101]).

It is not only the lower educated or elderly who become the victim of phishing. In 2015, for example, 0.5% of Dutch citizens with a university education became the victim of phishing, against 0.3% with, at most, a secondary education.[102] The age groups of 35 to 65 and 65 to 75, both had 0.3% in phishing victims. A recent field study showed that also university employees are fooled by phishing; 19% responded to a non-personalised email (addressing them as 'Dear Employee').[103]

Asymmetric information is the second underlying cause of successful phishing attempts. Phishing email recipients do not know how they can verify the identity of the sender or the authenticity of a website. It is, for example, possible to lead visitors of a specific website to a forged version of that website via a malicious DNS server. Furthermore, it is also rather simple for cyber criminals to impersonate the sender of an email message.

A third underlying cause is the public character of the internet. Anyone is able to send any message via email and to visit any website. This is the fundamental strength of the internet, but it is also a vulnerability, as this invites misuse. Cyber criminals can use the internet to send large numbers of messages at low costs.

Policy options

There are various measures that can be taken to increase resilience to phishing emails and malicious websites. For example, the awareness and behaviour of internet users can be addressed. This is being done in the Netherlands, for instance, by the Dutch Payments Association (in their campaign 'Hang up, click away, call your bank') and by the government's Fraudehelpdesk and the website on the safe use of internet

[101] Nickerson (1998).
[102] Source: CBS, Veiligheidsmonitor.
[103] See this web message.

(veiliginternetten.nl). In addition, companies and other organisations can test the risk awareness of their staff by sending them fake phishing emails – a type of digital fire drill. The degree to which such awareness campaigns effectively prevent phishing is, however, still unknown.

Large recipients of email (email server management companies and ISPs) are able to filter out phishing emails by using advanced spam filters and by checking email accounts for known phishing emails or malicious senders. Browsers, such as Internet Explorer and Firefox, also check the reliability of websites. ISPs and browser providers can distinguish themselves from others by providing information on the level of security they offer their customers. For this reason, those companies do not broadcast their lists of malicious websites and phishing email senders. When they do, this affects their competitive position.

Although companies are motivated to keep such lists of malicious websites and phishing email senders up to date, from a societal perspective it is inefficient not to publicise that information. The costs of a 'black list', after all, are independent from the number of people who use it; therefore, this information is a 'club good''.[104] This problem could be solved by a generic obligation for ISPs and other companies to report phishing emails and malicious websites to an independent organisation – provided that those companies retain sufficient incentive to go on collecting this information. On an international level, this may not be feasible, but nationally ISPs are already collaborating via the Abuse Information Exchange foundation[105].

Bona fide email senders have the ability to increase resilience. By using personal information that is only known to the legitimate sender and recipient, such as the name or customer number of the recipient, legitimate senders are making it more difficult for non-legitimate senders to impersonate them. Furthermore, ISPs, semi-public organisations and companies could increase their use of existing authentication techniques, such as DMARC, DKIM and SPF (also see Section 2.4).

3.3 Data leaks

A wide variety of personal and professional data on billions of people is being digitally stored, adapted and used. This yields large economic benefits, but also poses risks. As soon as data are saved, they can be wiped, manipulated, viewed, copied or made public, unintentionally or without the authorisation of the owner. All these cases are called data leaks (or data breaches).

[104] Economists speak of a club good if the marginal production costs are negligible and the owner is able to determine who could use the particular product.
[105] See the website of the Abuse Information Exchange.

Data leaks are so common that only very large or controversial incidents are discussed in the media. Examples of remarkable data leaks are the Panama Papers in 2016 (2.6 terabytes in fiscal data), Ashley Madison in 2015 (37 million users of this adultery website) and Home Depot in 2014 (data on 56 million credit cards).

Numbers and types of data leaks

There is much uncertainty about the total number of data leaks, because, among other things, organisations are not always obligated to report a data leak to the supervisory body. In the Netherlands this is the Dutch Data Protection Authority (DPA). However, even when reporting the leaks is mandatory, organisations may still decide not to do so; for example, because the expected damage to their reputation would be greater than the possible fine of not reporting it. Furthermore, companies and institutions may also not be aware of any data leaks from their organisation.

Table 3.2 Estimation of numbers and types of data leaks

Source	Reach	Number of data leaks in 2015	Number of files in 2015	Percentage unintended	Percentage government
Symantec	Global	305	492 million	22%	5.6%
Privacy Rights Clearinghouse	United States	157	114 million	24%	11%
Risk Based Security	Global	3,930	736 million	7%	12.2%
Gemalto	Global	1,673	708 million	24%	43%
Verizon	82 countries	2,260			8.5%

Note: 'Percentage unintended' is the share of accidental data leaks caused by organisations themselves.

Given these uncertainties, it is not surprising that estimations of the number of data leaks vary widely. Table 3.2 provides an overview of estimations from five different sources. The lower and upper bounds deviate by more than a factor of ten. The reasons for the differences between these estimations is unclear, because the reports provide little insight into the research methods used. There also appears to be no consensus on the main causes of the data leaks or on which sectors are affected the most. Credit card data are very appealing to cyber criminals; for example, 100% of all data leaks in the hotel business is related to credit card data.[106] Credit card numbers with the related security codes, names and expiration dates are used in so-called card-not-present (CNP) fraud.[107] Data leaks are the main cause of CNP fraud.[108]

Within Europe, CNP fraud is the main form of credit transfer fraud. The European Central Bank estimated that, in 2013, around 1.4 billion euros in fraudulent transactions took place, 60% of which via CNP fraud.[109] For years, the relative value of fraudulent transactions compared to the total has been fluctuating around 0.04%.

[106] Symantec (2016), p. 50.
[107] Card-not-present fraud is the misuse of credit card information in online transactions.
[108] Europol (2012), p. 10.
[109] ECB (2015). (link to the report)

In the Netherlands, the total damage from credit transfer fraud in 2015 came to 17.9 million euros,[110] representing a fraction of the total in iDEAL payments (18 billion euros in 2015[111]).

Economic consequences

Data leaks and the risk of such leaks have various economic and societal consequences. In the first place, there are the consequences for the organisations responsible for the data management; they must prevent data leaks and repair any vulnerabilities to their system. If data leaks nevertheless occur, they may face liability claims and reputation damage.

On the basis of stock exchange fluctuations after data leaks have been made public, the financial costs can be estimated. Cavusoglu et al. (2004)[112] show that organisations with a stock exchange quotation lose around 2% of their market value within two days of such leaks being publicised. This seems a significant economic effect, but is probable an overestimation of the total effect, because competitors are likely to profit from such a data leak. The market value of the sector as a whole, therefore, will drop only slightly or not at all. Effects on market value may also be only temporary. One of the few studies on consumer responses to data leaks is that by Kwon and Johnson (2015). They revealed that data leaks from hospitals, in the longer term, have a negative impact on the number of out-patient treatments. This effect is stronger in regions containing many hospitals. Whether there is a causal relationship is unclear; hospitals that appear to have their internal procedures in order may very well also deliver good quality health care and thus attract more patients.

The victims most seriously affected by data leaks are usually not the data management organisations but rather those whose data have been leaked. Their privacy has been invaded and they run the risk of becoming the victim of identity theft. The impact on these victims is often personal and difficult to express in monetary terms. The risk of data leaks may cause people to be reluctant to share their data with organisations; particularly, if they do not know how well their data would be protected, and what the organisation's liability position would be in case of a data leak.

Market failure around data leaks

There are two types of market failure around data leaks: asymmetric information and external effects.[113]

The market failure of asymmetric information has two sides. For one, it is not easy for organisations to inform their customers and users of how securely the data is being

[110] Press release, in Dutch, by the Dutch Payments Association (2016). (link)
[111] DNB, Table T5.12.
[112] The current effect of a data leak may differ from the situation of more than a decade ago, at the time the study by Cavusoglu et al. was published.
[113] Also see Van Eeten (2011) for a discussion on the economic aspects of data leaks.

managed, because insight into the security measures would benefit hackers as well as competitors, and be difficult for customers and users to check. Thus, customers hardly know to which degree their data would be protected.

A second reason why asymmetric information is problematic is that of users and customers not automatically knowing that their data have been leaked, nor when or where this happened. And when they actually suffer any damage due to a data leak, it is not always clear from where the leak originated. Moreover, organisations are not exactly motivated to report a data leak incident to their customers or to the supervisory body, because of the perceived risk of reputation damage. For these reasons, there are only few opportunities for companies to improve their reputation with respect to data security. The example of Apple refusing to help the FBI unlock an iPhone is one of those rare occasions.

The second type of market failure, the external effects, is related to the fact that organisations from where the data leaks originate, themselves, usually do not incur any damage from such incidents. Negative external effects occur when two parties share data belonging to a third party. The most important example is that of shared credit card information. If such data are intercepted by hackers, the credit card company suffers the damage, unless one of the parties was negligent and could be held liable. Because of this external effect, organisations and users sometimes feel insufficiently motivated to secure the data.

Sometimes, however, data leaks also have positive external effects. One example is that of intellectual property theft. In the Netherlands, companies are sometimes hacked with the objective of obtaining technological knowledge (AIVD, 2015). If this intellectual property is then used by a competitor, this leads to unintended knowledge spillover. The downside of the theft of intellectual property is that it makes investment in research and development (R&D) less attractive, as the possibility of theft diminishes the expected returns on innovation.

Policy options

There are several policy initiatives to solve the problems around data leaks. The European Commission has formulated a reform of the EU regulation of the protection of personal data. And in the Netherlands, since January 2016, organisations have been obliged to report data leaks to the Dutch Data Protection Authority (DPA). Following such a reported leak, the DPA can start an investigation and, where appropriate, impose a fine. The DPA does not publicise which organisations report data leaks, nor do they say what type of data this concerns. They can, however, order organisations to inform the people whose data were leaked.

A policy option could be to publicise information on data leaks. Advantages of such a policy would be that it would address the problem of asymmetric information on security measures, and that organisations would become strongly motivated to

protect data. A disadvantage of data leaks being made public is that this would increase the barrier to report data leaks to the supervisory body.

As indicated above, companies from which data leaks originate often do not suffer any direct damage themselves, but the damage suffered by third parties may be substantial. This problem could be solved by expanding liability in cases of data leaks. The effectiveness of such liability, in practice, will depend on the possibilities of tracing the source of the data leak.

4 DDoS attacks

4.1 Introduction

In October 2015, the Dutch police arrested five young people accused of performing two DDoS attacks on internet provider Ziggo. The attacks caused 60% of Ziggo's 3.6 million customers to be without internet connection for many hours.[114] Their motive was said to be extortion.[115] Following the attack, Ziggo adjusted the modems of all of its customers, in order to prevent damage from any new attacks. Those customers, incidentally, received no compensation from Ziggo for the disrupted access to the internet.[116] In that same year, the government website rijksoverheid.nl[117] and the websites and apps of Dutch public broadcasting company NPO[118] were also unreachable for many hours due to DDoS attacks.

Distributed Denial of Service (DDoS) attacks cause a certain service (e.g. a website) to become unreachable. DDoS attacks on websites usually overload the servers, flooding them with network traffic, thus causing them to be unreachable (NCSC 2015). These attacks often use a network of infected computers – a so-called botnet – or an amplification technique, in which third party servers are misused without them being hacked (Czyz et al. 2014).[119]

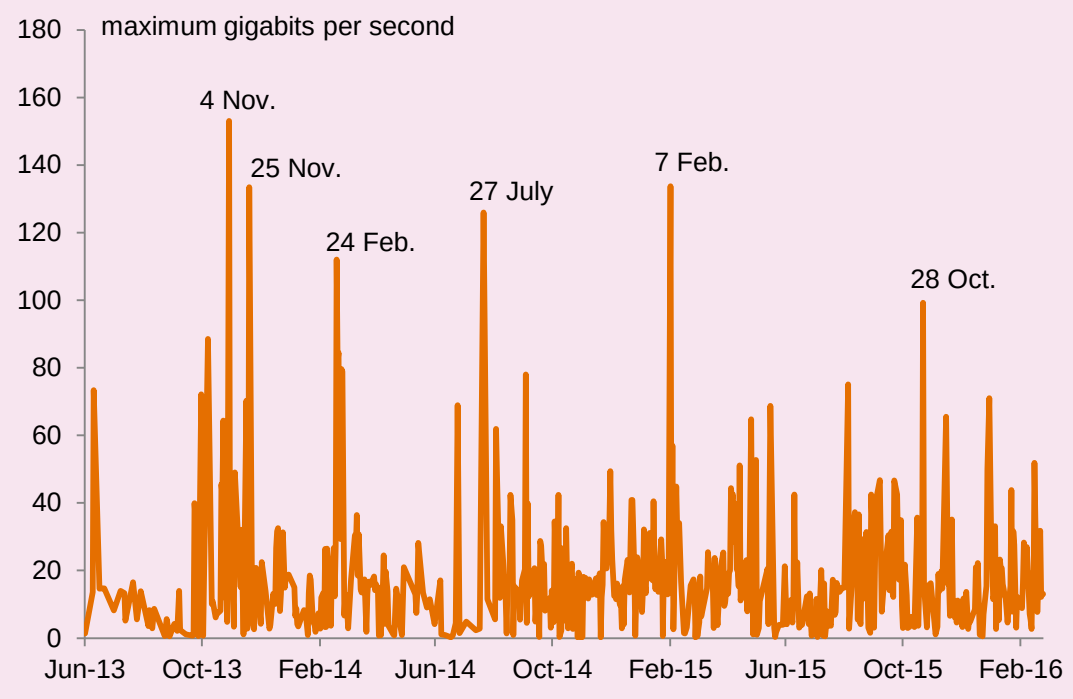
DDoS attacks occur frequently and directly affect many internet users. The consequences of such attacks vary, from being a hindrance due to slow network performance to the disruption of key processes.

[114] See this news message.
[115] See this article in De Stentor.
[116] See this news item by RTL News.
[117] Source: NRC. (link)
[118] See these messages: (link) and (link).
[119] An attack by one computer is known as a denial-of-service (DoS) attack. If multiple computers conduct the attack, this is known as a distributed denial-of-service (DDoS) attack.

4.2 Quantitative insights into DDoS attacks[120]

DDoS attacks strongly differ in intensity (bits per second) and duration, and in the targets they are aimed at. Figure 4.1 shows that, particularly in late 2014 and early 2015, a number of large attacks were carried out on targets in the Netherlands. The magnitude of such attacks in the Netherlands has not increased – the largest attack dates back to November 2013, when web hosting company Flexwebhosting was attacked.[121]

Figure 4.1 Varying peak intensities of DDoS attacks on Dutch targets



Source: Digital Attack Map. Data adapted by CPB.

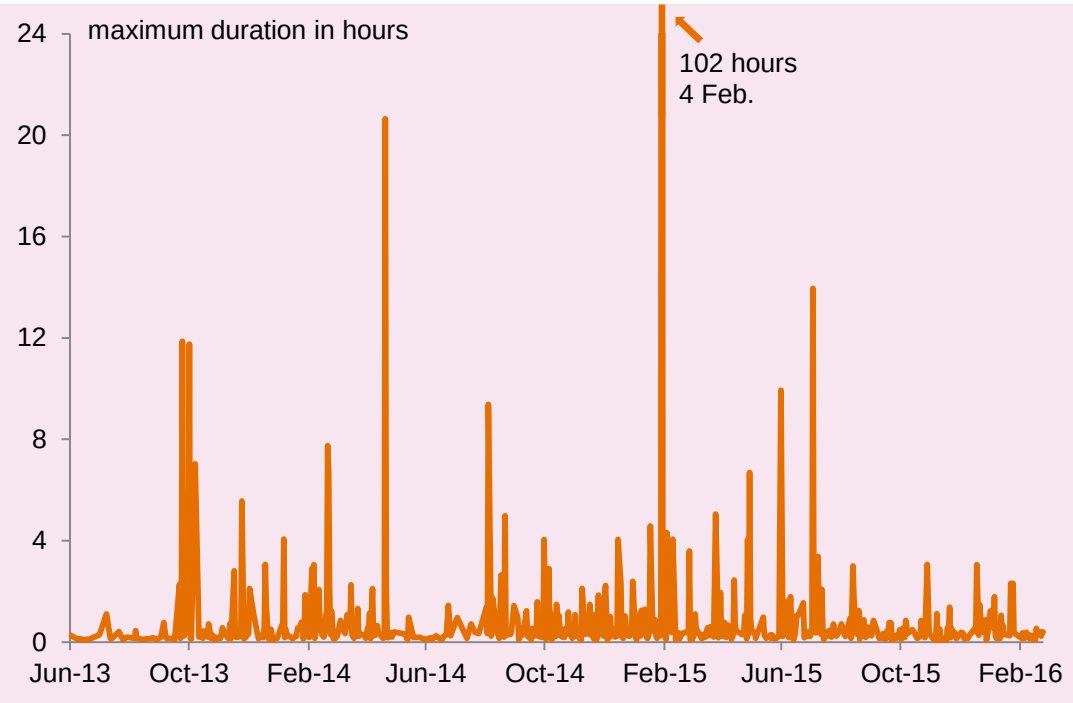
The impact of a DDoS attack is determined not only by the intensity of the attack, but also by its duration. A disruption of a few minutes is less damaging than one that lasts a whole day. The attacks vary strongly in duration, as is clearly shown in Figure 4.2. Most attacks last less than one hour (87%, NCSC 2015), with only a few exceptions.

From an international perspective, most DDoS attacks are aimed at the United States. Between March 2015 and February 2016, close to 13,000 attacks were registered there. Over the same period, the Netherlands had over 1,100 attacks, which put it in 25th place on a global scale. As a source location of DDoS attacks, however, the

[120] Data in this chapter were based on the Digital Attack Map and were adapted by CPB. Not all DDoS attacks are reported to Digital Attack Map, but it is the largest public data source available on this subject. Identification of a DDoS attack can be complex, because a strong increase in internet communication may also be legitimate. Data used here concern the top 2% of DDoS attacks reported to Digital Attack Map.
[121] See this news message.

Netherlands ranked 3rd, with 2,600 registered attacks. Most attacks originated from China (over 8,000).[122] The uncertainties around countries of origin is large; in 2015, the country of origin could not be determined in around 70% of cases.

Figure 4.2 DDoS attacks on Dutch targets usually short-lived



Source: Digital Attack Map. Data adapted by CPB. Based on the top 2% of DDoS attacks reported to Digital Attack Map.

4.3 Economic consequences

The economic consequences of DDoS attacks can be divided into three categories:[123]

1. Costs for potential targets
2. Costs for general internet use
3. Behavioural effects on internet users

The most visible costs are related to the damage caused to the target. Whenever an organisation's website is down, they not only lose turnover but also incur the costs of dealing with the attack. In addition, there are the costs of prevention and those related to the damage to the prospective users of the affected website.

Less visible is the damage caused to other internet users. Hackers infiltrate computers on a large scale in order to form botnets. The rise of the Internet of Things

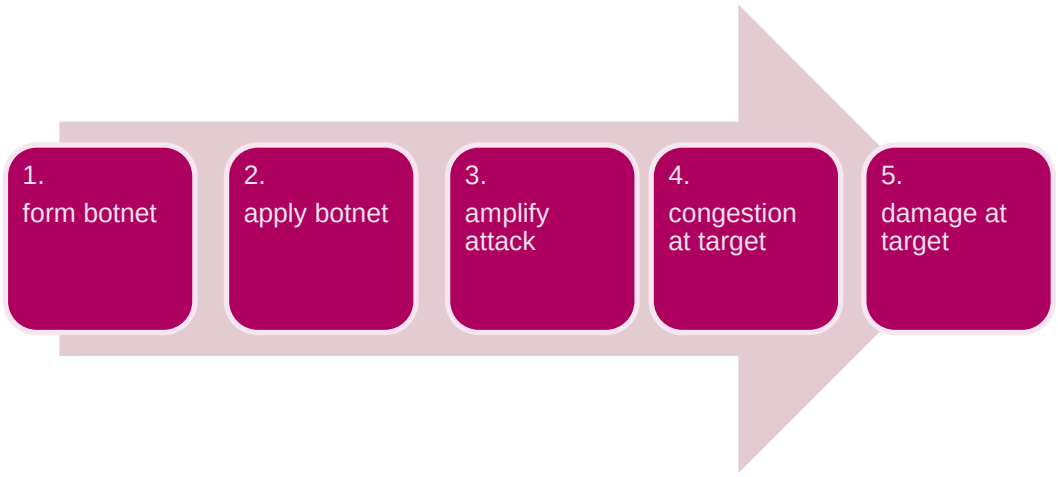
[122] The numbers of attacks sent and received between two countries appear to depend on the number of internet users and average internet performance speed (Overvest and Straathof 2015). In addition, also economic relationships play a role, while cultural differences appear to have no impact on the number of attacks between countries.
[123] Ciere et al. (2015) provides an elaborate description of the types of costs that can be related to cybercrime.

(IoT) will further increase the opportunities for cyber criminals to form and expand botnets. Furthermore, such attacks also use part of the capacity for the usual internet traffic. In particular during very large attacks, this may have noticeable consequences for parts of the internet; for example, the attack on Spamhaus in 2013 also caused problems at the London Internet Exchange (LINX).[124]

4.4 Economic mechanisms

Figure 4.3 shows a – simplification of – the five different phases of a DDoS attack. Attacks start by the formation and application of a botnet, sometimes amplified (e.g. via DNS servers), resulting in congestion and damage on the side of the target. In each phase, the attacker can utilise particular vulnerabilities in order to increase effectiveness of the attack. The government could consider applying specific policy measures for each of those vulnerabilities.

Figure 4.3 Construction of a DDoS attack



Software vulnerabilities play a large role in the formation of a botnet. They enable the installation of malware on a large number of computers. Software vulnerabilities are difficult to prevent or avoid, as users mostly are unaware of the vulnerabilities of the software they are installing. This is a problem of asymmetric information (Section 2.3).

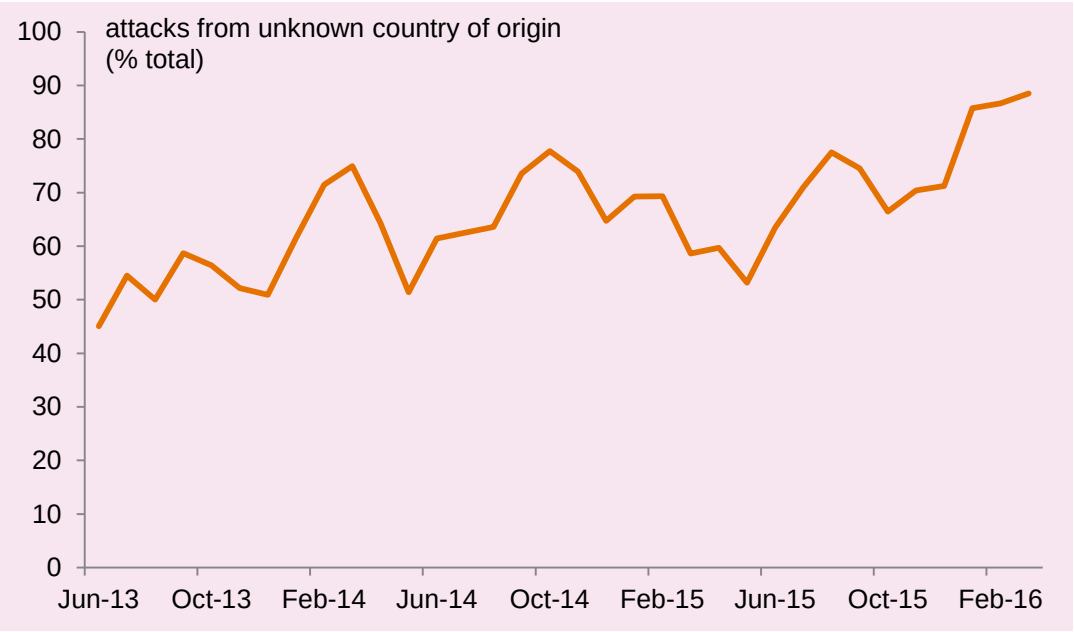
In order to be able to apply a botnet for longer periods of time, it is important to the attackers that the users of infected devices themselves are not hampered by an attack. Thus, they do not become alerted or encouraged to look for malware on their computer, nor to improve their level of security. Modest requests for information from a large number of devices, together, may form a sizeable attack. A successful botnet utilises the external effect that internet users with infected devices have on other users.

[124] Internet communications The internet traffic handled by LINX was halved during the attack. (link)

Certain DDoS attacks use amplification mechanisms (phase 3), which are often used as an alternative to a botnet, such as attacks via a DNS server.[125] Because the DNS server sends multiple amounts of information to the target, the DDoS attack becomes much stronger (Czyz et al. 2014). Attackers also use several techniques ('multi-vector attacks') to circumvent DDoS detection methods.

The amplification of DDoS attacks uses two of the internet's vulnerabilities. In the first place, DNS servers are public – this is essential to their functionality. But the main problem is the ease with which the origins of an information request can be forged; for every information package sent through the internet, senders themselves indicate from which internet address the package is being sent. Displaying a fake identity is what is known as 'spoofing'. This vulnerability caused asymmetric information about the true identity of internet users.

Figure 4.4 Share of DDoS attacks, worldwide, with unknown country of origin



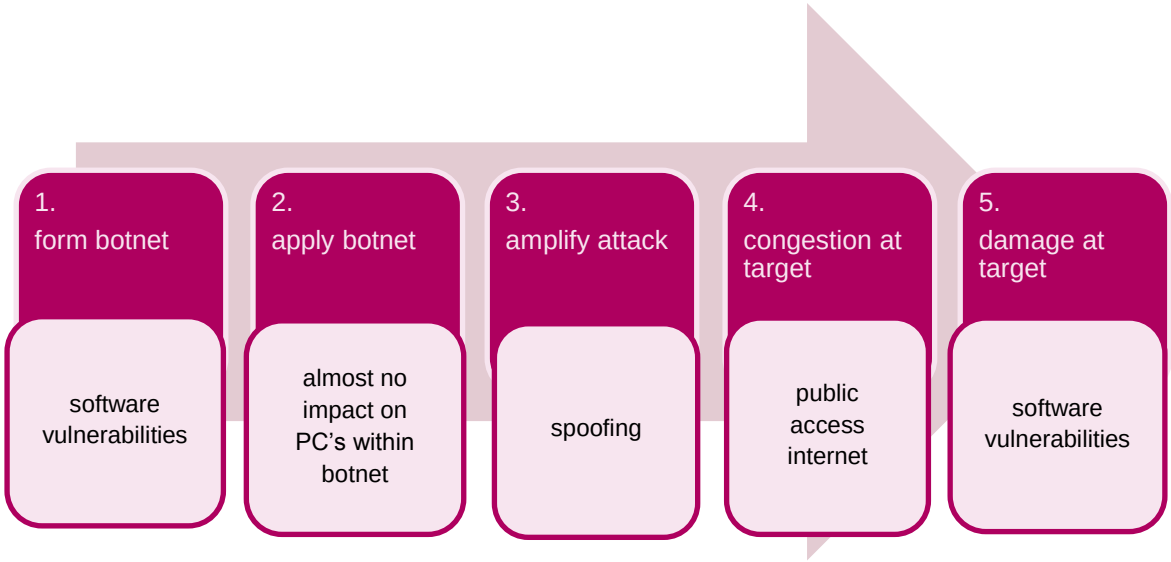
Source: Digital Attack Map. Data adapted by CPB. For 2015, the country of origin of the attacks could not be determined in around 70% of cases. During DDoS attacks, a large amount of data arrives at the IP address of the targets. The organisations that are a potential target of such attacks, and for whom continuity of services is important, can take a number of measures to prevent disruption. They can, for example, ensure that there is temporary or permanent additional capacity available; for instance, via their hosting company or ISP. Organisations with such capabilities of rapid scale up are less attractive targets and, thus, the chances of having to use that additional capacity becomes less likely. Another solution could be to separate legitimate from illegitimate data communication.

[125] Information about a given domain name is requested from the DNS server. The DNS server subsequently sends its answer not to the infected device but to the IP address that the infected computer is falsely indicating as its own.

Spoofing increasingly appears to be a problem in DDoS attacks. Figure 4.4 shows the share of DDoS attacks, worldwide, for which the country of origin could not be determined. In 2013, the country of origin of DDoS attacks could be determined in half of all the cases, whereas in early 2016, the origins of 90% of all attacks remained unknown.

The effect of a DDoS attack depends on the target's software vulnerabilities. Potential targets do not automatically fully protect themselves against DDoS attacks. This is partly due to the fact that vulnerabilities at an organisation cannot easily be spotted by others – until they are attacked. Thus, there is asymmetry in the information between potential targets and other internet users.

Figure 4.5 Vulnerabilities used in DDoS attacks



As a result of this asymmetry, the customers and suppliers of a company cannot fully assess how vulnerable that company would be to DDoS attacks. Customers that value disruption-free communication are unable to distinguish between companies that invest effectively in limiting their vulnerability and those that do not. Investments to reduce such less vulnerability, therefore, cannot be recovered.

Figure 4.5 summarises the vulnerabilities used in DDoS attacks. Lack of clarity on the vulnerabilities of others (asymmetric information about security) plays a role in the formation of botnets and in the damage caused by an attack. Spoofing (asymmetric information about identity) enables misuse of the public access to DNS servers, which can be used to amplify a DDoS attack. The public access to the internet enables internet users to unwittingly approach a particular target (externality), thus creating congestion. And a target may not have invested enough in security because this cannot be seen by others (asymmetric information about security).

4.5 Policy options

How could the government contribute to the prevention of DDoS attacks? This should ideally occur at the source – where botnets are formed via malware. More secure software makes it more difficult for malware to be installed. But because of continual technological developments it is not easy to formulate, let alone enforce, minimum security standards on this subject. In certain cases, the government can set technical requirements. DNS servers are less vulnerable to spoofing, for example, if the BCP38 protocol is used. Because, if these servers are better able to determine the origins of internet communications, amplification attacks could be recognised at an earlier stage.[126] However, without direct obligation or responsibility for countering such amplification, the incentives for ISPs to implement BCP38 are limited.

Government policy could also be directed at potential target of DDoS attacks. For example, it could create transparency about the degree of security at organisations and about how often attacks cause actual disruptions. In that way, customers are more able to estimate how likely such disruptions would be. Disadvantage of this transparency is that it also informs the attackers of which potential targets are less secure. A possible alternative could be for a supervisory body to check organisations behind the scenes, as is already common practice in the financial sector.[127]

The government, furthermore, could award ISPs more responsibility for the prevention and combating of botnets and DDoS attacks.[128] ISPs have the information and the possibilities needed to take appropriate measures. The question here is why ISPs would need to take such measures, in addition to their contractual agreements with their users. The answer is twofold; in the first place, market failure as described above leads to insufficient prevention. And, secondly, internet users differ in their response to a DDoS attack. A coordinated approach to the type of DDoS attacks that are currently offered as a 'service', could be more effective than the heterogeneous solutions applied by the potential targets.[129]

Then there is the question of how those responsibilities should be divided between ISPs. After all, internet communication between users travels via the networks of multiple ISPs. One possibility would be to make ISPs responsible for the protection of their own customers against usual-sized DDoS attacks. They could charge those customers for this service. Customers who need additional protection against exceptionally large DDoS attacks could acquire this themselves, separately.

[126] See this message. (link)
[127] Supervision away from the public eye has its own problems. What is the mandate of a supervisory body to act in cases where organisations are found not to be following instructions? How would a supervisory body, for example, determine which security level would be acceptable? How should a supervisory body act if, after an incident, it appears the incident was partly due to a lack of supervision?
[128] This is the case in Finland, among other countries.
[129] DDoS attacks via the application layer are not as easily addressed by ISPs, because ISPs are not allowed to inspect communications within the application layer.

An alternative possibility could be to make ISPs liable for relaying DDoS traffic to other ISPs. This would have the advantage of attacks being dealt with closer to the source, in turn reducing network congestion. A disadvantage would be that DDoS attacks are difficult to distinguish from ordinary internet communications, because they are sent by very many different IP addresses. If ISPs would be held liable for relaying the DDoS attack traffic, this would also give them an interest in the prevention of vulnerabilities on the side of their customers. Currently, there is little incentive for ISPs to intervene when the devices of their bona fide customers appear to have been infected with malware and may have become part of a botnet.

Dutch ISPs are already actively involved in combating botnets and DDoS attacks. For example, they exchange information on botnets via the Abuse Information Exchange. Furthermore, companies are collaborating in the fight against DDoS attacks, via the Dutch Continuity Board.[130] In the case of extremely large DDoS attacks, this collaboration offers participating parties the possibility to separate the communication between members from all other internet traffic. A possible next step in this collaboration could be to also focus on smaller DDoS attacks.

[130] See The Hague Security Delta for more information. (link)

Literature

Acemoglu, D., A. Malekian and A. Ozdaglar, 2013, Network Security and Contagion, NBER Working Paper 19174.

AIVD, 2015, *Jaarverslag 2015* [annual report 2015].

Anderson, R. and T. Moore, 2006, The economics of information security, *Science*, vol. 314(5799): 610–613.

Ayres, I. and S. Levitt, 1998, Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack, *Quarterly Journal of Economics*, vol. 113(1): 43–77.

Bank of England, 2015, *Systemic Risk Survey Results*.

Becker, G., 1968, Crime and Punishment: An Economic Approach, *Journal of Political Economy*, vol. 76: 169–217.

Bundesministerium für Wirtschaft und Technologie, 2013, *Der IT-Sicherheitsmarkt in Deutschland* [The IT security market in Germany].

Cavusoglu, H., B. Mishra and S. Raghunathan, 2004, The Effect of Internet Security Breach Announcement on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, *International Journal of Electronic Commerce*, vol. 9: 70–104.

Czyz, Jakub, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey and M. Karir, 2014, Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks. In: Proceedings of the 2014 Conference on Internet Measurement Conference. ACM: 435–448.

CBS, 2015, *ICT, kennis en economie* [ICT, knowledge and economy].

CBS, 2015, *Veiligheidsmonitor 2015* [Safety monitor 2015].

CPB, 2016, Risicorapportage financiële markten [CPB Financial Stability Report[, CPB Communication.

CPB, 2016, *Kansrijk innovatiebeleid* [Promising innovation policy], CPB Book 20.

Ciere, M., Gañàn, C. and M. van Eeten, 2015, Report on model development and adequacy of existing models and data, Delft University of Technology.

Coase, R.H., 1960, The Problem of Social Cost, *Journal of Law and Economics*, vol. 3(1).

Cooter, R. and Th. Ulen, 2000, *Law and Economics*, 3rd edition, Addison Wesley Longman.

Cuyper, R. de and G. Weijters, 2016, Cybercrime in cijfers: een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices [Figures on cybercrime; exploration of the possibilities to include cybercrime in the National Security Indices], *WODC Memorandum 2016-01*.

De Nederlandsche Bank, 2015, *Jaarverslag 2015* [annual report 2015].

Dutch Association of Insurers, 2016, Verzekerd van cijfers 2015 [Data on insurance 2015].

Dutch Safety Board, 2012, Het DigiNotarincident: Waarom digitale veiligheid de bestuurstafel te weinig bereikt [The DigiNotar incident; why digital security mostly is not discussed in the boardroom], The Hague.

Eeten, M. van, 2011, Gedijen bij onveiligheid: afwegingen rond de risico's van informatietechnologie [Profiting from insecurity; considerations around the risks of information technology]. In: D. Broeders, M. Cuijpers and J. Prins (red.), *De staat van informatie* [The state of information], Amsterdam: Amsterdam University Press.

European Central Bank, 2015, Fourth report on card fraud.

European Commission, 2015, Public Private Partnership on Cybersecurity.

ENISA, 2016, ENISA Threat Taxonomy: A tool for structuring threat information.

Europol, 2012, Payment Card Fraud in the European Union.

Gemalto, 2016, Findings from the 2015 breach level index.

Google, 2016, Transparency Report.

IDC EMEA, 2009, The European Network and Information Security Market.

ITU, 2015, Key ICT indicators for developed and developing countries and the world.

Markey, E. and H. Waxman, 2013, Electric Grid Vulnerability: industry responses reveal security gaps. US House of Representatives.

Microsoft, 2015, Microsoft Security Intelligence Report.

National Cyber Security Centre, 2014, Cybersecuritybeeld Nederland 4 [Cyber security report on the Netherlands].

National Cyber Security Centre, 2015, Cybersecuritybeeld Nederland 5 [Cyber security report on the Netherlands].

Nickerson, R., 1998, Confirmation Bias: A Ubiquitous Phenomenon in Many Guises, Review of General Psychology, vol. 2: 175–220.

OFT, 2014, Supply of Information and Communications Technology to the Public Sector.

Overvest, B. and B. Straathof, 2015, What drives cybercrime? Empirical evidence from DDoS attacks, CPB Discussion Paper 306.

Pierre Audoin Consultants, 2013, Competitive Analysis of the UK Cyber Security Sector.

Pierre Audoin Consultants, 2012, L'observatoire de la filière de la confiance numérique en France.

Ponemon, 2016, Global Encryption Trends Study.

Riek, M., R. Böhme, M. Ciere, C. Gañán and M. van Eeten, 2016, Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries, Working Paper.

Risk Based Security, 2016, *Data Breach Trends.*

Samani, R., 2013, Cybercrime Exposed.: Cybercrime-as-a-service, McAfee White Paper.

Secunia, 2015, *Vulnerability Review.*

Symantec, 2016, Internet Security Threat Report.

The World Bank, 2016, World development report 2016: Digital Dividends.

Tijdelijke commissie ICT, 2015, Eindrapport [Temporary ICT Committee, Final Report].

Tjong Tjin Tai, E., B. Koops, D. Op Heij, K. Silva and I. Skorvánek, 2015, Duties of care and diligence against cybercrime. Tilburg University.

Shapiro, C. and H.R.Varian, 1998, *Information Rules: A Strategic Guide to the Network Economy*, Harvard Business Review Press.

Verizon, 2016, 2015 Data Breach Investigations Report.

VKA/SEO, 2016, Economische kansen cybersecurity [economic opportunities cyber security].

Vollaard, B., 2003, Performance contracts for police forces, CPB Document 31.

Vollaard, B. and J. van Ours, 2011, Does regulation of built-in security reduce crime? Evidence from a natural experiment, *Economic Journal*, vol. 121: 485–504.

Appendix

Table A: Overview of data used

Data source	Data location	Time period	Type of data
ICT use according to personal characteristics, CBS	http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=71098ned	2005–2013	ICT use per educational level
Safety monitor, CBS	http://www.veiligheidsmonitor.nl/	2008–2015	Number of incidents of cybercrime, victims of cybercrime
Tables on crime and law enforcement 2014, CBS	https://www.cbs.nl/nl-nl/maatwerk/2015/43/tabellen-criminaliteit-en-rechtshandhaving-2014	2005–2014	Hacking in criminal law
Regional Assessment map, Microsoft	http://www.microsoft.com/security/sir/threat/default.aspx	2014–2015	Cyber threats to Windows users
Digital Attack Map, Google	https://www.google.com/ideas/products/digital-attack-map/	2013–2016	Number of DDoS attacks
Google Transparency Report	https://www.google.com/transparencyreport/	2014–2015	Number of encrypted emails, number of phishing websites
Security threat report, Symantec	http://www.symantec.com/security_response/publications/	2013–2015	Numbers of data leaks
Dutch Payments Association	http://www.betaalvereniging.nl/nieuws/daling-fraude-met-internetbankieren-zet-door/	2010–2015	Credit transfer fraud
Cyber Security Assessment Netherlands, NCSC	https://www.ncsc.nl/	2014–2015	Ransomware, cybercrime, key sectors
The Judicial System	www.rechtspraak.nl	2011–2015	Cybercrime court cases
cvedetails.com	www.cvedetails.com	2015	Software vulnerabilities
Statistica	www.statistica.com	2015	Market share of operating systems
Fraudehelpdesk	www.fraudehelpdesk.nl/		Number of phishing emails
Global Encryption Trends Study, Ponemon Institute	https://www.thales-esecurity.com/knowledge-base/analyst-reports/global-encryption-trends-study	2005–2015	Encryption use
Systemic Risk Survey, Bank of England	http://www.bankofengland.co.uk/publications/Pages/other/srs/default.aspx	2015	Risks to the financial system
Arbor Networks	www.arbornetworks.com/	2015	Motivation DDoS attacks
National Coordinator for Security and Counterterrorism	www.nctv.nl/onderwerpen/nv/bescherming-vitale-infrastructuur/		Key sectors

Table B: Overview cyber security risk assessment for the economy

Section	Stylised facts	Consequences for the economy	Market failure / causes	Policy options
2.1 Detection and prosecution of cybercrime	Low number of criminal complaints (8%), and slim chance of being caught; fines are lower than illegal profits	Growth in financially motivated cybercrime; Reduction in confidence and internet use	Anonymity of (foreign) perpetrators; regional knowledge lacking; increase in the significance of the internet for the economy	Digital filing of criminal complaints; increase knowledge on cybercrime among police; more international coordination; fines should match criminal profits
2.2 Market for cyber security	Market size estimated at between 0.4 and 7.5 billion euros	Sub-optimal security level; disruptions to public services	No professional procurement by government, as the emphasis is on price over quality; firms bear only part of any damage	Certify providers of cyber security; stimulate new security solutions through SBIR
2.3 Software vulnerabilities	In 2015: Windows 7 was found to have 147 different vulnerabilities (49 of which critical)	Software vulnerabilities pave the way for ransomware, data leaks and DDoS attacks	Providers not liable for software problems; asymmetric information on software quality; coordination problems in detecting and patching vulnerabilities	Make organisations liable for the damage caused; greater transparency about software quality
2.4 Encryption and authentication	Nearly 70% of emails have TLS encryption	More secure online communication; hampering detection	Coordination problems lead to ineffective use of encryption	Compulsory standards; public infrastructure
2.5 ICT dependence of key sectors	DDoS attacks and phishing cause serious problems in all key sectors	Large-scale disruptions within key sectors due to cyber attacks; unexpected effects because of complex level of dependence	Companies underinvest in cyber security, because private incentives are smaller than the benefit to society	Integral government supervision; collect and share information on vulnerabilities
2.6 Digital divide	Victimhood increases with educational level of internet users: primary 8%, secondary 12%, higher 13%	Limited ICT benefits for disadvantaged households	Criminals focus on people on higher incomes; behavioural effects	Ensure a minimum level of security
3.1 Ransomware	Rare (<1%). Average payment a few hundred euros; only few people are prepared to pay	Socially undesirable redistribution of money; crippling production or services	Asymmetric information on the level of security of websites/emails; detection problems	Regular back-ups; Also see policy options in Sections 2.1 and 2.3

	(<15%)			
3.2 Phishing and malicious websites	70000 complaints reported at the Fraud helpdesk in March 2016, over half of which concerned the impersonation of financial institutions	Less confidence in online communication; extra costs for separate, secure email accounts	People behaving less rationally; asymmetric information on security level of emails/websites; public character of the internet	Information campaigns; publicly available black lists of websites and senders; authentication techniques
3.3 Data leaks	Occurring often; credit card information the most popular objective	Loss of market value and/or customers; less confidence in data sharing	Asymmetric information on the security level of data management; negative external effects of data leaks by third parties	Make organisations liable for the damage caused; make the reporting of data leaks compulsory (on 1 Jan. 2016 implemented in the Netherlands)
4 DDoS attacks	In 2015: 1100 known attacks *on* and 2600 known attacks *from* the Netherlands; in 70% of cases the country of origin is unknown	Direct financial damage for victims; expensive separate networks; lack of confidence in online communication	Software vulnerabilities enable botnets; asymmetric information on security; public character of the internet	Transparency on security; greater responsibility for ISPs

Publisher:

CPB Netherlands Bureau for Economic Policy Analysis
P.O. Box 80510 | 2508 GM The Hague
T (070) 3383 380

July 2016