CPB Netherlands Bureau for Economic Policy Analysis

CPB Communication | 2017, July 3

Cyber Security Risk Assessment (CSRA) for the Economy

On request by the Ministry of Security and Justice

Centraal Planbureau

CPB Communication

Centraal Planbureau
Bezuidenhoutseweg 30
2594 AV Den Haag
Postbus 80510
2508 GM Den Haag

T 088 9846000
I www.cpb.nl

Contactpersoon
Bastiaan Overvest
Bas Straathof

To: Ministry of Security and Justice

Date: 3 July 2017
Subject: Cyber Security Risk Assessment (CSRA) for the Economy

1 Introduction

Society is digitising. The five most valuable companies in the world are ICT companies. The Dutch population makes extensive use of the Internet, and the government is also focusing increasingly on the use of digital means. This digitisation also involves an increase in the economic importance of cyber security. Cyber security contributes to economic opportunities, and prevents damage caused by ICT failure or disruptions, whether caused unintentionally (e.g. software problems) or intentionally (e.g. by cyber criminals).

The purpose of the Cyber Security Risk Assessment for the Economy (CSRA 2017) is to provide more insight into the economic importance of cyber security.[1] The main questions are about the developments in the field of cyber security and the related consequences or risks to the economy and society at large. Policy options are also discussed, where appropriate.

The CSRA 2017 provides an economic analysis of cyber security, with market failure and economic consequences being the central themes. Market failure may lead to either less or more cyber security than would be considered optimal, from a societal point of view. A lack of security hampers the use of ICT, but a maximum level of security, generally speaking, is also not optimal; the costs of complete security often outweigh the benefits to society. An economic analysis provides insight into economic risks and options for policy responses.

[1] This risk assessment has been partly funded by the Ministry of Security and Justice. Contributing authors are: Bastiaan Overvest, Bas Straathof, Rinske Windig, Anne Marieke Braam and Roel van Elk (all CPB), and Tatiana Kiseleva (currently DNB). We furthermore hereby would like to thank the following people for their suggestions and comments: Michel van Leeuwen (NCTV/NCSC), Lisa Reizevoort (VWS), Frederike Diersen (VWS), Lucien Engelen (Radboud UMC), Dennis Broeders (WRR). Ronald van der Luit (EZ) and Paul Ducheine (Defence). Responsibility for the report lies fully with CPB Netherlands Bureau for Economic Policy Analysis.

This report describes main risks and looks back over the past 12 months. Chapter 2 discusses a number of 'problem areas', Chapter 3 discusses threats and manifestations, while the final chapter focuses on data flows in public health care.[2] The problem areas discussed include the ICT dependence of vital processes (Section 2.1), detection of cyber crime (Section 2.2), software vulnerabilities (Section 2.3), the cyber security market (Section 2.4), and encryption and authentication (Section 2.5). The threats and manifestations discussed include the theft of confidential corporate information (Section 3), phishing and malicious websites (Section 3.2), data leaks (Section 3.3), and ransomware (Section 3.4).

1.1 Main findings

These are the main findings of this report:

- State-sponsored hackers (hackers working on behalf of a country), are aiming to intervene in political parties and democratic institutions and processes – also in the Netherlands. These interventions put pressure on international economic relationships, thus harming economic interests of the Netherlands as a small, open economy.
- In the Netherlands, 11% of the population has indicated to have been a victim of cybercrime. This is a slight decrease from last year.
- Cybercriminals derive scale advantages from a digital infrastructure (e.g. for anonymous communication and the anonymous exchange of money). The international nature of cybercrime limits the possibilities of law enforcement agencies to counter these economies of scale. This means the chances of being caught are slim and the profitability of such criminal activity remains high. Timely international collaboration may aid an effective response.
- Intelligence agencies use software vulnerabilities ('zero-days'). Unlawful publication of such information immediately leads to a less safe ICT environment for users, as well as to societal damage. An assessment framework and a response strategy are policy options that may mitigate or prevent such damage. An assessment framework helps to determine whether a zero-day vulnerability could be used for intelligence purposes or should be reported to the software provider involved. In cases of leaked zero-day information, a well-prepared response plan limits societal damage.
- Encryption enables the protection of intellectual property, competition-sensitive information and personal data, around the world. Weakened encryption due to built-in 'back doors' reduces the level of protection. However, such back doors also make it easier for intelligence agencies to analyse large-scale communication.

[2] This subject was chosen for the large societal interest related to health care and the fact that, in the health care sector, large amounts of confidential data are generated, exchanged and leaked. The CSRA 2016 featured DDoS attacks as its special subject.

- There is relatively little known about the magnitude of the damage caused by cybercrime. As a result, this may cause ICT users to be insufficiently aware of the risks. Awareness can be increased by more information becoming available, for example, through statistical research or increased corporate transparency.
- It may sometimes take years before large data leaks and other cyber incidents come to light. This is why reputation mechanisms function less optimally, which increases the importance of encryption, preventive supervision and security standards.
- Incidents at hospitals and municipalities show that the risks of data leaks particularly relate to local administrative data flows.
- A mandatory public infrastructure for the exchange of data in the health care sector can simplify compliance with standards, prevent the dependence on a single private party, and provide citizens with insight into who has access to their data. Whether the benefits outweigh the risks could be investigated.

1.2 Looking back at 2016–2017

What were the main incidences and developments in the field of cyber security? This section is limited to the period of time between the previous risk assessment and 29 June 2017.

International incidences

- June 2016. Theft of the internal correspondence of the Democratic Party in the United States by Russian hackers. Publication of 20,000 emails via WikiLeaks.
- October 2016. Large DDoS attacks via a botnet of Internet of Things appliances, such as security cameras and smart TVs.
- December 2016. Data leak of a billion accounts at Yahoo! was detected. The leak itself occurred in 2013 and 2014.
- April 2017. Hacker group 'The Shadow Brokers' published secret information from the United States' NSA about hacking techniques.
- May 2017. Large-scale ransomware-campaign 'WannaCry' infected, among others, Telefónica in Spain, Renault factories in France, and multiple NHS hospitals in the United Kingdom.
- June 2017. Tens of thousands of companies in over 60 countries were infected with the Petya virus (also known as ExPetr). The malware removed data from the infected computers.

International policy developments

- July 2016. The European Parliament issued the Directive on Security of Network and Information Systems (NIS Directive).
- November 2016. The United Kingdom presented its National Cyber Security Strategy 2016 to 2021.

National incidences

- February 2017. Possible data leak was discovered at the Dutch tax department.
- March 2017. DDoS attacks on Dutch voting advice websites *Stemwijzer* and *Kieskompas*.
- March 2017. Ransomware detected at the Dutch House of Representatives.
- May 2017. Q-Park parking garages infected with the WannaCry ransomware.
- June 2017. Dutch TNT Express and APM Terminals, among others, were disabled by Petya virus.

National policy developments

- July 2016. Anti-ransomware project No More Ransom was set up by the police.
- October 2016. Publication of the advice report by Herna Verhagen, 'Digitaal droge voeten' [digital dry feet].
- December 2016. The Cyber Crime Act III was adopted by the Dutch House of Representatives.
- February 2017. The Intelligence and Security Services Act was adopted by the Dutch House of Representatives.
- February 2017. Establishment of the 'Veilige E-mail Coalitie' [safe email coalition].
- June 2017. Introduction of the Cyber Security bill.

The risk assessment 2016 identified a number of cyber security risks and presented policymakers with a number of recommendations. What was done with those recommendations? Table 1.1 summarises the developments since the 2016 publication, for the main risks and policy options.

Table 1.1 Looking back at the main findings of the risk assessment 2016

Main findings July 2016	Looking back
Financially motivated cybercrime, such as ransomware, is on the increase	A worldwide ransomware attack infected hundreds of thousands of PCs, in over 150 countries.
Reconsider international agreements on the export of cyber knowledge	Export restrictions for data security and computers have either been specified or eased.[3]
Product liability to improve software security	Ministry of Economic Affairs is investigating options to improve software security. Cyber Security Council publishes explanation on legal framework.
Rules for authentication and encryption standards could be enforced more effectively	Establishment of the 'safe email coalition' (Veilige E-mail Coalitie) by the business community and government to implement standards.[4]
Serious data leaks and DDoS attacks remain likely	Multiple large data leaks and DDoS attacks took place over the last period.
Sophisticated attacks may threaten the financial sector	There have been a few new incidents at banks abroad.

[3] See the declaration from the plenary meeting of the Wassenaar Arrangement.
[4] Click here to read the coalition's declaration of intent.

2 Problem areas

2.1 ICT dependence on vital processes

Main points

- State-sponsored hackers also focus on political parties and democratic institutions in the Netherlands.
- The threat to the security of vital processes is particularly related to state-sponsored hackers, which may also put pressure on international economic relationships.
- Sharing of information in international context is needed, in order to protect vital organisations against the threat of cyber attacks. The NIS Directive may also help to do so.

Developments

Vital processes are services that are of crucial importance for a proper functioning of society, and whose disruption would have immediate and large consequences.[5] Examples of vital processes are power supply, drinking water supply and the storage of nuclear equipment and weapons. Private companies and government organisations responsible for such vital processes increasingly make use of ICT — as does everyone else.

Various incidents have occurred abroad, including the ransomware infections at telecom provider Telefónica and the UK's National Health Service[6], the hack of a large Brazilian bank[7], the distribution of malware via the Polish financial supervisory body[8] and a disruption of Amazon Web Services.[9] There are, furthermore, clear indications of the North Korean Government having organised a hacking of the SWIFT financial transactions system, early in 2016.[10]

Significant disruptions of Dutch processes included those of the government services of DigiD and MijnOverheid, which lasted for several hours.[11] This prevented people from logging on to the government websites of the tax department and public employment services (UWV). In addition, the NCSC received signals in 2016 from companies in vital sectors having been confronted with ransomware, DDoS attacks and phishing, although those incidents did not lead to serious disruptions.[12]

[5] See this explanation by the NCTV in which the vital processes are identified.
[6] For example, see this article in the New York Times.
[7] Cyber criminals were believed to have had access to websites, internal emails and servers. (source)
[8] Multiple Polish banks were infected, according to this article.
[9] At the time of the disruption, various apps, IoT equipment and websites such as Github, Citrix and Expedia, were unavailable. (source)
[10] Source: Group IB, 2017. (link)
[11] For example, see this news article.
[12] Source: NCSC (2016), Cybersecuritybeeld Nederland 2016 ('CSBN 2016'). (link)

On 27 June 2017, port operator APM Terminals appeared to have been infected with the Petya virus. At the time of publication of this report, the impact of this infection on shipping operations in Rotterdam was still unknown.

Last year, the effect of interference by state-sponsored hackers into elections[13] became a real and substantial risk. In the United States, the 2016 presidential elections were affected by what is believed to have been a Russian hack[14] of the emails of the US Democratic Party. And in France, in May 2017, a large number of hacked emails — some of which forged — of presidential candidate Emmanuel Macron were placed online. Manipulation of elections through big data techniques also forms a risk, in addition to hacks.[15] Moreover, disinformation ('fake news') can be distributed very easily within the digital domain.[16] This type of manipulation may also have affected presidential elections in the United States and France, as well as the Brexit referendum in the United Kingdom.[17]

In the Netherlands, there have been several incidents in relation to the democratic process. For example, in March of 2017, computers at the House of Representatives were found to have been infected with ransomware[18], DDoS attacks were carried out on the voting advice websites *Stemwijzer* and *Kieswijzer*[19], and hackers attempted to access information about the inquest into the shooting down of Malaysia Airlines Flight 17.[20] The Dutch General Intelligence and Security Service (AIVD) (2017) confirms that, also in the Netherlands, Russia is attempting to influence public opinion, and says it is investigating Russian activities.[21] To date, such attempts in the Netherlands appear unsuccessful.[22]

In addition to these incidents, there have been concerns about the reliability of the election procedures for the House of Representative. Although, since 2007, the voting computers have been replaced by paper ballots[23], the vote-counting procedures still use digital means, such as USB flash drives and software. These have appeared

[13] Although elections are not a vital process according to the definition by the NCTV, when they are affected this may have a significant impact in the longer term.
[14] According to this report by three US intelligence services, Russian president Putin ordered interference into the US presidential elections, probably with the intention of helping Donald Trump.
[15] See this background article in the Scientific American.
[16] In their empirical analysis of fake news in US social media, Alcott and Gentzkow (2017) show that pro-Trump fake news items were shared 30 million times on Facebook, against 8 million times for pro-Clinton fake news. See Alcott, H. and Gentzkow, M. (2017), Social Media and Fake News in the 2016 Election, *Journal of Economic Perspectives*, vol. 31(2): 211–236.
[17] See the contribution by Rid Thomas to the US Senate enquiry, this article in The Guardian, and this article in the New York Times.
[18] See this article in *de Volkskrant*.
[19] See this article in the *Financieel Dagblad*.
[20] See this news item by RTL News.
[21] See the AIVD's annual report (2017), p. 7.
[22] See this on CNBC.
[23] Incidentally, there are no indications of voting computers actually having been tempered with. Allers and Kooreman (2007) found no significant effect of the voting computer system on the turnout or results of elections for the municipal council or House of Representatives, over the period between 1994 and 2006. See Allers, M. and P. Kooreman (2007), Stemmachines beïnvloeden verkiezingsuitkomsten niet, *ESB*, 628–630.

vulnerable to being manipulated by cyber criminals or state-sponsored hackers.[24] In order to mitigate the risks, as much as possible, the government has adjusted the election procedures.[25] These incidents show that a dependence on ICT also causes democratic processes to be vulnerable.

Organisations with vital processes, currently, are not required to report cyber incidents to the NCSC. Under the proposed legislation on cyber security (Cybersecuritywet), it will be mandatory for these organisations to report security breaches. Such mandatory reporting is likely to increase the insight into cyber threats to vital infrastructure. A threat to one vital process may also occur in another vital process, and this proposed legislation enables cyber security firms and 'vital' organisations to learn from each other's experiences, in the area of cyber security.

In July 2016, the European Parliament adopted the Directive on Security of Network and Information Systems (NIS), in order to improve the digital security for vital processes within Europe. This directive obligates the EU Member States to exchange knowledge and collaborate, internationally. The proposed Dutch 'Cyber Security Act' is to implement the NIS Directive in the Netherlands.

Risks

Attacks by state-sponsored hackers pose the largest risks to vital processes. Vital processes are not the most attractive targets for 'ordinary' cyber criminals, because such processes usually have better security than any other targets. This also applies to the public domain, where there is a risk of digital interference at democratic institutions via hacking, the distribution of fake news, and data theft.

An additional risk of attacks by state-sponsored hackers is that of escalation. These attacks may increase the pressure on international economic relationships[26], or the victim of such a cyber attack may conduct a counter attack on the attacking country. Attempts to interfere in election processes seem directed at the promotion of protectionism, which leads to concrete risks for international collaborations and agreements, including those of the European Union, NAFTA, NATO and the Paris Climate Agreement. This is disadvantageous for the open Dutch economy. Yet another risk concerns an insufficient exchange of information about sophisticated attacks on vital processes. Information sharing already is taking place on a national level, within the Information Sharing and Analysis Centres (ISACs), which is facilitated by the NCSC. This will be further supported by the proposed mandatory reporting under the 'Cyber Security Act'. The prevention of cyber attacks requires international collaboration. To this end, the EU's NIS Directive obliges the Member

[24] See the report 'Onderzoek OSV en proces' by Fox-IT (2017). (link)
[25] Parliamentary letter by the Ministry of BZK, dated 3 March 2017. (link)
[26] In late 2016, for example, the United States expelled 35 Russian diplomats, in response to the Russian interference in the US presidential election process, and, in February 2017, the EU decided to extend the boycott of Russian products.

States to establish a collaboration framework within which both expertise and information are actively exchanged.

2.2 Detection of cybercrime

Main points

- Eleven per cent of the Dutch population have indicated to have been the victim of cyber crime, which is a decrease compared to the last year.
- Cybercrime remains profitable; technological developments, such as the Internet of Things, cybercrime as-a-service, and bitcoin mixers represent new targets and lower the costs for the criminals; the chances of being caught also remain slim.
- The ongoing innovation by cybercriminals is complicating their detection. Detection also continues to be hampered by people's low level of willingness to file a criminal complaint, and by the international character of cybercrime.
- Cybercrime could be more effectively detected through enhanced supervision on cybercrime 'as-a-service' and more international collaboration.

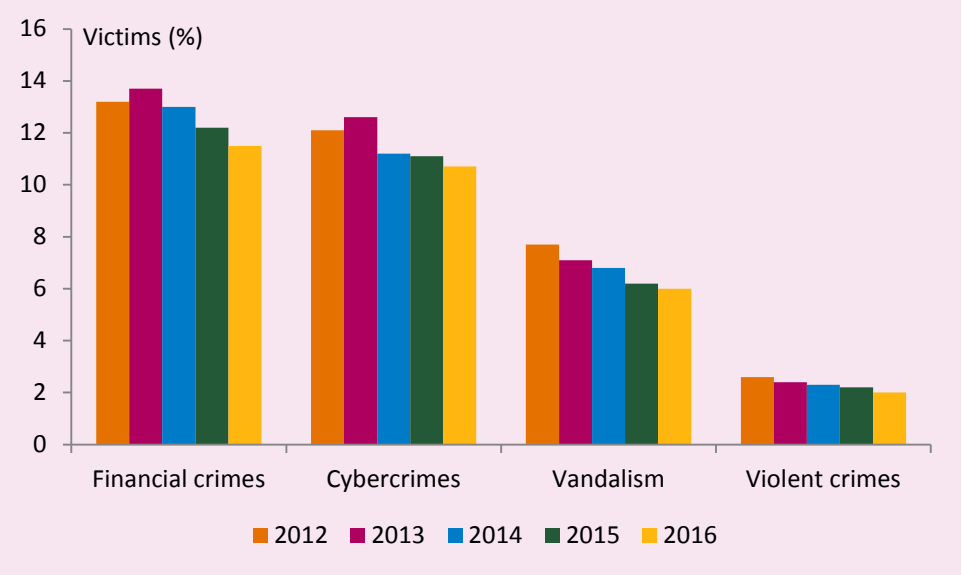
Developments

Cybercrime[27] is no longer a rare phenomenon. In the Netherlands, it is as prevalent as financial theft; according to a household survey there were 18 cybercrimes per 100 inhabitants in 2016.[28]

There is no concrete evidence of the threat of cybercrime increasing for households or businesses. The number of cybercrimes even appear to have decreased, over the last years (Figure 2.1). In 2016, 10.7% of the Dutch population was the victim of one or more cybercrimes, whereas, in 2015, this was 11.1%. The decrease in the number of victims was larger for other types of crimes, which thus increased the share of cybercrime.

[27] The subject of this section is cybercrime in a broad sense. Specific types, such as phishing and ransomware, are discussed in the next chapter, which also discusses the economic consequences of cybercrime.
[28] CBS Netherlands' Safety Monitor 2016. Netherlands Statistics (CBS) enquires about five types of cybercrime: identity fraud, sales fraud, hacking and cyber bullying.

Figure 2.1 Victimhood cybercrime and other crimes



Source: Netherlands' Safety Monitor (CBS)

In 2016, 7.6% of cybercrime victims registered a criminal complaint.[29] For more traditional offences, this was 24.7%. In 2015, 2,180 criminal complaints of hacking were filed.[30] In that year, the Dutch Public Prosecution Service (Openbaar Ministerie) investigated 124 cases of cyber crime. This number increased[31] in 2016 to 171 – which is low, considering that 11% of the population indicated to have been a victim of such crime.

Cyber crime may involve immediate costs, such as in the case of sales fraud[32] and internet banking fraud[33]. Costs may also be indirect, in the form of time and money invested in security solutions.

New technologies are changing the nature of cyber crime. Over the last year, for example, devices intended for the Internet of Thinks (IoT) appeared to be poorly protected. In 2016, an estimated 1.5 million IoT devices were infected with Mirai malware. The devices were forming an enormous botnet with which unprecedentedly large DDoS attacks could be conducted.[34] Moreover, the popularity of smartphones also provides criminals with opportunities: because of the relatively small screen, people are more likely to be deceived by a phishing email on a smartphone than on a PC or tablet. Users of mobile apps generally assume these to be properly checked by

[29] Source: CBS Netherlands' Safety Monitor 2016.
[30] Source: CBS Tabellen criminaliteit en rechtshandhaving 2015 [tables on criminalty and law enforcement].
[31] Source: Annual report 2016 of the Dutch Public Prosecution Service.
[32] The Dutch Fraud Help Desk, for example, received 3,625 such reports in 2015. The average costs involved were well over 3,000 euros.
[33] The Dutch Banking Association reported internet banking fraud of 822,000 euros in 2016; which is a 78% decrease, compared to 2015. (link)
[34] See, for example, here or here.

the providing platform; however, in 2016, hundreds of such apps were found to be unsecure.[35]

Cybercriminals are able to outsource various steps in the criminal 'production process' and specialise further. Examples are the renting out of botnets[36], distribution of ransomware,[37] and platforms that help people whitewash bitcoins.

Another technological development can be seen in cryptocurrency. Cybercriminals use bitcoins in mutual transactions, and ransom payments to lift an infection often must be done in bitcoins as well.[38] It is easy to acquire bitcoins anonymously, but the financial traffic in this cryptocurrency can be traced. This incomplete anonymity makes it difficult for users to bank illegal profits. Bitcoin mixers help to anonymise the use of bitcoins. They remove the link between bitcoin transactions and the cryptocurrency itself, by allowing the exchange of bitcoins between users, which simplifies whitewashing. New alternatives for bitcoin, such as 'ether tokens' — the cryptocurrency tokens provided by the public blockchain application platform Ethereum— try to increase the level of privacy and anonymity. After bitcoin, ether tokens are currently the most valuable cryptocurrency.[39]

In 2016, the police harvested a number of successes. One example is the set up of www.nomoreransom.org by the Team High Tech Crime of the Dutch National Police, Europol and cyber security firms. This website helps victims of ransomware to decrypt their data. Another example is the rounding up of a large botnet, named Avalanche, late 2016, in a coordinated police effort involving 10 countries.[40]

Late December 2016, the Dutch House of Representatives adopted a legislation proposal on computer crime (Wetsvoorstel computercriminaliteit 3 (WCC3)). In cases of suspicion of serious crimes, this Act authorises the remote and concealed investigation of suspect PCs or servers, and making their data content inaccessible. This may be needed, for example, when a certain server is being used to execute a DDoS attack or to spread ransomware. In principle, the Act is limited to the Netherlands. If suspected equipment is located abroad, a request for legal cooperation is still required. Only in cases that are urgent and where the country of origin is unknown, is the police allowed to act immediately.

Risks

The profitability of cybercrime appears undiminished. These types of crimes, therefore, remain a persistent problem for detection services. ICT provides the cyber

[35] Source: Intel Security Mobile Threat Report 2016. (link)
[36] For example, see this article about DDoS-as-a-service.
[37] For example, see this article by Trend Micro.
[38] Source: Europol (2016), p. 8.
[39] Source: https://coinmarketcap.com/currencies/#EUR, accessed on 6 April 2017.
[40] For example, see this news item.

criminals with an advantage over 'traditional' criminals.[41] For example, it is easier to remain anonymous on the Internet than out on the street, digital scale-ups are less complicated, and it is simpler to operate across borders. Technical innovations and developments continue to provide new possibilities for criminals, whereas detection services sometimes lack the expertise or authority to act on them. In this respect, the trend of further nationalism (Brexit, Russia) is also hampering the detection of international cybercrime — because of the declining trust between law enforcement agencies.

Another type of risk is that of hackers increasingly infecting IoT devices with ransomware or malware, or even of switching off such devices. This last impact may lead to economic damage if it involves equipment on which civil or industrial processes depend. Industrial robots, for example, are often connected to the Internet without any form of security.[42]

Policy options

In order to counter cybercrime, efficient and international collaboration between detection services is important. An option worth investigating is that of countries allowing each other to operate across borders within the cyber domain.[43] This could be agreed on in bilateral covenants or EU regulation. Similar to what is currently in the WCC3 Act, law enforcement should comply with protective preconditions, such as that of a legal review.

In addition, the focus on cybercrime as-a-service could be increased. Services such as bitcoin mixers and DDoS as-a-service, can be used for either legitimate or criminal purposes.[44] Meanwhile, it could be investigated how to counter criminal use without needlessly restricting legitimate use.

2.3 Software vulnerabilities

Main points

- Vulnerabilities in IoT appliances are partly the outcome of a trade-off between security and user-friendliness.
- Intelligence agencies use undisclosed software vulnerabilities, so-called zero-days. If such vulnerabilities are subsequently used by third parties, this may lead to a suddenly more unsecure ICT environment for users.

[41] Overvest et al. (2017) discuss the economics of cybercrime. See Overvest, B.M., T. Kiseleva and S.M. Straathof, 2017, Wat maakt cybercriminaliteit anders? [Why is cybercrime different?], *ESB*, 4746: 698-699.
[42] See this study by Trend Micro.
[43] The United States unilaterally decided to enable detection services to hack equipment that is located abroad. See this article.
[44] An organisation could use DDos as-a-service to check the stability of its own website.

- Responsibility for precautionary measures, security standards and a response strategy for intelligence agencies when leaking zero-days vulnerabilities, may reduce the impact of software vulnerabilities.

Developments

Software vulnerabilities are common. Each year, dozens of vulnerabilities are detected in large operating systems, such as Windows by Microsoft and OSX by Apple. A technological cause is the increasing complexity of software.[45] The likelihood of a fault occurring in more complex software is probably greater and the chances of detection (of each fault) smaller.

An economic cause is that of providers —sometimes implicitly— weighing factors such as user-friendliness, price and security against each other. A 100% secure software is rarely the optimal outcome of these considerations. Things go awry when providers and users do not factor in the impact on others, or when both groups are not equally informed of all the related risks.

IoT devices are an example of products for which, from a societal perspective, an undesirable choice is made between user-friendliness and security. For these types of devices, user-friendliness (plug & play) and product development speed are important conditions for commercial success. This may be at the expense of security, such as in the case of unencrypted communication between devices and weak passwords (e.g. using *admin* or *0000*).

Poorly secured IoT appliances form a risk, particularly because this involves a large number of devices; the number of IoT devices currently is estimated at 15 billion and is projected to grow to 200 billion by 2020.[46] In 2016, tens of thousands of IoT devices became infected with Mirai malware. These devices form a large botnet with which unprecedentedly large DDoS attacks can be conducted.[47] Unsecured devices can also be turned off, remotely[48], or become infected with ransomware.[49] And because industrial robots are often connected to the internet without any security, production processes are also vulnerable to simple attacks.[50]

Over the past months, it has become apparent that intelligence agencies have knowledge about a large number of undisclosed software vulnerabilities (zero-days)[51]. In March 2017, WikiLeaks published some documents showing that US

[45] The number of code lines is a measure by which software complexity can be estimated. In 1992, 2.5 million lines were sufficient for Windows 3.1. The current Microsoft Office Suite consists of around 44 million lines.
[46] Source: *A guide to the Internet of Things* by Intel (2016).
[47] For example, see this article on Krebs on Security.
[48] Source: this article on tweakers.net about BrickerBot.
[49] An example is the infection of smart TVs, as described here.
[50] See this study by Trend Micro.
[51] A zero-day is an undisclosed error or weak point in software, for which there is no solution yet. Zero-day vulnerabilities can be used, for example, to install malware or intercept data.

intelligence agency CIA has such zero-day knowledge about, among other things, cars, smart TVs, browsers and operating systems. Since August 2016, hacker group The Shadow Brokers has been publishing zero-day vulnerabilities of the US NSA for Windows, among other things. With this zero-day knowledge, it is believed that thousands of PCs were infiltrated within one week of publication.[52] In May 2017, the 'WannaCry' ransomware was shown to have been based on a leaked NSA zero-day vulnerability. This appears also to have been partly the case, last June, when the 'Petya' virus infected computers all over the world. Although Microsoft had already repaired this particular vulnerability, many users had not yet installed the related 'patch'.

Risks

Badly secured IoT devices are easily hacked. This poses financial and operational risks to the owners of those devices and the parties that depend on the devices, and also create problems for the victims of attacks by botnets consisting of those IoT devices.

The search for and concealment of zero-day vulnerabilities by intelligence agencies poses the risk of sudden entry into, and distribution within, the public domain. In such cases, software providers are forced to develop many patches within a short amount of time, and users then quickly need to update the software on their devices. As these processes take some time, large groups of users, following a zero-day leak, will be working with unsecure software until those vulnerabilities have been repaired.

Policy options

There are various possibilities for improving the security of software and other ICT products. A better utilisation of existing regulation could already help towards that end.[53] Currently, providers only support software for a limited period of time, for example for two years, even though the lifespan of the device is much longer. Providers could, beforehand, state the minimum amount of time that they will provide such support. Another option would be to set security standards for certain products. For example, IoT devices could require users to install a password themselves.[54]

In order to mitigate the impact of software vulnerability leaks, intelligence agencies could be obligated to prepare a response plan. With such a plan, comparable to 'living wills' and solvency plans of banks, intelligence agencies would be prepared to deal with unintended publication of zero-day vulnerabilities. A response plan should

[52] Source: The Register. (link)
[53] See this overview of the legal framework on the obligation of implementing precautionary measures on cyber security.
[54] The European Commission is currently investigating the need for and possibilities of improving software security via product liability law. For example, see here.

contain a description of the software vulnerabilities, all available information on repair options, as well as a protocol describing who should be informed and at what time. Whether an intelligence agency has an adequate response plan in place can only be determined in hindsight. In addition to a response plan, intelligence agencies could use an assessment framework to determine, in the case of a new zero-day vulnerability, whether this should be reported to the software provider or could be used for their own operations.

2.4 Market for cyber security

Main points

- Organisations increasingly outsource their ICT security and confidential data to specialised companies.
- The Dutch market for cyber insurance is still small.
- It is difficult for government, businesses and households to determine the need for and quality of cyber security products, which is why they are not always optimally protected.
- A 'bug bounty program' may improve the cyber security of the digital government.

Developments

Cyber security expertise is offered by a wide variety of companies on the 'market for cyber security'. There is a broad range of cyber security products and services. Examples are security advice, antivirus software, identification systems and penetration tests (or pen testing). Businesses increasingly leave their ICT and data security to external providers. The use of paid cloud services by businesses, for example, increased between 2014 and 2016, from 28% to 35%.[55] Outsourcing of cyber security to reliable providers can be the solution for companies that lack ICT knowledge themselves.

A relatively new service on the cyber security market is that of cyber insurance. Such insurance covers the damage caused by cyber incidents. This may specifically involve liability claims, the costs of repair, fines imposed by supervisory bodies, and the costs resulting from ransomware infections. This market is still small, at the moment, but it is growing fast.[56] The Dutch Association of Insurers estimates the Dutch market of cyber insurance has a premium volume of 10 million euros. In comparison, in 2015, the premium turnover for liability insurance was 1 billion euros, and 700 million euros for legal insurance.

[55] CBS Cyber security monitor 2017.
[56] According to this article in the Dutch FD newspaper, the premium turnover is expected to more than double between 2017 and 2020.

It is still unclear how the cyber insurance market will develop in the future. A possible reason for the limited size of the current market is that the damage caused by cyber incidents is difficult to quantify. Another possible reason is that companies lack reliable information and are therefore insufficiently aware of the likelihood and impact of cyber incidents.

Cyber insurance may cover costs related to ransom payments or to fines imposed by the Dutch Data Protection Authority.[57] Such cover is undesirable from a societal perspective; it turns ransomware into a profitable revenue model, and may counter the deterring effect of fines.

Risks

A risk related to the cyber security market is that of continued uncertainty about the need for and quality of market solutions. This causes companies to either run unnecessary financial risk or overspend on illusory solutions. This problem is caused by asymmetrical information; users often are less able to assess the effectiveness of security solutions. Security providers, in turn, may tend to exaggerate the threats.

There is also a risk of the government using insufficiently secure ICT. The national government has set itself the target of providing digital services to all citizens and companies, from 1 January 2018 onwards (known as the digital government: 'Digitale Overheid'). This ambition implies that government organisations need to digitise a large number of services. This should also involve a large public demand for cyber security services. Public purchasers, however, often have only a limited knowledge of ICT and cyber security, have to contend with an imperfect decision-making structure, or do not provide opportunities for smaller providers, due to unnecessarily strict requirements for participation in tenders.[58] This is why technological possibilities are not always used in the most optimal, secure way. This poses a risk to the security of digital government services.

Policy options

More and particularly reliable information is needed, in order to reduce the uncertainty about the need for and necessity of cyber security. CBS in currently (2017) investigating cyber security among Dutch companies, and this may reduce such uncertainty. A second possible solution would be a certification system. The European Commission intends to propose measures to this end, in September 2017.[59] A public cyber expertise centre for SMEs would be a third option. It is, however, still uncertain whether SMEs are running too much risk and whether this would lead to unfair competition for private cyber security companies.

[57] For example, see this description of a cyber insurance that covers ransom payments and imposed fines.
[58] Source: report by the temporary ICT committee (Tijdelijke Commissie ICT (2015)).
[59] See http://ec.europa.eu/newsroom/document.cfm?doc_id=44527.

The security of digital government services could be guaranteed more effectively by the introduction of some financial incentive (e.g. bug bounty programs) for reporting vulnerabilities within the national government's digital environment. This would also include a 'responsible disclosure policy' that would clarify, in advance, how reports will be addressed by the government. In this way, the government would stimulate ethical hackers to report any vulnerabilities in its digital services, and increase the likelihood of timely repair of such vulnerabilities.

2.5 Encryption and authentication

Main points

- Encryption and authentication are becoming simpler and their use is increasing.
- The political support for 'back doors' is increasing.
- Encryption enhances privacy and helps companies around the world to protect intellectual property, competition-sensitive information, and personal data. On the other hand, back doors make it easier for intelligence agencies to analyse communication on a large scale.
- The current Dutch Cabinet's view on encryption makes it an international frontrunner.

Developments

Encryption and authentication are techniques that may mitigate the risks of phishing, hacks and data leaks. Encryption is a means of limiting access to information to the people who are in possession of the right access codes. Examples of encryption techniques are the Pretty Good Privacy (PGP) program[60], the Transport Layer Security (TLS) protocol[61] and the Signal Protocol[62]. Authentication techniques help to identify people or devices. Examples of authentication techniques include the combination of user names and passwords, fingerprints or tokens, as are used by some banks.

Encryption is becoming simpler to use, because communication platforms do so automatically or semi-automatically. Encryption providers also innovate, for example through programs that automatically encrypt sensitive information as soon as it is being transmitted.[63] On a global level, Google reports a strong increase in the adoption of TLS. Over the course of 3.5 years, this increased from 27% late 2013, to 84% in March 2017.

[60] PGP was the encryption technology on mobile phones that, up to 2016, was used frequently by criminals. In 2016, the Dutch police confiscated a server containing encrypted communication (source), and, in March of this year, they managed to decode the messages (source).
[61] TLS is a security protocol for encrypting emails. In order to establish a secure connection, both sender and recipients have to use TLS.
[62] This is the protocol used by WhatsApp, among other things, to protect chats.
[63] For example, see this user experience

The government is investigating new alternatives for the current Dutch identity management platform 'DigiD'. Currently, a pilot project is being conducted, named Idensys. It is a method for securely and simply logging on, for example via an app or selfie. The government is also experimenting with a service called iDIN, a new service that citizens can use for identification, using the existing authentication methods of their banks. In addition, the government is investing half a million euros in strong encryption.[64]

There are two factors that put pressure on the reliability of encryption and authentication. Firstly, vulnerabilities of existing techniques come to light, on a regular basis. For example, two-factor authorisation based on text messages (sms) appears easy to circumvent[65], encrypted PGP messages have been hacked[66], and it also appears that the encryption of WhatsApp messages cannot always be guaranteed.[67]

Secondly, intelligence agencies and politicians often put pressure on providers to weaken their encryption. For example, at the request of the US Government, Yahoo! is believed to have been searching through emails for intelligence agencies, since 2015.[68] The aftermath of the terrorist attack on the UK's House of Commons in March 2017, prompted calls for weaker encryption of certain communication applications, such as WhatsApp.[69] And in the United States, two senators presented a bill proposing back doors.[70]

Risks

Weakening encryption increases the possibilities for intelligence agencies to analyse communication, on a large scale, but also involves risk. In the first place, it would be a technological challenge to limit access to such 'back doors' to only a select number of intelligence agencies. If there is the technical option of hacking encrypted communication or data, others will also try to obtain such knowledge. In the second place, limiting the level of encryption may harm people's trust in online services or transactions. In the long term, this may lead to changes in the behaviour of both citizens and companies. Limitations on encryption could, for example, increase the risk of intellectual property theft; as a result of which, companies may be less inclined to innovate.

Limitations on encryption in non-EU countries, however, offer opportunities for providers of cloud and communication services on the Internal Market. The reason

[64] See this message.
[65] For example, see this background item on Wired.
[66] See here.
[67] According to this article, this is about the web version of WhatsApp.
[68] For example, see this article by Reuters, and this article on nu.nl.
[69] For example, this news article.
[70] See this press release by senator Richard Burr.

for this is that European providers, in such cases, will be able to offer greater protection than their non-EU competitors.

Policy options

Strong encryption contributes to cyber security, as well as to privacy and protection of corporate information, in particular. The Netherlands has formulated a Cabinet view[71] on encryption that states that limitations on encryption are undesirable. This will contribute to the objectives mentioned above.

[71] See the Parliamentary Letter about encryption.

3 Threats and manifestations

3.1 Theft of corporate information

Main points

- Not much is known about incidents of confidential corporate information being stolen, which is why companies may be insufficiently aware of the chances of such theft.
- The risk of theft of confidential corporate information reduces the incentive to invest in research and development.
- Companies may apply both digital (encryption, authentication) and non-digital means (e.g. patents and screening of employees) to protect knowledge.
- Companies could increase their transparency about incidents; for example, by reporting on them in their annual reports.

Developments

Theft of technological knowledge is an old phenomenon. In 552 BC, two Byzantine monks smuggled a few silkworms out of China, in order to end the Chinese monopoly on silk. In our time, theft of confidential corporate information is considered one of the largest cost categories related to unsecure cyber systems for companies. Verhagen (2016), for example, warns against cyber threats aimed at intellectual capital. Deloitte (2016) estimates the economic costs, in the Netherlands, of theft of intellectual property and strategic information at 2.5 billion euros, annually.[72]

There is much uncertainty about the theft of confidential corporate information within the cyber domain. Although the theft of such information is seen as an important risk, only few incidents are commonly known. One such example is that of the ASML company, who reported attacks by hackers in the annual report of 2015. According to ASML, the attacks had no impact on operational management.[73] Another example is that of the Dutch–German company, Rheinmetall Defence. Starting in 2012, Chinese hackers are believed to have had access to the company's technological information.[74]

It is remarkable that so few incidents are reported, seeing that companies are often the target of cyber attacks, according to intelligence agencies. Moreover, publicly listed companies are obliged to a forthwith publication of information that would

[72] See H. Verhagen (2016), Nederland digitaal droge voeten [Digital dry feet for the Netherlands], and Deloitte (2016), Cyber Value at Risk in the Netherlands.
[73] For example, see this article on Tweakers.
[74] For example, see this article in *de Volkskrant*.

materially affect their profits. If commercially sensitive information is regularly stolen from Dutch companies, one would therefore expect more press releases about this.

A possible explanation for the absence of such press releases is that, although companies are in fact attacked, hackers are hardly successful in stealing confidential corporate information. Another explanation could be that incidents are kept secret because of security reasons – even though this is against the reporting obligation under the Dutch Financial Supervision Act. A third explanation, which may seem less likely, is that hacks occur only rarely among Dutch publicly listed companies.

Risks

The risk of the theft of confidential corporate information may have negative effects on the economy.[75] For example, it can reduce the incentive for companies to invest in R&D or reduce market research. After all, the risk of theft and use of new knowledge by competitors would decrease the expected returns on such investments.[76]

To prevent a company from having to compete against the results of its own confidential corporate information, a solid protection of intellectual property is necessary. Because of the limited degree of reporting about confidential corporate information, companies may be insufficiently aware of the risks. This may cause them to invest too little in the digital protection of their intellectual property.

The risk of theft seems particularly large in cases of trade barriers between countries. The countries currently associated with digital espionage (China, Russia, North Korea) are also countries for which trade restrictions are in place. This is not a new phenomenon; during the Cold War, there was a trade embargo. On the basis of Stasi archives and industrial data, Glitz and Myersson (2017) show that East German spies worked at West German companies.[77] They demonstrate that the espionage strongly reduced the productivity differences between both countries, particularly in the sectors faced with the highest trade barriers.

Policy options

Companies can improve the protection of their crucial information; for example, by using encryption and authentication techniques and screening of employees.

---

[75] Friedman et al. provide an economic analysis of confidential corporate information, and show why sometimes companies have good reasons for not applying for patents (formal intellectual property). See Friedman, D., W. Landes and R. Posner (1991), Some Economics of Trade Secret Law, *Journal of Economic Perspectives*, vol. 5(1): 61–72.

[76] Empirical research by Aghion et al. (2015) about the European Internal Market shows that stronger protection of intellectual property leads to increased innovation within competitive sectors. See Aghion, P., P. Howitt and S. Prantl (2015), Patent rights, product market reforms, and innovation, *Journal of Economic Growth*, vol. 20(3): 223–262.

[77] A. Glitz and E. Myersson, 2017, Industrial Espionage and Productivity. (link)

Companies may also apply for a patent, in certain cases. As long as the legal protection of the patent is adequate, such a patent will protect a company in an indirect way against theft by competitors. If infringements of European patents in China (and vice versa) can hardly be addressed, this will negatively affect international revenue options, and induces the theft of technological knowledge. Compliance with international agreements about respecting each other's intellectual property will prevent this.[78]

Finally, companies being transparent about cyber incidents may contribute to larger awareness of the risks of corporate theft. This may be achieved via an obligation for large companies to report cyber security incidents in their annual reports.

3.2 Phishing and malicious websites

Main points

- Phishing is the starting point of much cybercrime.
- In 2016, the number of reported phishing emails and the number of discovered malicious websites increased.
- It continues to be difficult for every user to separate fake from real, under all circumstances; the focus should therefore be on prevention.

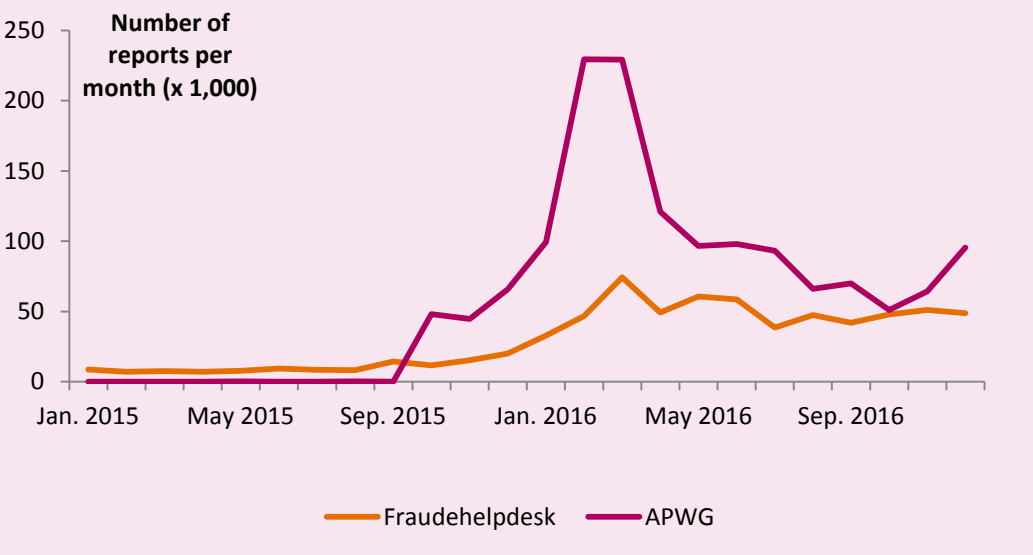
Developments

'Phishing' is the collective term for various types of fraudulent emails. Through these emails, the senders are trying to obtain personal data, install malware[79], send spam or collect on fake invoices[80]. According to some experts, as much as 91% of all cybercrime starts with a phishing email.[81] The recipients of phishing emails are sometimes led to a malicious website (or 'phishing site'). In March 2016, the email accounts of various members of the US Democratic Party were hacked in this way.[82]

In 2016, there was a strong increase in the number of reported phishing emails (Figure 3.1). The Dutch organization Fraud Help Desk reported around 10,000 incidents in 2015, whereas in 2016 this number increased to nearly 50,000. A comment to be made regarding these data is that the increase in the number of reports is only an indication of the real increase in the use of phishing. The increase in the number of reports may also have been caused by people becoming more familiar with the reporting offices.

[78] According to a report by the US Government, the protection of intellectual property in China is still insufficient (Source)
[79] Between April 2016 and February 2017, on average, 1 in 250 emails contained malware, according to Symantec Monthly Threat Report. (link)
[80] According to this article by Fortune on Facebook and Google, fraud was committed for as much as a hundred million US dollars.
[81] This study by Trend Micro from 2012, for example, argues that 91% of focused attacks take place via phishing, as is confirmed by information in a report by PhishMe from 2016.
[82] For example, see this news article.

Figure 3.1 Strong increase in the number of reported phishing emails in 2016

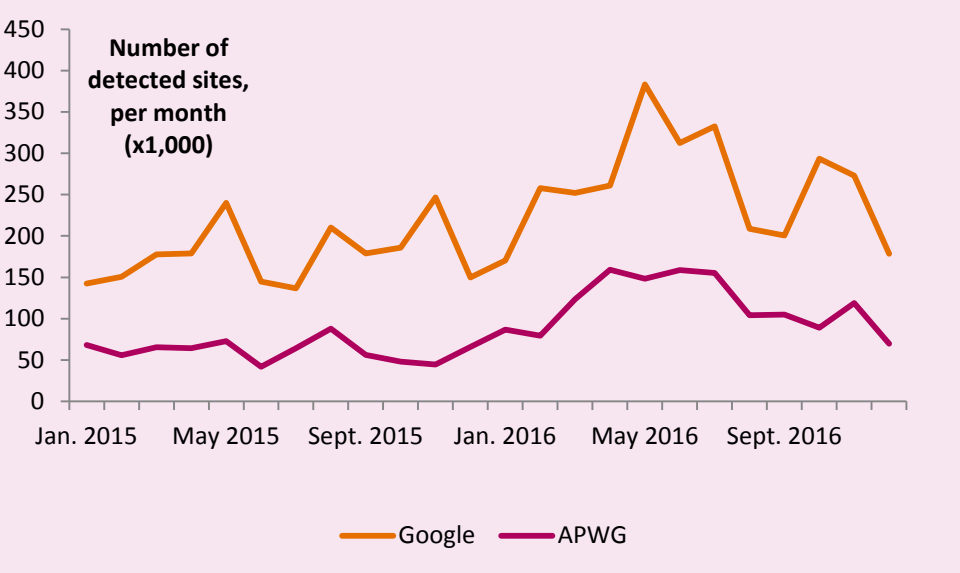


Source: Fraudehelpdesk and Anti-Phishing Working Group (APWG)

The number of malicious websites also increased (Figure 3.2). In 2016, Google uncovered 3.1 million malicious websites, nearly a million more than in 2015.

A logical explanation for this increase in that phishing is still profitable. Cyber criminals apparently continue to be successful in circumventing security measures and appear reliable.

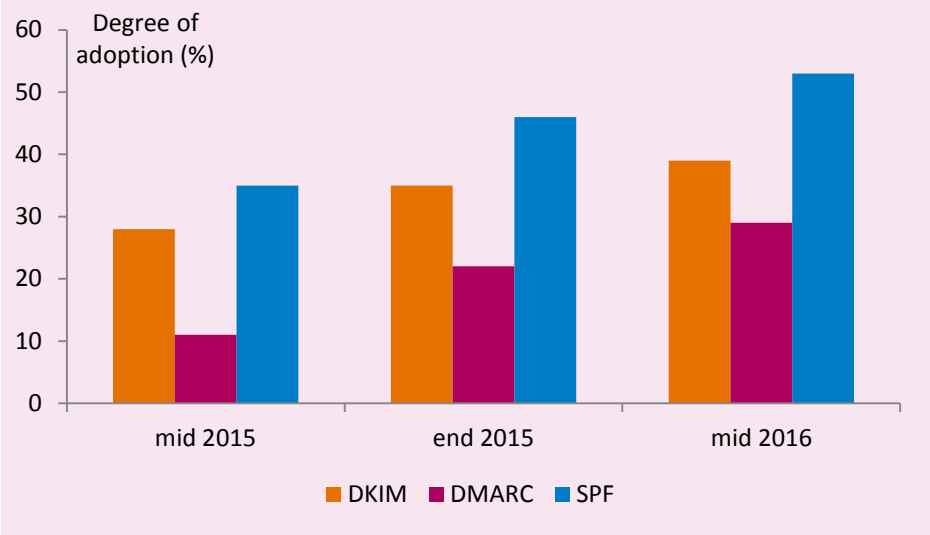
Figure 3.2 Number of detected phishing websites increased in 2016



Source: Google Transparency Report and APWG

There are standards for safer emails (named DMARC, DKIM and SPF). These standards help to prevent forgery of the name of the recipient or content of the email message. In February 2017, companies and government organisations agreed on stimulating the implementation of these standards.[83] Between mid 2015 and mid 2016, the adoption of these standards among government organisations did increase, from an average 25% to 40%, although this is still below target.

Figure 3.3 Adoption of standards increased



Source: Forum Standaardisatie. Note: degree of adoption among around 150 government domains.

Another explanation is that cyber criminals are applying new strategies, such as so-called IDN homograph attacks[84] or messages personalised with public or stolen data.[85]

Risks

Phishing emails and malicious websites are becoming increasingly difficult to distinguish from genuine websites. Phishing is likely to continue to be profitable, and thus will continue to inflict damage. Economic damage may occur through various forms of cybercrime that follow from a successful phishing email. Less visible, but present nevertheless, is the effect of phishing on general confidence in emails and the costs of prevention.

Policy options

If a seemingly reliable email message reaches users, a number of recipients will always be fooled by it. It is therefore important to prevent phishing emails from

[83] This is the Safe Email Coalition. For more information, see this article.
[84] This attack uses the fact that some letters, from various alphabets, such as Latin, Cyrillic and Armenian script, look the same in Unicode. See this article for more information.
[85] For example, data from millions of LinkedIn users were stolen in 2016, for a phishing campaign. (source)

arriving at their destination. This may be achieved by stimulating the use of security standards, such as DKIM, DMARC and SPF.

3.3 Data leaks

Main points

- Data leaks often are discovered at a late stage — sometimes not until years later.
- The later a leak is discovered, the less useful it is to apply repressive (ex-post) supervision. Effective protection of personal data, therefore, will also need to be focused on preventing data leaks.

Developments

Personal and corporate data are increasingly stored in digital form, by governments, businesses and societal organisations. In case of a data leak, data are destroyed or manipulated, or provide unauthorised people with access. Data leaks may be the result of carelessness (e.g. people losing USB flash drives containing personal data) or cybercrime. Criminals may, for example, use credit card information or blackmail the owner of sensitive personal data. Part of the damage also ends up at the organisation from which the data was leaked.[86]

Data leaks may take on large proportions, such as the Panama Papers (2.6 terabytes in fiscal data) and the leak at Yahoo! (data on 1.5 billion accounts). Sometimes, there also are long delays before data leaks become known. For example, the data leak at Yahoo! occurred in 2013, but only became known in 2016. Something similar occurred with Myspace in 2016, where it took three years for a theft of millions of login data to become public.[87] In February 2017, Dutch TV programme Zembla warned about the risk of data leaks at the Dutch tax service, over the 2013–2016 period.

Table 3.1: Estimated number of data leaks

Source	Reach	Number of data leaks 2015	Number of data leaks 2016
Symantec	Worldwide	1211	1209
Privacy Rights Clearinghouse	United States	157	538
Risk Based Security	Worldwide	3930	4149
Gemalto	Worldwide	1673	1792
Verizon	82 countries	2260	1935

[86] Krishnamoorthy (2016) shows that, after a data leak is disclosed, the market value of publicly listed companies decreases by an average 0.3%. See Krishnamoortyh, S. (2016), Stock market impact of privacy breach disclosures & their sentiment-based countermeasures (ex-ante), *Master's thesis, VU University Amsterdam*.
[87] See this article on PC Mag.

There is much uncertainty about the total number of data leaks. Table 3.1 provides an overview of estimates from five international sources. The magnitudes in these estimations vary greatly.

In the Netherlands, in 2016, 5,849 incidents were reported to the Dutch Data Protection Authority (DPA[88]). In the first quarter of 2017, this figure had increased to 2300.[89] In most cases (45%), a data leak is created by information being sent to the wrong recipient. Data leaks due to phishing, hacking or malware occurred in 7% of cases. The last may not seem like much, but digital data leaks can contain enormous amounts of data.[90] Over the period from January 2016 to March 2017, no fines were imposed by the DPA.

Risks

One of the risks of data leaks is that they inflict damage via misuse of the leaked information. If illegally obtained personal data are up for sale, criminals can use this information, for instance, for spear phishing. This is what seems to have happened to the data of millions of LinkedIn users. These data had been leaked in 2012 and appeared to have been used in a phishing campaign in 2016.[91]

Another risk is that of data leaks continuing to occur because organisations have too little incentive to prevent them. This may be the case at organisations with a dominant market position (e.g. hospitals and government organisations). If, following the disclosure of a data leak, the clients of such organisations are unable to leave and go to a competitor; thus, the reputation mechanism is less effective. Data leaks, often, are disclosed long after the fact, which means that stakeholders (clients, board members, supervisory bodies) cannot intervene in the early stage — if they are informed at all. And, finally, there is less incentive to prevent such leaks if organisations believe the chances of being fined by the supervisory body are unlikely.

Policy options

Prevention is an important element of the supervision of the protection of personal data. This can be achieved via market scans, on-site check-ups, or by providing information about security standards. Preventative supervision also calls for a credible and proportional fine policy.

[88] In the Netherlands, the reporting of data leaks has been mandatory since January 2016. All organisations that fall under the Dutch Data Protection Act (this includes SMEs and the self-employed) are obliged to report a data leak to the DPA within 72 hours of discovery.
[89] See this press release by the DPA.
[90] The DPA, for example, has mentioned a data leak at a customer portal whereby the data of 680,000 people had possibly been freely accessible.
[91] See this blog by Fox-IT.

3.4 Ransomware

Main points

- Little is known about actual ransomware infections.
- The distributors of ransomware employ new technological possibilities, such as IoT devices, new software vulnerabilities and botnets, as well as new ways of infecting those targets that are likely to have a greater willingness to pay.
- There is the risk of ICT users underestimating the impact of ransomware, which may cause loss of data or disruption to certain processes.

Developments

Up to May 2017, it was rather difficult to properly interpret the risk of ransomware, as there are no administrative data on prevalence, and victims of cybercrimes seldom lodge an official criminal complaint. The discovered number of ransomware variants did increase, from 35 in 2015 to 193 in 2016.[92] Furthermore, a number of remarkable incidents occurred. For example, an Austrian hotel could not issue new room keys because of a ransomware infection[93], and in the Netherlands, the House of Representatives was also believed to have been infected.[94]

The risk perception of ransomware changed on 12 May 2017. On that day, the WannaCry ransomware variant infected hundreds of thousands of computers, within a very short period of time.[95] In this way, for example, the Spanish telecom company Telefónica and UK hospitals became infected.[96] WannaCry seems to make use of software vulnerabilities of Windows ('Eternal Blue'), leaked by hackers in April. At the end of June 2017, a new virus, Petya, appeared, which poses as ransomware, but it looks like Petya is overwriting data (destroying them) instead of encrypting them.

The use of zero-day vulnerabilities is illustrative of the fact that cyber criminals innovate. Hackers not only search for new software vulnerabilities, they are also looking for new vulnerable software. In the past, ransomware particularly affected PCs, whereas currently also tablets, Android smartphones[97] and smart TVs[98] are becoming infected. The revenue model is also changing. The Popcorn Time virus, for example, offers victims a choice between paying a ransom and sharing a link with two others which will infect them. The data is subsequently said to be decrypted as soon

[92] Source: F-Secure. (link)
[93] See this article on Wired.
[94] According to, for example, this article on nu.nl.
[95] See, for example, this entry on Wikipedia.
[96] At Telefónica, the impact of the virus on operational management was limited (source). The infection at the National Health Service resulted in blocked access to patient information and failing medical equipment connections. Medical personnel, therefore, had to resort to pen and paper and their own mobile telephones (source)
[97] This has been going on since 2014. See this explanation by Kaspersky about Koler ransomware.
[98] See this article on PC World.

as those other two victims pay up.[99] It is becoming easier for cyber criminals to spread ransomware through 'ransomware-as-a-service' services.[100]

Ransomware can also be used as a supplement to the income of cyber criminals, rather than be their main revenue model. In the case of the GameOver botnet, many computers were infected across the world, particularly with the purpose of stealing money directly from businesses and wealthy private citizens. Not all of the infected computers within the botnet were located at this target audience; in order to still make money from those, the hackers developed the CryptoLocker ransomware.[101]

In July 2016, the NoMoreRansom project was started at the initiative of Europol, the Dutch police and a number of cyber security companies. NoMoreRansom helps the victims of ransomware to unlock their data. Over the period between July 2016 and March 2017, 75,000 people around the world regained access to their data via NoMoreRansom.[102]

Risks

ICT users may underestimate the risk and consequences of a ransomware infection, because ransomware and its prevalence are relatively unknown, and because of the continually changing strategies of the ransomware distributors.[103] This may lead to unnecessary loss of data and the disruption of processes that depend on this data.

Policy options

To increase the insight into ransomware, more research could be done in this form of cybercrime. Businesses and government organisations could also provide greater transparency about the number of infections and their organisational consequences. The government could provide a financial incentive to ethical hackers, in order to find rapid solutions for new ransomware variants, such as unlocking and prevention techniques.

4 Data flows in health care

Main points

- The possibilities for eHealth are increasing, but currently care providers relatively seldom share medical files among themselves or with clients.

[99] See this article on Wired.
[100] For example, see this article by Trend Micro.
[101] Source: 'Inside the Hunt', article on Wired. (link)
[102] See this news article in the NRC newspaper.
[103] Although the WannaCry ransomware has received a large amount of attention, the number of –known– infections in the Netherlands seems to have been limited to the Q-Park car parking company. See this article in the Telegraaf newspaper.

- Reports of data leaks and incidents at municipalities show that the risks of data leaks particularly apply to local administrative data flows.
- A mandatory public infrastructure for data exchange could make it easier for standards to be complied with, prevent dependence on a single private party and provide citizens with insight into who has access to their data. Whether these advantages would outweigh the risks could be investigated.
- Supervisors and supervising bodies will also need to possess technical expertise and have effective data security in place, in order to function effectively.

4.1 Introduction

The health care sector is primarily important for public health care, but its economic importance is also substantial; expenditure on health care amounts to 14% of GDP. In addition, a healthy population and labour force contributes to prosperity and human well-being. Cyber security, therefore, is very important in the health care sector, as large amounts of personal data are being created and exchanged.

Similar to the situation in other sectors, digitisation in health care involves a number of concerns with regard to cyber security. For example, around the world, more ransomware infections occurred in this sector than in any of the others.[104] In May 2017, 40 hospitals of the National Health Service in the United Kingdom were infected with the WannaCry ransomware. Dutch hospitals also appeared vulnerable; of 25 hospitals surveyed, 15 (60%) indicated that they had been affected by ransomware during the previous three years.[105] This led to far-reaching consequences; many care providers no longer had access to medical data, various units had to be closed and patients were passed on to other hospitals.[106] Dutch hospitals did not appear vulnerable to the WannaCry ransomware.

Large amounts of administrative data are being exchanged within the health care system. This includes invoices from care providers and those related to the use of medication. The exchange of administrative data is directly related to how the health care system is organised. The health care sector, as a semi-public sector, is more regulated than any of the other economic sectors. Thus, health care organisations are obliged to exchange information, for example, with supervisory bodies and insurance companies. In addition, administrative data are often also used in medical research.

The sizeable exchange of personal data in the health care sector is also reflected in the number of data leaks reported to the DPA. Nearly a third of all reports are from

[104] For example, see this article.
[105] Source: this NOS news article.
[106] Source: Wired.

the health care sector (see text box). This is twice as much as one would expect based on the the sector's share in the economy.

Mandatory reporting of data leaks in health care

Since 1 January 2016, institutions are obliged, under the Data Leaks (Reporting Obligation) Act, to report data leaks to the DPA. In the first quarter of 2017, 666 cases from the health care sector were reported to the DPA; 27% of the total number of reports (source). In 55% of cases, this involved simple incidents of personal data having been sent to the wrong recipient; 4% concerned hacking, malware or phishing (source). The amount of personal data involved differed strongly between reports. In 32 of the cases, the consequences were serious enough to warrant investigation by the DPA. In addition to reports from the health care sector, 331 reports came from municipalities — some of which were also health care-related.

An example is that of a large data leak at the Antoni van Leeuwenhoek hospital, where an unsecured hard disc containing personal and medical data on 781 patients was stolen from a car (source: NOS). Also, in May 2017, a USB flash drive was stolen from an employee of Roche Diagnostics Nederland, which contained data on close to 2000 patients of the VUmc (VU University Medical Center Amsterdam) (source).

Data leaks often remain unknown (source: Kaspersky). Within the health care sector, 31% of organisations say to have reported their most recent incident to the DPA, against 47% in the financial sector. The relatively large number of reports from the health care sector, therefore, is not the result of more willingness to report, but likely reflects the sector's vulnerability to data leaks.

This chapter provides an overview of the risks involved in data flows in the health care sector. First, the risks around the exchange of medical files and administrative data within the Dutch health care system are discussed. Included are the subjects of upcoming technologies, new players, and alternative use of medical data. The final section summarises the main risks and policy options.

4.2 The Dutch health care system

Within the Dutch health care system, a wide variety of organisations are actively involved in the exchange of information. Figure 4.1 shows the most important data flows, for both medical files and administrative data. The figure distinguishes seven categories: gatekeepers, care providers, insurance companies, administration offices, data processors, research institutes and supervisory bodies.

Gatekeepers and care providers

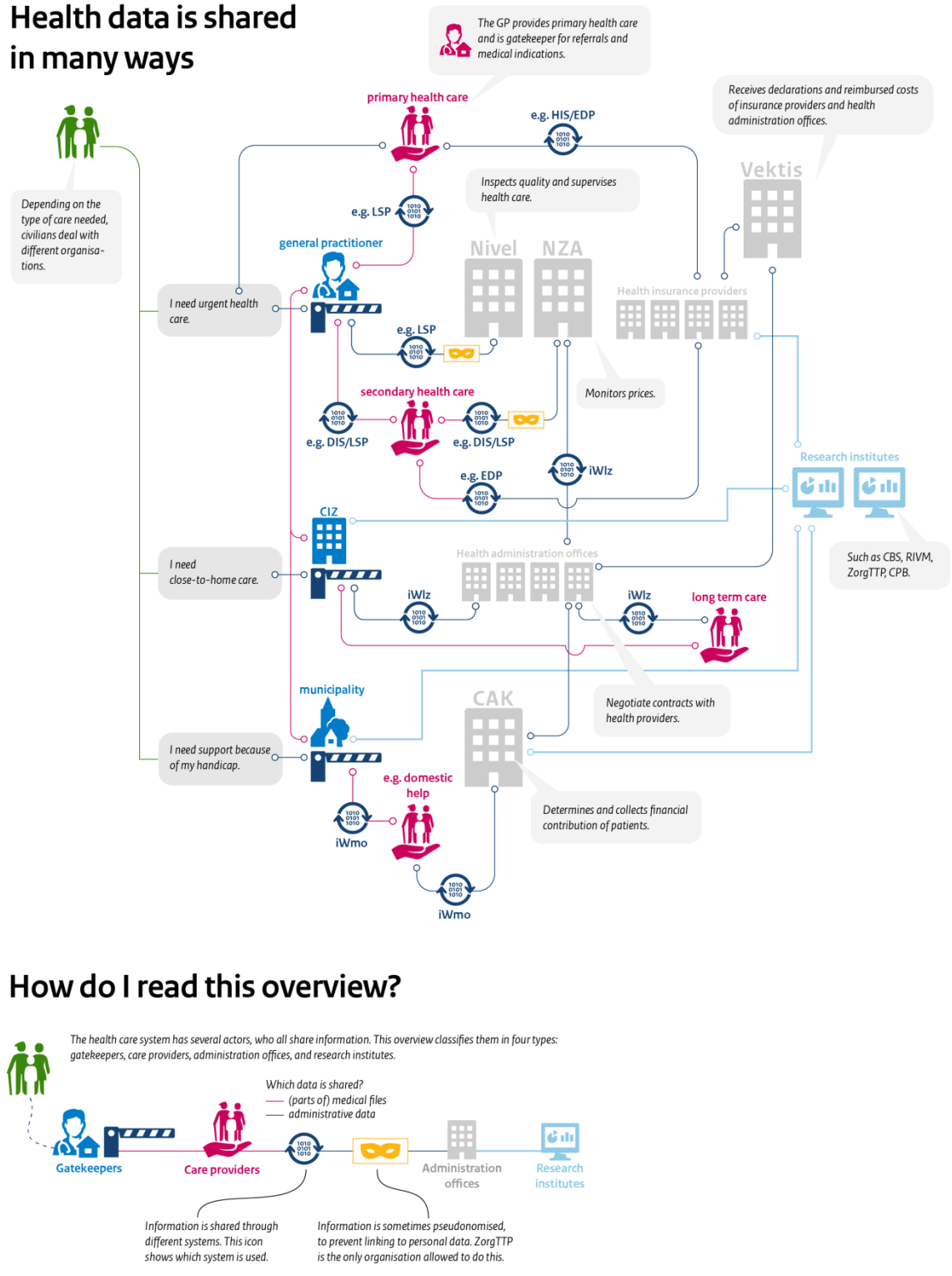
The complex organisation of the Dutch health care system has the side effect that large amounts of administrative data are being exchanged. In addition, elements of, or even complete medical files need to be shared by care providers, in order to receive health care. For example, all primary health care in the Netherlands, including visits to the general practitioner and dentist, is freely available, but other types of care require a referral or medical indication. Depending on the type of care ('cure' or 'care'), access can be gained through various so-called gatekeepers: general

practitioners, the Dutch centre for care assessment (Centrum indicatiestelling zorg (CIZ)) and municipalities. Within the 'cure' environment, the general practitioner determines the need for medical care (Dutch Health Insurance Act (Zvw)); while, within the 'care' environment, the CIZ assesses the need for long term close-to-home care (Long-term Care Act (Wlz)), and municipalities are responsible for providing home-care support (Social Support Act (Wmo)).

Within the cure environment, care providers use for example the national exchange platform ('landelijk schakelpunt' (LSP)) for storing and sharing medical data. Participants in the LSP platform are general practitioners (currently 91% of all GPs), chemists and care *groups* (i.e. health care provided by multiple types of providers).[107] The actual *use* of the LSP platform appears to be lower; of the participating GPs, only 68% of them are using the platform.[108] Hospitals use the DBC information system (DIS) for collecting data about the type of care that is provided and invoiced by care providers.

[107] See this page of VZVZ, accessed on 20 June 2017.
[108] Source: Nictiz (2016), Fig. 9.1 (link). Because general practitioners also use other communication means, in addition to the LSP platform, the share of LSP in data exchange is lower than the percentage of participating GPs.

Figure 4.1 Administrative data, in particular, are shared among multiple organisations



Within the care environment, there is widespread use of iStandaarden [iStandards]. These information standards are managed by the National Health Care Institute, and consist of a series of regulations and agreements about the exchange of medical data between users. One of the iStandards is iWlz; using this standard is mandatory for care providers, CAK, CIZ and health insurance organisations, when communicating about medical data concerning Wlz care. Communication about the care provided under the Wmo has its own iStandard: iWmo. This standard is not mandatory and is used by providers of health care and support, municipalities and the CAK. In addition, health care institutions have their own information systems and often also their own patient portals.

Under the current system, all GPs and municipalities must organise their own data security. This poses the risk of medical data being insufficiently secure at GP practices, which means information system are vulnerable, for example, to ransomware attacks. Furthermore, data leaks may not be discovered. At municipalities, there is also the risk of insufficient awareness of the need for securing medical data. Even large municipalities, such as Rotterdam and Eindhoven, were found to have less than optimal data security.[109]

Citizens have the right to determine who has access to their medical data, but they have no way of checking whether gatekeepers and care providers, in practice, are complying with their wishes. Nor can they check how their personal medical file is secured. Large care providers, such as hospitals, have far more of an incentive to maintain a good reputation, with respect to data security, compared to small gatekeepers and care providers. In case of an incident, a hospital would receive far more media attention than, for example, a general practitioner's office. Besides, large organisations will experience more incidents, statistically speaking, than small organisations, under the same level of security. Thus, the reputation mechanism is less effective for smaller organisations.

Another issue is that the costs of protection against certain attacks or incidents are too high for small organisations to bear. The reasons for this are twofold; first, many types of security costs are independent of the scale to which they apply. Second, for those smaller organisations, the benefits of prevention do not outweigh the costs, due to limited liability; the financial damage for the health care organisation cannot be larger than the costs of bankruptcy.

The limited market incentive for cyber security at smaller gatekeepers and care providers increases the relevance of their supervision by the DPA and IGZ. The variety of data systems at general practitioners and municipalities does mean that it is costly for such supervisory bodies to check whether data are adequately

[109] For example, see the article 'Wij weten alles van u', in *De Groene Amsterdammer*, 3 May 2017.

protected.[110] This leads to the risk of gatekeepers and care providers underinvesting in cyber security.[111]

Insurance companies

With the implementation of market regulation in 2006, health insurance companies have been given an additional role. In addition to dealing with invoices and payments, they also have to enter into agreements with care providers about type of care and related costs. The insurance companies receive administrative data from the care providers about medical treatments and the use of medication. Vektis, the Dutch business intelligence centre for health care, receives claim forms from health insurance companies in an automated way, and therefore possesses a data set of administrative data, including personal data, medication use, the insured care in the Netherlands, as well as demographic data.

Vektis and insurance companies both have administrative data from which the health of every Dutch citizen could be derived. Risks of data leaks and insufficient security currently seem relatively low, as insurance companies benefit from having a good reputation. After all, policy holders can take their business elsewhere, when they have no confidence in their current insurance company — although the choice of health insurance companies is fairly limited.

Administration offices, data processors, research institutes and supervisory bodies

Data which are exchanged via various information systems (e.g. DIS) can partly be used for research purposes. They are used, for example, to map population health levels and waiting lists for certain types of care. In addition, these data are used to enhance the quality of health care. Examples of such Dutch research institutes are Statistics Netherlands (CBS) and RIVM. CBS is the only organisation in the Netherlands authorised to link data to Citizen Service Numbers (BSN). All other organisations must use their data in such a way that it can no longer be traced back to an individual citizen. In order to protect patient data, certain organisations apply pseudonymisation to personal data.[112] The ZorgTTP foundation carries out such a procedure on behalf of, for example, institutes (including health care), government authorities, statutory bodies and research firms.[113]

Supervisory bodies such as the Dutch Healthcare Authority (NZa), DPA and IGZ monitor compliance in relation to public health care interests. The NZa particularly supervises the behaviour of health insurance companies and care providers, and is provided with access to administrative data, in order to do so. The DPA supervises

[110] The health care institutions investigated by the DPA all were found to have implemented insufficiently effective precautionary measures. (Source)
[111] For example, in late 2016, the DPA indicated that patient portals at hospital websites were insufficiently secure. (Source)
[112] The DPA (2016) has indicated that personal data, even after pseudonymisation, can be traced back to individual people, and therefore are still regarded as personal data (link).
[113] Open source alternatives for pseudonymisation, such as PEP (link), are available but not often used.

the privacy of citizens and has the authority to impose fines in cases where the data security at health care organisations is insufficient. From May 2018 onwards, such fines can reach 20 million euros, or 4% of the offender's annual turnover. Supervisory bodies have no access to the actual medical files, themselves. The IGZ safeguards the quality of health care providers, and under certain strict conditions, can be granted access to medical files.

Supervisory bodies are important, as health care users have no insight into the activities of administration offices and research firms, nor do they have the possibility to switch between administration offices. Therefore, the incentive for administration offices and research firms to maintain a good reputation is not always very large. [114] This also applies to data processors, such as ZorgTTP, who play a central role in the security of data flows. An inadequate reputation mechanism increases the risk of large-scale data leaks and general shortcomings in cyber security, unless supervisory bodies are able to provide sufficient counterweight.

4.3 Upcoming technologies and new data flows

A fundamental feature of digitisation is the development of new 'general purpose technologies', such as online platforms, robots and big data (Bijlsma, Overvest and Straathof 2016). These new technologies offer benefits to patients, clients and care providers, while also involving new risks to cyber security. These risks are related to new data sources, new providers of products and services, and new data applications.

New data sources

Digitisation leads to a series of products and services that also may have a medical application. Mobile devices, such as smartphones, smartwatches and Fitbits, monitor physical activity and heart rate, also in healthy people. These devices enable users to measure and share medical data, and to provide it to third parties for analysis. Certain medical tests and examinations, such as for diabetes and Parkinson's disease, can simply be carried out using an app. In certain cases, patients are then directly dependent on the device that is connected to the internet.

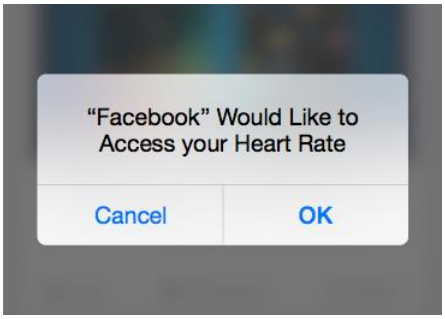
Devices with a medical application are not the only source of health-related data. More indirect sources, such as searches on the Internet, IoT devices, social media, and supermarket purchases, can increasingly be used to derive certain aspects about a person's health.

Data flows do not only originate from formal roles of organisations in the health care sector, but also from the use of technology. The further digitisation of society also

[114] These organisations may differ with respect to the importance of reputation; for example, a data leak at CBS may have consequences for the willingness of citizens and organisations to provide their data to CBS.

involves the increase in the range of devices and data sources that could provide insight into someone's health. The protection of health data, thus, is no longer the exclusive responsibility of the health care sector, but expands to also include companies with a wide variety of backgrounds.

Figure 4.2 Health-related data sharing is simple



New providers

Technology companies, such as Apple, Google, Amazon and Facebook, provide products and services that can also be applied to health care. These companies sometimes directly facilitate medical applications. The *HealthKit* and *ResearchKit* by Apple, for example, offer a platform for health apps that can use mobile devices. The *ResearchKit* is focused explicitly on medical research and can also be used in combination with third-party accessories (e.g. blood pressure monitors). Another example is the application of *machine learning* by Google when establishing diagnoses.[115]

Technology companies, in general, are aware of cyber security risks, and have a reputation to protect as reliable suppliers. There is a strong reputation mechanism in health-related services; a blunder at a health service may harm the trust in all services offered by the particular company. A limited risk here could be that medical data in the Netherlands are considered more sensitive than in the — often US — domestic markets of these companies. Another risk is that also the companies with insufficient security are able to offer health apps on a platform that users believe to be secure. Platforms could screen the providers of apps, but they also benefit from the accessibility of the platform.

Not only technology companies are focusing on health care; electronics companies also increasingly develop more medical devices. In principle, the same reputation mechanism applies to these company as to technology companies, although the related cyber risks are relatively new. This last point may translate into an absence of security updates for software in medical devices — particularly those that are connected to the Internet. The fact that these companies are still struggling with the

[115] For example, see this article.

cyber security of medical devices is apparent, among other things, from a survey by the Ponemon Institute (2017) among producers and professional users of these types of devices.[116] For example, 80% of producers and health care organisations indicate that medical devices are difficult to secure. And only 37% of producers expect that vulnerabilities in those devices will be discovered. Furthermore, the responsibility for the security of medical devices is not well-organised; for example, a third of respondents indicated that no-one carried the ultimate responsible for cyber security. Larger producers, such as Philips, continue to build their reputation in the area of cyber security,[117] and are able to achieve advantage over their competitors by producing cyber-secure devices.

New data applications

New data sources are continually being created. In addition, the possibilities for data analysis are also increasing. Because the decrease in the costs of computer calculations and data storage is continuing (Moore's law), the use of analysis techniques such as machine learning is continually improving.

New data application methods are emerging from a combination of new data sources and improved analysis techniques. Medical applications include the fields of diagnosis and treatment. There are also certain non-medical applications, such as for insurance companies.

Machine learning has been applied successfully, on a small scale, in the diagnosis of skin cancer and diabetes. A much-used method in automating diagnoses is that of a neural network that is being trained by experts. This form of diagnosis has the advantage that a neural network is potentially better at diagnostics than experts themselves, and such a network may be used by multiple patients — simultaneously and location-independent. For example, a smartphone could register whether someone has an increased risk of certain complications.[118] As the applications of machine learning increase and improve, diagnoses and the determination of related treatments will shift from individual care providers to the companies that offer such diagnoses and treatment suggestions as a service. This will increase the health care sector's dependence on ICT.

Medical data may also be used for non-medical purposes. Health insurance companies, for example, could use their own administrative data and those of other parties to optimise contracts with care providers, to bring the provision of care more in line with its demand. They can also use those data to directly offer insurance policies to certain people and avoid the riskier insurance seekers.[119] In addition,

[116] Link to the study by Ponemon.
[117] For example, see the security policy of Philips Health Care.
[118] For example, the Apple Watch can be used to detect signs of heart disease. See this article.
[119] Insurance companies are legally obligated to accept every new applicant for a basic health insurance policy. However, they can focus their marketing instruments directly on certain population groups.

health data may also be part of personal profiles that are used, for example, for targeted advertisements, or for directly approaching voters in the run up to elections and referenda (Section 2.1).

Another risk that may be created from all the new ways of applying health data, is that the process of collecting and sharing those data is not sufficiently transparent, particularly when this is done by companies outside the EU. In such cases, supervisory bodies may not have sufficient insight into the security of those data flows.

4.4 Policy options

Under current policy, associations of health care providers (*zorgkoepels*) often play an initiating role. For example, in collaboration with such associations, the NCSC set up an Information Sharing and Analysis Centre (ISAC) to exchange information about cyber security. Furthermore, in late 2016, the Dutch Association of Mental Health and Addiction Care (GGZ Nederland), the Dutch association for detergents, maintenance products and disinfectants (NVZ) and the Netherlands Federation of University Medical Centres (NFU) took the initiative to set up the Computer Emergency Response Team for dealing with acute cyber security problems in health care (Z-CERT).

The health-care ISAC and Z-CERT collaborations could directly increase cyber security in the health care sector. In addition, policymakers have three types of instruments to enhance cyber security:

- mandatory standards;
- supervision;
- secure public services, such as ICT infrastructure.

Mandatory standards may form a basis for providing data security, as they enhance access to security expertise. In addition, they facilitate secure data exchange between organisations. As long as the standard is voluntary, there is no additional incentive to protect data. In 2015, for example, only 56% of Dutch hospitals were in compliance with the standard for data security in health care (NEN-7510[120]). The share of hospitals actually certified according to the standard is even lower, with 21% or less.[121] Since May 2017, compliance with this NEN standard in the Netherlands is mandatory for organisations in the health care sector that wish to use Citizen Service Numbers (BSN).[122] The DPA is responsible for the supervision of this compliance

[120] Since May 2016, there is a new version of the NEN-7510 standard that will be implemented in October 2017. This new standard is intended to be more in line with international standards.
[121] Source: RIVM. (link)
[122] Regulation about the use of Citizen Service Numbers in health care (link).

where this is related to the protection of personal data, and the NZA supervises this when related to regulations regarding the health insurance market.[123]

Because NEN-7510 is related to a certain part of data security in the health care sector,[124] the government is able to investigate whether additional standards, for example, for network quality and data integrity, could also become mandatory. Furthermore, it could be investigated whether the supervision of health care data systems could be organised in a more integral manner.[125]

The use of standards cannot offer sufficient security by itself, as threats to cyber security are often unpredictable; even well-designed data systems may have serious vulnerabilities. Cyber criminals and state-sponsored hackers continue to innovate. Because of that strategic interaction, the use of standards in cyber security offers less certainty than in road safety or health care itself. Therefore, supervisory bodies in cyber security cannot fully rely on certification by third parties. To be effective, they will need to gain technical expertise in data security, themselves.

Small organisations, such as primary health care providers, are currently using several systems, simultaneously. Mandatory compliance with standards in data security may lead to the convergence into a small number of private and public systems, as data exchange between systems becomes more expensive. This does pose the question of whether it would be desirable for data exchange to become dependent on a single, private company. In cases of dependence, the government may consider to obligate gatekeepers and care providers to exchange data via a secure public infrastructure (e.g. the LSP platform).

A public infrastructure for the exchange of data has the added advantages that also small health care organisations are able to simply comply with the standards for data security, and that citizens are provided with insight into who has access to their data. If it is easy for health care users to determine what happens with their data, this may provide additional incentive to care providers to handle those data in a secure manner. The LSP platform, currently, already provides patients with the possibility of knowing who has access to their data, but of course only when these data are exchanged via this platform.

[123] Articles 13 and 15 of the Dutch Act about the use of Citizen Service Numbers in health care (Wet gebruik burgerservicenummer in de zorg) (link).
[124] The following areas of data security are not within the subject area and fields of application that apply to the Dutch NEN 7510-1 and NEN 7510-2 standard: a) methodologies and statistical testing for an effective anonymisation of personal health data; b) methodologies for pseudonymisation of personal health data; c) the network quality of service provision and methods for measuring the availability of networks used in health care informatics; and d) data quality (distinguishing data integrity).
[125] Currently, the IGZ, DPA and NZa, together, are responsible for the supervision of different aspects of the same data system.

Mandatory use of a public infrastructure carries two risks. The first being that infrastructure failure leads to large-scale problems — the risk of *single point of failure.* This risk could be mitigated by pluriformity[126] and local organisation — for example, using blockchain technology. The second risk is that when a mandatory infrastructure is not designed to be user-friendly, care providers will use unsecure alternatives. A strategy to prevent such a risk would be to first stimulate voluntary use of a public infrastructure by investing in user-friendliness.

Reports of data leaks and incidents at municipalities show that the risks of data leaks, here, particularly concern local administrative data flows. The government, therefore, could investigate whether the advantage of a mandatory public infrastructure in health care would outweigh the risks. A public infrastructure may increase cyber security — and therefore also privacy — in the health care sector, as well as improve the quality of the health care provided.

[126] Citizens, currently, can already log on to government and health care organisation infrastructure, in various ways; for example, see here.

Publisher:

CPB Netherlands Bureau for Economic Policy Analysis
P.O. Box 80510 | 2508 GM The Hague
T (088) 9846 000

July 2017