Multidisciplinary aspects of digital security

Natascha van Duuren, Jan Nienhuis, Victor de Pous

knvi

Multidisciplinary Aspects of Digital Security

Natascha van Duuren LLM
Jan Nienhuis BSc CISSP
Victor de Pous LLM (eds.)

Multidisciplinary aspects of Digital Security

Multidisciplinary aspects of Digital Security

Natascha van Duuren
Jan Nienhuis and
Victor de Pous (eds.)

knvi

ISBN: 978-90-9036671-5
NUR: 820

COMPETENS

IT SKILLS FUND

The Competens Foundation, Skillsfund for IT, financed the translation of this publication. This foundation’s mission is to support initiatives to strengthen IT skills for growth and innovation in the Netherlands. This publication adds to that mission, because it supports IT skills growth by sharing insights, experiences and best practices gained around digital security from a multidisciplinary perspective.

ifip

The International Federation for Information Processing - is the global non-profit federation of societies of ICT professionals that aims at achieving a worldwide professional and socially responsible development and application of information and communication technologies.

Contents

Foreword

With the collection 'Multidisciplinary aspects of digital security', the Netherlands Association of Information Professionals (KNVI) once again shows the value of its professionals' focal area. Authors from a range of professions in information technology, information management and information governance have examined and described the topic from different angles of approach. This is thus a fine example,, like with many other social topics, of how to make sense of different trends in society by cooperation, exchange of information and through sharing knowledge. The professional organisation also conveys that in this collection, another fine addition to the series of books published by the KNVI Special Interest Group IT & Law.

With this collection, the KNVI also defines the term 'digital security' and outlines a more over-arching picture of all its aspects. Cybersecurity and information security are fields that have been under development for some time, and are increasingly attracting the attention of administrators and decision makers. And rightly so, because the underlying themes can no longer be ignored. There is legislation for complying with cybersecurity and information security. Organisations, processes and employees must be able to work safely and handle their data securely. But more is needed, society needs guarantees that there will be no accidents in the area of digital security. Can you count on businesses giving you secure access to their online shops? Are your devices actually secure, and does everyone get sufficient - customised - information to structure their lives? And have the implications for your personal life been taken into account? Asking these questions also means answering them. We even venture the assertion that the answer is 'not yet', or sometimes 'no'. And that is worrying.

Many professionals are familiar with the internal programs for employees focusing on digital and information security. Many readers will have completed a GDPR course, the results of which are stored in their personnel file. Don't open any phishing emails, keep your desk clean and protect the organisation's reputation are the standard takeaways. Bricks, Bytes and Behaviour as a framework for the new way of working. The framework-setting Government Information Security Baseline

(BIO) and the relevant ISO standards already take us a long way. You will also encounter an explanation of the aforementioned terms in this collection. Along with the necessary broader perspective as well. Because it is important to look at the broad societal significance of digital security.

Did you know, for example, that in countries around us, digitally attacking businesses and other governments is a 'regular' office job for many people? That household breadwinners work at an office 9 to 5 carrying out cyber attacks? And that if you pay the ransom, the helpdesk will help you unlock your systems, and give you a tip as to where the leak in the software was? You just won't receive any customer satisfaction survey afterwards. In the big Security Operations Control rooms (SOCs), you can see the millions(!) of attacks lighting up in digital flashes of light on the screens. That is still somewhat manageable because they are visible.[1]

It becomes more difficult if two freight lorries close off the A12 or the A15 and bring logistics Netherlands to a standstill (thus disrupting 50% of Europe's imports and exports). Or if a Chinese port is offline for a week, resulting in furniture still not being delivered to furniture stores months later. Or if the atomic clock of our electricity grid deviates by a microsecond and the entire grid collapses, and all the smaller power plants in Europe fly out of their housing like the wires in an old-fashioned fuse box.[2] Or if a pipeline is shut off remotely and half a continent no longer receives any petrol.[3] Or if government organisations combine your data, without your knowledge, and use these for various convenient applications, like the social score worked out in China to the last detail. But that could never happen in the Netherlands, right? Or if you use an app to pay an online business, only to find your credit card maxed out thereafter. Only then does digital security's role as one of the greatest threats to global society become tangible.[4] In the top five after political and economic instability, extreme heat and the collapse of ecosystems.[5]

[1] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[2] https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html

[3] https://www.theguardian.com/technology/2021/jun/17/ransomware-working-from-home-russia

[4] https://www.oliverwyman.com/our-expertise/insights/2020/jan/globalrisks2020.html

[5] https://ourworldindata.org/natural-disasters

Attention to digital security is sorely needed - knowing that other fields and professions are also developing and moving ahead in the direction they have taken. It is not yet the case that machines are demanding rights, for example the right to never be switched off, as Moshe Hoffman of MIT expects. And it is true: our BIO framework is also not yet prepared for these kinds of developments. But the start of that path has now indeed been levelled, and we, as humans, have done that ourselves - an example of Smart Humanity like no other:[6] 'We built "them", but we do not understand them', say Jon Kleinberg and Sendhil Mullainathan in relation to computers and their programs.[7] So it is about time to make society aware of its responsibility to become familiar with and competent in digital security. High time to call on government and politics to put the topic even higher on the policy agenda and political agenda. And to task the professionals in the broader field with supporting colleagues, administrators and decision makers and society as much as possible in this respect.

Paul Baak & Wouter Bronsgeest
(co-chairs of KNVI)

[6] Bronsgeest, W.L., Waart, S. de (eds.), Smart Humanity, de mens met 1-0 op voorsprong, Uitgeverij Nubiz, Hilversum, 2020

[7] Brockman, J. (ed.), Machines die denken, invloedrijke denkers over de komst van kunstmatige intelligentie, Maven Publishing, 2016

Editorial

What started with a few basic measures to protect computer systems and the data they process automatically against inadvertent uncertain incidents, such as power outages and fire and water damage, has grown into an advanced, constant battle to make - and keep - information, systems and infrastructure strong enough to withstand both inadvertent and deliberate digital threats, especially computer crime. It goes without saying that digital security is vital today. Without ICT, everything would more or less come to a standstill. A society that is becoming increasingly dependent on digital processes and chains, while analogue fall-back options are in many cases no longer available, *must* take protective measures. This then means that literally everyone must take into account the digital threats and ways of mitigating these risks.

According to the National Cyber Security Centre (NCSC), which, together with the National Coordinator for Security and Counterterrorism (NCTV), set up the Cyber Security Assessment Netherlands 2021, cooperation and knowledge sharing are indispensable in this context. Vulnerabilities and threats in the digital domain must be tackled from a broad perspective.

This message was well received by the Royal Association of Information Professionals (KNVI). For decades, the organisation and its predecessors have been working on knowledge development and sharing, including on information security. In this, a multidisciplinary approach has been expressly chosen each time, which is also evident from the unique series of books[8] to which this collection belongs.

While the NCSC opts for ‘cybersecurity’, without wishing to engage in a discussion of scientific principles, we sometimes use - in the title as well as to some extent in

[8] N.H.A. van Duuren and V.A. de Pous (eds.), *Multidisciplinaire aspecten van blockchain*, Amsterdam, 2019, N.H.A. van Duuren and V.A. de Pous (eds.), *Multidisciplinaire aspecten van artificial intelligence*, Amsterdam, 2020 and N.H.A. van Duuren and V.A. de Pous (eds.), *Multidisciplinaire aspecten van COVID-19 apps*, Amsterdam, 2021.

the separate chapters - the term ‘digital security’; a fundamentally broader notion that also encompasses offline media and information and which, for example, includes measures relating to the quality of digitalisation.

This collection therefore envisages providing insight into the broader aspects of the security of digitalisation and the status quo in that domain and fostering more advanced awareness and additional knowledge among the target group: professionals (irrespective of expertise, work area or industry), administrators at government organisations and politicians. Digital security is also a perfect example of a topic that requires a broad-based multidisciplinary approach. After all, it is important to avoid taking a strictly technical or legal view of the countless issues and challenges related to security measures and risk management in and for the digital domain. Only a broad, multidisciplinary approach can increase our digital resilience, limit the effects of digital disasters and prevent social, sectoral, organisational and/or personal disruption resulting from these incidents.

We thank all the authors who contributed. The contributions were written in a personal capacity and were deliberately kept concise in nature. The chapters contain valuable analyses and suggestions, but emphatically do not provide advice for concrete cases. They are based on current knowledge and the current state of affairs. We are thoroughly aware that developments in this domain are taking place quickly and that this will inevitably mean that certain insights could be outdated to some extent in the foreseeable future and will require revision. We are convinced that this book will contribute to multidisciplinary knowledge sharing on network and information security, in particular for the target group mentioned. We also thank the international federation of national associations for information processing (IFIP) and Competens for their financial contribution to this publication.

Natascha van Duuren, Victor de Pous and Jan Nienhuis

1. Digital security – a development that never stops

Jan Nienhuis

Although we have only become acquainted with digital abuses on a large scale over the past decades, these are not a new phenomenon. The development of digital technology took off after the Second World War. 1969 saw the creation of ARPANET, which for the first time in history connected computers at a great distance from each other in a shared network. Within two years, the first computer virus emerged, along with the corresponding antivirus software: Creeper and Reaper. They were the result of an academic exercise and did no real harm. But just as children learn and develop through play, the first digital viruses also laid a foundation. It is interesting to see how we evolved from this kind of beginning to a world of ransomware and cyber warfare.

Origins

During the 1970s and beginning of the 1980s, threats in the digital domain were still manageable. The biggest threat concerned data loss and unauthorised access. An early example of computer abuse in the Netherlands occurred in 1972. 'The removal of computer tapes and especially the reporting in the newspaper De Telegraaf gave the Netherlands a wake-up call when the head of computerisation at a chemical company at Rozenburg made off with all the available tapes, including the back-ups, and later offered these for sale to his employer'.[9]

Passwords had already been in use for more than ten years at that point, but in the mid-1970s people started to worry about the security of computers and software. The biggest threat was malicious insiders, but with the development of telecommunications, the threat from outside grew as well. From 1967, the US Defence Science Board was already working on the security of computers with an external connection. Further initiatives in 1972, 1973 and 1977 ultimately

[9] V.A. de Pous, *Recht op elektronische technologie 1982-2003*, contained in the collection Eerlijk zullen we alles delen, 2003 http://www.informationdynamics.nl/pwisse/pdf/FS_Eerlijk_Zullen_We_Alles_Delen.pdf, 2008 GBO.Overheid

culminated in the 1985 publication of the so-called ‘Orange Book’ by the US Department of Defence.[10]

Hacking also began to take on serious dimensions in the 1970s, and the concerns about that resulted not only in more robust software. In 1979, Kevin Mitnick (16 years old at the time) hacked into an important computer at Digital Equipment Corp. (DEC). This and subsequent breaches ultimately landed him on the FBI’s most wanted list.[11] During that same time period, hacker David Scott Lewis provided the inspiration for the film Wargames (which came out in 1983)[12], in which a computer of NORAD[13] is hacked - by no means an impossibility at that time.

In 1986, German national Markus Hess used computers of the University of Bremen to break into the system of Lawrence Berkeley Laboratory. From there he obtained access to ARPANET and MILNET. Hundreds of computers were hit and information was sold to the KGB. Hess was arrested and convicted of espionage.[14] These types of incidents prompted security to be taken increasingly seriously. A race between ‘good’ and ‘evil’ forces arose.

Cryptography

In 1995, Netscape introduced the Secure Sockets Layer (SSL). This protocol encrypted the content of internet traffic so that only the recipient could decipher the information. This made advanced cryptography accessible for all. Secret codes have been around since antiquity. The Caesar rotation cipher, for instance (in which the letters of the message are replaced with a letter located a fixed number of places further on in the alphabet), which takes its name from Julius Caesar, who used it to send secret messages during his military campaigns. Modern cryptography is based on mathematical comparisons. Encryption algorithms can be roughly divided into three main groups: symmetric encryption, asymmetric encryption and hash functions.

The strength of symmetric encryption is highly dependent on the algorithm. A simple cipher (such as the Caesar rotation cipher) is easy to find and

[10] https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf

[11] https://www.mitnicksecurity.com/about-kevin-mitnick-mitnick-security

[12] https://venturebeat.com/2008/08/12/a-qa-that-is-25-years-late-david-scott-lewis-the-inspiration-behind-the-film-war-games/

[13] North American Aerospace Defense Command

[14] https://peoplepill.com/people/markus-hess-1

to crack. The Enigma, used to encrypt German communications during the Second World War, employed multiple variable keys on top of each other. And yet this code, too, was cracked. Both the Polish[15] and British secret services (in which Alan Turing played an important role) were able to figure out the keys and thus decipher secret German messages.[16] Modern symmetric encryption algorithms are practically undecipherable if the key is unknown. They can also be rapidly calculated. But how do you exchange the key securely?

Asymmetric cryptography uses two keys: a public key and a secret, private key. Information converted using the one key can only be deciphered with the other key. The calculations are complex and time consuming, however. That is why this method is often used to exchange small encoded quantities of information, such as symmetric keys.[17] Since Diffie and Hellman laid the foundation in 1976 for modern asymmetric cryptography,[18] various algorithms have been developed. The most commonly used (RSA (1977), DSA (1991), ECC (1985)[19]) have to date proved (almost) uncrackable in their current version. New developments are needed, however, more on this later.

Hash functions are a special form of one-way encryption. A hash algorithm computes a unique output of fixed length from random input. Change one character in the source and the result of the hash changes drastically. A hash cannot be traced back to the original, however. These algorithms work fast and are often used as a means of verification.

The future: quantum computing

A game-changer in computing could be the quantum computer. They will probably not replace normal computers, but they are unequalled in optimising and processing mathematical data.[20] They are so good, in fact, that the two large prime numbers that form the basis of, among others, the RSA algorithm can be quickly

[15] Budiansky, S. Battle of Wits: The Complete Story of Codebreaking in World War II by Stephen Budiansky, New York: Free Press, 2000

[16] Winterbotham, F.W. *The Ultra Secret*, London: Futura, 1975

[17] Nienhuis, J. Cybersecurity-perspectief van Blockchain *Multidisciplinaire aspecten van Blockchain*, Amsterdam: DeLex, 2019

[18] Diffie, W. and Hellman, M. New Directions in Cryptography *IEEE Transactions on Information Theory* 22, 644-654, 1976.

[19] https://www.sslcertificaten.nl/support/Terminologie/Algoritmes

[20] https://www.kaspersky.nl/blog/rsa-postquantum-howto/25081/

discovered, meaning this form of encryption cannot be considered quantum-safe.[21] Symmetric encryption algorithms with a long enough key are indeed considered quantum-safe. Hash functions (to the extent not already cracked) with sufficient key length are also quantum-safe.[22]

Quantum computers are still in their infancy, but efforts are under way to find the breakthrough that will make more powerful ones possible. These could arrive next year, in ten years' time, or perhaps never. Still it is necessary to already be thinking about forms of cryptography that can resist new mathematical wonders.[23] Various methods to serve as replacement are under development, including Error code correction, Lattice-based Cryptography and Isogeny Elliptic Curve-based Cryptography (IECC).

Virus age

As we have seen, computer viruses have been around as long as computer networks.[24] Since its introduction in 1981,[25] the personal computer has developed into an increasingly powerful and vulnerable device. Local networks were created to connect them (IBM Token ring around 1984[26] and Ethernet II in 1985[27]). These networks were in turn connected to ARPANET - which became the backbone of the internet at the end of the decade. Files and programs were exchanged on floppy disks (remember those?). It proved an ideal environment for malicious code to spread. Email emerged as a revolution in communication, but also as a new platform for spreading malicious code. The virus age had begun.

Commercial antivirus software quickly followed. In 1987, John McAfee's business established itself with its VirusScan product, IBM started developing its own antivirus product after its office in Belgium was hit hard by infection with the Cascade virus.[28] A year later, specialised businesses around the globe were working on detecting and neutralising computer viruses. A race between people creating

[21] https://www.youtube.com/watch?v=lvTqbM5Dq4Q

[22] Https://www.agconnect.nl/artikel/kwantumcomputer-bedreigt-straks-encryptie-kom-nu-actie

[23] https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography

[24] https://corewar.co.uk/creeper.htm

[25] https://nl.wikipedia.org/wiki/Personal_computer

[26] https://en.wikipedia.org/wiki/Token_Ring

[27] Liere, J. van. *Ethernet door dik en dun*, Gouda, 1997

[28] https://encyclopedia.kaspersky.com/knowledge/year-1987/

viruses and those fighting them arose and continues to this day. The viruses became more and more malicious and their name is legion. A new threat reared its head with the development of the World Wide Web: there was henceforth no need to copy or download files - a visit to an infected website would do the trick.[29]

Traditional antivirus products were no longer sufficient. The number of virus signatures had grown from a few hundred to several million, with ever new strike areas being discovered and abused. 'Endpoint protection' made its entrance, with new ways of identifying and eliminating groups of malware (malicious software). These platforms slowly improved. But it was not enough.

In 2017, the world was shook up by WannaCry, which exploited a vulnerability in the SMB protocol (used to share files on the network). It proved to usher in a new form of digital crime. Ransomware has since been one of the most feared threats and will most likely remain so for the time being.[30]

Threat hunting and artificial intelligence

It is difficult to get an overview of the multitude of digital threats. Moreover, the playing field is constantly changing. Hostage taking by cryptolockers is being approached extremely professionally; DDoS attacks and malware can simply be ordered online. Every reason for the security industry to join forces. Information on threats is exchanged (information on defending against them is a trade secret). Known hacker networks are monitored closely. Ethical hackers use their skills to pinpoint weaknesses in order to help secure systems better.[31] Big Security Operating Centres (SOCs) sign up as many customers as possible to make the major investments and efforts profitable, but also to have large volumes of traffic to analyse. This ensures that a large volume of threat information is actively amassed.

Artificial intelligence (AI) and machine learning are increasingly being used to analyse all these data.[32] These systems seek out deviations in the normal traffic patterns and then alert the human expert who assesses whether there is a serious alarm or a false positive. The automated detection is becoming better and better, and automated response is already a realistic option. Various SIEM systems offer

[29] https://encyclopedia.kaspersky.com/knowledge/year-2001/

[30] https://www.nctv.nl/binaries/nctv/documenten/publicaties/2020/06/29/cybersecuritybeeld-nederland-2020/Cybersecuritybeeld+Nederland+2020.pdf

[31] Hof, C. van 't. *Cyberellende was nog nooit zo leuk*, Rotterdam: Tek Tok, 2021

[32] In relation to this generally, see: Natascha van Duuren and Victor de Pous, *Multidisciplinaire aspecten van artificial intelligence*, 2020.

the possibility of, for instance, automatically blocking suspicious traffic and isolating the organisation's own computers that are affected for further investigation.[33] AI can also help predict security errors by monitoring social media. A study by the University of Ohio achieved an astonishingly accurate result with this.[34]

State actors

Organisations such as the US National Security Agency (NSA), hacker collectives associated with the Russian government, the Israeli secret service, state-backed Chinese and Korean hackers and, last but not least, our own intelligence services and police use the same techniques as hackers to gain control of information, spread information and misinformation, sabotage technological developments and sometimes disrupt entire societies. Examples abound: an (unproven) claim that Boeing secrets were passed on to Airbus by the Chinese government[35], the attack on an Iranian nuclear complex (the Stuxnet virus, discovered in 2010[36]), an advanced attack on the Ukrainian energy network[37] in 2016 that had far-reaching societal consequences.

This has given rise to a new form of warfare. It depends less on military power, and more on the ability to manipulate and sabotage a society.[25] A country that is at odds with itself and economically weakened does not pose a great threat to its neighbours. An aggressive neighbour could see it as easier prey. This realisation prompted European legislation - implemented in the Netherlands in, inter alia, the Wbni (Network and Information Systems (Protection) Act) and the designation of vital sectors and businesses.[38] Time will tell whether this is enough.

[33] https://www.ibm.com/security/intelligent-orchestration, https://www.darktrace.com/en/?utm_source=cpc-google&utm_medium=search&utm_campaign=campaign_brand_benelux&gclid=EAIaIQobChMIiPaC8of18wIVCbTtCh1n6gsgEAAYASAAEgIlxfD_BwE, https://swimlane.com/solutions/security-automation-and-orchestration

[34] https://arxiv.org/pdf/1902.10680.pdf

[35] https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/

[36] https://spectrum.ieee.org/the-real-story-of-stuxnet

[37] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[38] https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni

In conclusion

As far back in human history as we can look, people, businesses, generals and governments have worked to protect certain information and there have been criminals, competitors, spies and diplomats working to get a hold of it. The digital era has created new possibilities for achieving these goals. Cybersecurity is a constantly evolving playing field, in which advanced technology supports a good organisation. Unfortunately, no technology is 100% effective and every organisation makes mistakes. Incidents will always occur, therefore, even if digital security is a priority on the strategic agenda.

One of the starting points of a security strategy should therefore be that the system may already be compromised. In that case, effectively responding to an incident is suddenly just as important as preventing it.

Lessons from history

- Everything that can be done will happen at some point. Even if it is not permitted, sooner or later someone will try it.
- Digital security can better be viewed as a process rather than a project.
- The digital threat assessment is constantly changing. The value of information also often changes over the course of time. Suitable measures change too, therefore.
- Digital security incidents happen, despite all the measures taken. A well prepared response helps with the recovery.

2. Aspects of digital security law

Victor de Pous

Privacy law puts mandatory, risk-based security measures in the spotlight, but digital security law covers a wider and more diverse field. ‘Breaking through security’, for instance, is part of the offence of computer hacking, while the circumvention of technical facilities is, in principle, criminalised in copyright law. In addition, encryption technology may be subject to export rules. Those who do not keep their know-how confidential miss out on the protection of the Trade Secrets Act. Aside from a statutory or contractual duty of care, a criminal offence or a condition for exercising rights, digital security affects fundamental rights. Are the police allowed to press a suspect’s thumb on his or her smartphone to unlock information? Yet another aspect concerns the question of how software producer, user and ethical hacker should deal with security vulnerabilities. Is it desirable to make it a crime to pay up when held hostage by ransomware? Will the use of encryption nonetheless be regulated after thirty years of debate? Rarely has a specialist area of law become so widespread, so rapidly developing and so crucial to society.

National security

The second Rutte cabinet was ‘not amused’ when in late November 2015 it was surprisingly revealed that the British NCC Group had bought Fox-IT Holding BV for 133 million euros.[39] This Dutch company provides digital security services to a large number of government organisations, including (the encryption for) the security of our state secrets. While in an effort to prevent undesirable control in the digital sector, the Telecommunications Act was only recently amended[40] as a generic protective measure, to include a preventive notification requirement, the

[39] https://fd.nl/ondernemen/1128389/security-specialist-fox-it-voor-recordbedrag-verkocht, en https://www.nrc.nl/nieuws/2017/01/24/wakker-geschrokken-na-britse-overname-6381515-a1542736.

[40] New chapter 14a in the Telecommunications Act. The Telecommunication Sector (Undesirable Control) Act came into force on 1 October 2020.

government was left with little alternative but to make special continuity and protection arrangements.

'These agreements are based on a number of conditions, such as housing all crypto-related contracts at a separate business unit Fox Crypto BV and segregating the ICT systems of Fox Crypto BV and the other units of Fox-IT,' Minister Ollongren (Home Affairs) reiterated in 2020 in response to turmoil in the boardroom, about which parliamentary questions had been asked.[41] The Civil Service Information Security (Classified Information) Decree (VIRBI 2013) also applies to people, equipment, information and the physical location of Fox Crypto.[42]

What struck us earlier is that the primary issue is not being debated. What is the State *indeed allowed* to outsource in the digital domain?[43] The issue of outsourcing is each time limited to setting criteria for implementation and the contractor. That, however, is step two. In the meantime, the Netherlands has lost a large part of its digital sovereignty, the Cyber Security Council (CSR) warned on 14 May 2021.[44] One of the concrete issues that now demands action is the 'implementation of a digital autonomy cybersecurity assessment framework'.

Security of smart devices

Another issue of control is playing out at the micro level. Just think of all the products containing a digital component. From a smart energy meter to a doorbell. It hardly needs explaining that such a device requires an adequate level of security at the time of first delivery as well as during its economic life, given the legitimate interest of the user alone. Practice shows a different picture. The focus is evidently more on the consumer market than on 'operational technology' (OT). This consists of sensors and technology for the direct monitoring and/or control of industrial equipment, assets, processes and events. To give a specific example, our flood control systems. Or traffic control systems.

[41] https://www.rijksoverheid.nl/documenten/kamerstukken/2020/07/01/beantwoording-kamervragen-over-schorsing-directieleden-fox-it

[42] Decision of the Prime Minister, Minister of General Affairs of 1 June 2013, no. 3124134, containing the Civil Service Information Security (Classified Information) Decree 2013.

[43] See, for instance: V.A. de Pous, *Geen enquête maar sourcingsbeleid* in https://www.agconnect.nl/blog/geen-enquete-maar-sourcingsbeleid.

[44] Https://www.cybersecurityraad.nl/actueel/nieuws/2021/05/14/%e2%80%98digitale-autonomie-nederland-staat-onder-druk%e2%80%99

For years, the supervisory authority Agentschap Telecom has been repeatedly sounding the alarm about the lack of digital security for devices that are wirelessly connected to the internet, and in 2020 it finally drew up its own 'eight simple requirements' for improvement, plus a contact point for unsafe devices.[45] This is also the opinion of the Dutch Consumers' Association. The association tried to enforce at law a better software security update policy at Samsung for - low-end - Android smartphones, but was denied twice in court.[46] After a long delay, European legislation will be introduced setting minimum digital security requirements for smart, wireless devices. The EU Radio Equipment Directive (RED; 2014/53EU) is being amended for this purpose, but the amendment will only enter into force in mid-2024.[47]

A somewhat neglected situation is that when the customer wants to maintain or connect the - secured - digital product himself. Are these actions legally permissible and factually possible?[48] And with what consequences, such as for warranty and maintenance by or on behalf of the manufacturer? A practical example. In order to be able to install a complementary hydrogen system in his second-hand Tesla Model S to increase the range, a Dutch owner needed to gain access to secured information technology. He managed to obtain this information, but the manufacturer disapproved of the action, 'hacked back' and declared the car stolen. In turn, the owner changed the software again so that the manufacturer could no longer make telemetric contact with the car.[49]

[45] https://www.agentschaptelecom.nl/actueel/nieuws/2020/08/26/acht-simpele-eisen-kunnen-de-cyberveiligheid-van-%E2%80%98slimme-apparatuur%E2%80%99-sterk-verbeteren

[46] *Consumentenbond v Samsung Electronics Benelux bv*, Amsterdam District Court, 8 March 2016, ECLI:NL:RBAMS:2016:1175 and *Consumentenbond v Samsung electronics Benelux bv*, The Hague District Court, 30 May 2018, ECLI:NL:RBDHA:2018:6310

[47] https://www.rijksoverheid.nl/actueel/nieuws/2021/10/29/minimumeisen-aan-digitale-veiligheid-slimme-apparaten

[48] European software law (Software Protection Directive) also plays a role here. It gives the licensee a legal right to error correction (included in Section 45j of the Copyright Act) and a right to interoperability (Section 45m of the Copyright Act), while Section 29a(4) of the Copyright Act provides exceptions to the criminalisation of circumventing effective 'technical provisions' intended to prevent abuse.

[49] https://futurism.com/hacked-tesla-drives-hydrogen and https://www.carblogger.nl/deze-hesla-komt-na-3-minuten-tanken-1100-km-ver/

Embedding in legislation

As early as 1987, there was a motley collection of regulations with digital security as a requirement.[50] Today, the law has both old, as included in the State Secrets Protection Act, and newer information security regulations. This often involves dealing with the general problem of a lack of confidentiality in data processing. Measures should prevent incidents or limit their consequences. If you take a step back, another issue that comes to mind is that of safeguarding the continuity and reliability of services and, ultimately, public interests. *This digital duty of care trend is continuing.*

The General Data Protection Regulation (GDPR), which lays down the general rule that the controller and processor must take 'appropriate technical and organisational measures' to 'ensure a level of security appropriate to the risk' is now well known.[51] On a closer look, the European privacy legislation contains a series of security obligations, including privacy by design.

We find digital security law codified in many and various regulations. To name just a few: The Telecommunications Act, Medical Treatment Contracts Act, Police Files Act, EU Regulation eIDAS (on electronic identification and trust services for electronic transactions), State Secrets Protection Act, Civil Service Information Security Regulation (VIR), Civil Service Information Security (Classified Information) Decree (VIRBI), EU Network and Information Security Directive (NIS), EU Trade Secrets Directive, EU Medical Devices Regulation, Penal Code, Archives Act, Government Information (Public Access) Act and Copyright Act. It also follows from this brief summary that the legal framework goes beyond security *requirements*, which in turn go beyond the technology for and processing of *personal data*.

European cybersecurity legislation

The first European Cybersecurity Act came into force on 1 August 2016 in the form of the NIS Directive. On 29 May 2018, the Lower House unanimously adopted the Dutch law based on this Act through a substantive amendment and name change to the already existing Data Processing and Notification Obligation Cybersecurity

[50] V.A. de Pous, Some remarks on regulations in which security of computer systems and/or data and/or data files and/or communication of data has been made a statutory requirement, included as Annex IV in Report of the Computer Crime Commission, Information Technology and Criminal Law, 1987. This study was also published as a separate publication by the Expertise Centre Foundation (Stichting het Expertise Centrum).

[51] Article 32(1) GDPR.

Act, which had entered into force shortly before (1 January 2018). In addition to the Network and Information Systems (Security) Act (Wbni), which entered into force on 9 November 2018 and for new notification requirements on 1 January 2019,[52] Dutch law has a decree of the same name (Bbni). The order in council designates providers of an essential service as well as other vital service providers, the digital service providers or DSPs.[53]

All these parties are required to take appropriate measures to manage security risks, minimise the consequences of incidents and to report serious incidents. Not even three years later, the European Commission is already working on a revision. This proposal extends duties of care and notification, widens the scope to include new sectors (waste water, public services and space travel) and sub-sectors of existing industries, and also aims to achieve closer European cooperation.[54]

Before that happens, the Wbni will be amended autonomously by the Netherlands. Organisations that are not a vital service provider and are also not part of the national government will have access to more threat and incident information about their own network and information systems.[55] Please note. The availability of this detailed information provision may cause an adverse effect. Those who subsequently fail to take action and whose omissions cause damage will not be able to invoke force majeure as easily in liability proceedings.

Encryption

The thirty-years' 'encryption war' has yet to end. The political battle wages again and again.[56] Governments that want access to encrypted data and data traffic find critics from different backgrounds - so not only privacy activists - radically opposed. In the Netherlands as well. We do, however, note changing views. For example, the third Lubbers cabinet wanted to prohibit under criminal law the offering, provision, possession and application of cryptography in telecommunications, unless the user of the encryption had a licence or authorisation from the government. That was the

[52] https://zoek.officielebekendmakingen.nl/stb-2018-387.html

[53] https://zoek.officielebekendmakingen.nl/stb-2018-388.html

[54] https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2

[55] https://www.internetconsultatie.nl/wijzigingwbni

[56] https://en.wikipedia.org/wiki/Crypto_Wars

gist of a *preliminary draft* law that was leaked in reasonable likelihood on purpose.[57] That was March 1994. Partly under pressure from employers' organization VNO and the Data Protection Authority, the blueprint was withdrawn three months later.

But in March 1996, at a conference in Boston, Data Protection Authority chair Peter Hustinx welcomed initiatives from the White House and the OECD for a 'socially acceptable solution' to the use of strong encryption systems, so that investigators could still unlock the information.[58] Two years later, the same supervisory body advised the government 'strongly' against restricting the use of encryption.[59] At the moment, the Netherlands is still adhering to the firm standpoint taken by the second Rutte cabinet on 4 January 2016. There will be *no* 'restrictive legal measures regarding the development, availability and use of encryption in the Netherlands'.[60]

The Council of the EU takes a different view. In its - non-binding - resolution of 14 December 2020, it states that authorities must be able to gain access to encrypted data in certain cases, such as for the purpose of combating terrorism, organised crime and child abuse. [61] In the words of the Council: 'security through encryption and security despite encryption'. Also striking: according to the Dutch Surpreme Court , the police may press the thumb of a refusing suspect onto his iPhone to unlock information. [62]

Broad spectrum

Digital security law is characterised by relevance, diversity and dynamism. At a hearing, the US Congress gauged sentiment on a legal prohibition on making payment in the event of a ransomware infection; the FBI and some security

[57] https://www.nrc.nl/nieuws/1994/03/24/wetsvoorstel-tegen-elektronische-geheimtaal-7218574-a137201

[58] In the form of a multilateral key escrow treaty that stipulates the decryption keys must be handed over and stored with an independent third party (comparable with a software escrow).

[59] https://autoriteitpersoonsgegevens.nl/nl/nieuws/encryptie-niet-aan-banden-leggen-%C2%A0

[60] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015

[61] https://www.consilium.europa.eu/en/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/

[62] Supreme Court, 9 February 2021, ECLI:NL:HR:2021:202

companies are in any event opposed.[63] According to the Belgian political party N-VA, espionage risks compel a ban on Chinese smartphones for people working in 'sensitive sectors'.[64] Lithuania goes a step further and advises consumers simply not to buy Xiaomi phones. These are new examples of the advancing geopolitics of digitalisation.[65] We already saw this in the Netherlands with regard to 'sensitive company takeovers' or attempted takeovers; Fox-IT in 2015 and KPN by América Móvil in 2013, respectively. Meanwhile, Huawei's position remains under pressure regarding the security of telecommunications networks, while in May 2018 the central government decided to phase out Russian Kaspersky Lab's anti-virus software due to security concerns.[66]

When taking a broad view, let's not forget the governmental *plans*, such as the National Digital Crisis Plan,[67] the Dutch Digitalisation Strategy (NDS) 2021,[68] the National Cybersecurity Agenda of 21 April 2018, which includes seven 'solid ambitions'[69] and the brand new i-Strategy.[70] And of course, Europe also imposes many digital security policies.[71]

Liability

Anyone with poor security can be held liable. Zoom Video Communications is considering settling a class action suit in the US - about 'zoombombing', privacy breach and misleading statements about end-to-end encryption - for 85 million

[63] 27 July 2021. https://www.judiciary.senate.gov/meetings/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks

[64] https://www.nieuwsblad.be/cnt/dmf20210802_93463783

[65] The Netherlands is not ready (yet), according to outgoing Minister Blok (Interior and Kingdom Relations). https://www.rijksoverheid.nl/documenten/kamerstukken/2021/11/04/beantwoording-kamervragen-over-het-bericht-litouwen-adviseert-consument-geen-xiaomi-telefoons-meer-te-kopen

[66] https://www.security.nl/posting/582760/Besluit+Wob-verzoek+inzake+uitfaseren+antivirussoftware+Kaspersky

[67] https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal

[68] https://www.rijksoverheid.nl/documenten/kamerstukken/2021/04/26/nederlandse-digitaliseringsstrategie-2021

[69] https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig

[70] https://www.rijksoverheid.nl/documenten/beleidsnotas/2021/09/06/i-strategie-rijk-2021-2015

[71] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

dollars.[72] Also interesting is the current practice of tech companies to get hackers to examine their software for security flaws. The remedy: 'bugs bounty' programmes with attractive prize money of up to a million dollars per case. But what will the provider do with the reports?[73]

The fact that not only digital providers but also user organisations run liability risks due to *inadequate digital security* should not come as a surprise. See, among others, the cases of Equifax (US, settlement of USD 700 million), British Airways (UK, fine of GBP 20 million) and HagaZiekenhuis (NL, fine of EURO 350,000).

Yet other legal aspects of digital security concern the breach of security (criminal law, both general and in copyright and database law), export regulations for security technology, the legal position of the Data Protection Officer (DPO), declarations regarding independent security audits,[74] open source software and security, digital evidence law (including lawful access to encrypted evidence), specific retention obligations for telecommunication data (the EU is working on a new regulation), digital access of citizens and companies to (semi) government (Digital Government Act (Wdo), eDIAS) and, for example, public procurement and purchasing requirements.

In conclusion

Digital security law is *here to stay* and will continue to grow in importance due to the seriousness of the threats and the consequences of incidents, especially in light of the dependence on ICT and data processing that has made people vulnerable at every level. We are noticing increasing attention for legal duties of care, as laid down in privacy legislation, among others. A relatively new category is formed by notification requirements that are triggered when a digital incident occurs. Meanwhile, regulators can impose high administrative fines[75] for both security

[72] https://www.govinfo.gov/app/details/USCOURTS-cand-5_20-cv-02155/USCOURTS-cand-5_20-cv-02155-1/context

[73] https://www.washingtonpost.com/technology/2021/09/09/apple-bug-bounty/

[74] Another topical debate: https://fd.nl/futures/1408633/stevige-kritiek-cyberbeveiligers-op-plan-voor-jaarlijkse-it-audit See also Chapter 22, IT report and assurance statement offer structural benefits.

[75] British Airways did not have the security of its online booking system in place in 2018, leading to credit card details of 420,000 customers being hacked. This resulted in an initial fine of GBP 183 million, which was reduced to GBP 20 million by the UK privacy regulator ICO due to the impact of COVID-19 on the airline. This problem - a data leak due to criminal actions *in response to security vulnerabilities*, both on the side of providers and user organisations - is gaining considerable ground.

breaches and reporting failures, while digital providers and user organisations will almost certainly be faced with legal requirements for secure hardware and software, including patching requirements, in the near future. With the amendment of the EU Radio Equipment Directive on security requirements for smart devices (well-considered : *embedded software*), the European Commission is making a start. But do not forget that digital security law is a much larger area of law.

Analysis and consideration

- Regulatory compliance - complying with laws and regulations - and the complementary fear of deterrent sanctions as a driver of digital security, can be negotiated. Anyone who looks only at the protection regulations misses out on other aspects of the law. Above all, this basic attitude carries the danger that the obligations become an unfortunate *fait d' accompli* - a burden - marginalising network and information security and the policy for it to a cost item.
- Digital security is fundamentally a *social* duty; an essential building block of socially responsible action. It is about the protection of vital infrastructures and services, the protection of the fundamental values and norms of the individual, as a citizen, employee, consumer, patient and more, and, properly speaking, the protection of the continuity of every organisation, explicitly including non-vital ones.
- As a permanent line of action, digital security belongs in the governance of an organisation, firmly anchored in up-to-date and advanced policies, including their legal components, and with adequate availability of people and resources for implementation and control.

3. Organisations and their role in the digital security domain

Frans van Paassen

Information security is purely a top-level issue. Board members, politicians and senior managers bear a great deal of responsibility in securing and maintaining the information supply. The importance of securing information is constantly growing in our highly digitalised society. All our data, whether from governments, businesses, educational, scientific or social institutions, let alone individuals, are stored on our own media or at third parties. We expect the information to be secure there: confidential, incorruptible and available. This kind of process requires substantial organisational and technical measures and resources.
But how do we know if the information security satisfies the requirements stipulated for this? What are the requirements, who sets them and how are the security measures taken tested? Fortunately, a range of organisations offer support in the eternal battle against criminals and - increasingly - state actors who try to steal, manipulate or otherwise misuse or sabotage our information.

The essence

The three well-known elements of confidentiality, integrity and availability of information make up the objective of information security. This was already true in the analogue, paper world, and is increasingly important in our digital world. What can you, as a non-IT expert, but as a responsible board member, politician or professional do to form a well-founded opinion on the degree of security of information relevant for your organisation? Relevant, because you bear responsibility for that information by virtue of your position and also because it could involve your own personal information.

In practice, large organisations at most have enough knowledge in house to form a suitable opinion on the quality of the security of their own IT environment, of that of their suppliers or customers and of the parties that provide the communication between those involved in the various chains. In any event for smaller parties, though certainly not exclusively, a multitude of organisations offer general and targeted support, in various ways.

Dutch Data Protection Authority (DPA) *** [76]

The Dutch Data Protection Authority (Dutch DPA) is the institution designated by law as independent supervisory body for compliance with the General Data Protection Regulation (GDPR) and other privacy legislation and regulations.[77] This concerns rules for the careful handling of personal data, including the security of processing. There are significant penalties for violations, and publicity or reputational damage can have a negative impact. For this reason, an organisation's senior management must also devote adequate attention to proper compliance.[78]

The GDPR is applicable to virtually all organisations in the Netherlands that process personal data. The GDPR provides that businesses and public authorities must take appropriate technical and organisational measures to secure personal data against breaches (data leaks). The GDPR leaves the exact details of these measures to the particular organisation. From time to time, the Dutch DPA issues guidelines or general recommendations on compliance with the GDPR, including on security aspects. In addition to providing advice and information, the Dutch DPA's duties include supervision, accountability and international tasks. The supervisory duty, for instance, includes complaint handling, investigation and, if necessary, enforcement action.

Radiocommunications Agency Netherlands (AT) *

The Radiocommunications Agency Netherlands (AT) ensures that the IT and communication networks in the Netherlands are available and reliable, so that the Netherlands is securely connected. The Radiocommunications Agency Netherlands

[76] **Guide:**

For the board member, politician, or responsible senior (non-IT) manager, we indicate how relevant an identified security institution and its publications or statements can be. The more stars (*****, ****** or *****)**, the more requisite basic knowledge an ultimately responsible officer of an organisation can gain from the institution in question. The institutions can be divided into legislative and regulatory authorities, supervisory bodies, drafters of standards and certifying institutions. Please note, sometimes roles can overlap.

[77] https://www.autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/missie-ambitie-kernwaarden

[78] https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens

(AT) is under the responsibility of the Ministry of Economic Affairs and Climate and plays both an implementing and supervisory role. The AT implements the legislation and regulations and also supervises compliance therewith.

In its annual plan, the Radiocommunications Agency Netherlands describes how it aims to contribute to the security of digital products and services and reports on this in separate publications or its annual report.[79] The AT is also a member of ETSI, a recognised European standardisation institution that helps support European policy in relation to telecommunications and digitalisation.[80]

Netherlands Authority for the Financial Markets *

The remit of the Netherlands Authority for the Financial Markets (AFM) is contained in the Money Laundering and Terrorist Financing (Prevention) Act (Wwft) and pertains to [81]exercising conduct supervision. Conduct supervision is firstly focused on orderly and transparent financial market processes for market parties and their customers, and also on supervising the financial markets and admitting financial undertakings to those markets. The AFM can impose enforcement measures on market parties, such as administrative fines, and can publish violations (naming & shaming).

An important expression of the AFM's policy is laid down in the Principles for Information Security for financial firms and audit firms[82]. The choice of measures and how these are fleshed out in detail lies with the organisations themselves. This is analogous to how the Dutch DPA outlines frameworks. Together with DNB, the AFM also provides the Innovation Hub, which supports innovation in financial products and services.[83]

De Nederlandsche Bank *

De Nederlandsche Bank (DNB) and the AFM work together, each from its own role. While the AFM focuses mainly on conduct supervision, DNB's focus is on prudential supervision: guaranteeing sound and ethical financial enterprises.[84] DNB supervises, for instance, that these enterprises periodically carry out risk analyses of control

[79] https://magazines.agentschaptelecom.nl/staatvandeether/2020/01/index

[80] https://www.etsi.org/about/etsi-in-europe

[81] https://www.afm.nl/nl-nl/over-afm/werkzaamheden/verantwoordelijkheden

[82] https://www.afm.nl/nl-nl/nieuws/2019/dec/principes-informatiebeveiliging

[83] https://www.afm.nl/nl-nl/professionals/onderwerpen/innovation-hub

[84] https://www.dnb.nl/betrouwbare-financiele-sector/

measures for information security. Alongside financial accountability, DNB also explicitly discusses reliability and continuity of automated information provision with the businesses.

DNB has made a useful instrument available by developing and maintaining the TIBER programme[85] (Threat Intelligence-Based Ethical Red teaming), which is dedicated to simulating, exploring and remedying genuine hacks. The TIBER-NL guide was initially intended for financial core infrastructures, but has also proved suitable for pension providers, insurers and vital sectors such as healthcare, telecommunications and energy.

European Union Agency for Cybersecurity *

The European Agency for Network and Information Security (ENISA) has a permanent mandate to protect society against the abuse of communication networks.[86] In this context, ENISA acts as an expertise centre, providing advice to stakeholders (such as member states, market parties and sectors) and supports the development and application of policy and legislation and regulations.

The SCSA Methodology was published recently; this is an IT assessment that prepares for ICT security and cybersecurity certification. Among other things, the SCSA assumes a direct connection between the desired security level and identified risks based on the objectives formulated.[87] The method ties in with generally accepted standards such as the ISO/IEC 27000 and ISO/IEC 15408 series.[88],[89]

National Cyber Security Centre **

The National Cyber Security Centre (NCSC), part of the Ministry of Justice and Security, focuses on the security of the (Dutch) digital infrastructure. The NCSC is the central information hub and expertise centre for cybersecurity in the Netherlands. The NCSC carries out investigations and risk analyses, provides

[85] https://www.dnb.nl/voor-de-sector/betalingsverkeer/tiber-samen-tegen-cybercrime/

[86] https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity

[87] https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment

[88] https://www.27000.org/

[89] https://www.iso.org/standard/50341.html en https://www.nen.nl/nen-en-iso-iec-15408-1-2020-en-269562

security advice[90] and issues publications that inform relevant parties about threats and preventing or remedying these.

The NCSC performs all sorts of activities at the request of the National Coordinator for Security and Counterterrorism (NCTV). The NCSC has developed a step-by-step plan and guide for organisations that indicates what basic measures are required for cybersecurity and how these steps can be taken.[91],[92]

Cyber Security Council **

As an independent and strategic advisory body to the government, the Cyber Security Council (CSR) gives solicited and unsolicited advice on future developments and threats in relation to cybersecurity. The council is made up of high-ranking representatives from public and private organisations and academia. Among other things, the CSR commissions studies, and recently published the advisory report 'Comprehensive approach to cyber-resilience', with support from Deloitte.[93]

One of the spearheads is that information in the cyber-resilience chain is quickly shared with all the parties involved. An accompanying infographic clearly illustrates how and on which spearheads the €833 million earmarked for cyber resilience should be spent in the 2021-2024 government period.[94] Please note: this investment is on top of what had already been budgeted for cyber resilience.

Open Web Application Security Project **

The OWASP foundation wants to reach consensus on the security of open source software through contributions from around the world. The OWASP sees as its key task raising awareness among developers of standards for the critical security of web applications.

[90] https://www.ncsc.nl/documenten/publicaties/2019/juli/02/wat-is-een-ncsc-beveiligingsadvies

[91] https://www.ncsc.nl/documenten/factsheets/2021/juni/28/cybersecurity-maatregelen-stap-voor-stap-naar-een-digitaal-veilige-organisatie

[92] https://www.ncsc.nl/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen

[93] https://www.cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

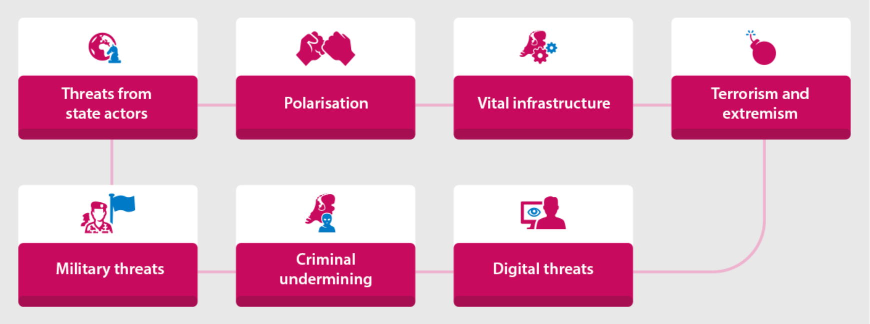
[94] https://www.cybersecurityraad.nl/documenten/mediateksten/2021/04/06/infographic-csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

To that end, the foundation disseminates its top 10 standards,[95] which are updated every few years. Items disappear, are merged, change in ranking and new ones are added.

National Coordinator for Security and Counterterrorism **

The National Coordinator for Security and Counterterrorism (NCTV) works, briefly put, on the comprehensive approach to national security.[96] The broad approach encompasses not only cybersecurity in the digital world, but also physical security in the real world. Therefore, the NCTV's mission is: we protect interests, detect threats and strengthen resilience.

In a three-yearly cycle, the NCTV decides on the National Security Strategy (NVS), with the developments of threats and risks against which we need to protect ourselves.[97]



The dynamic character of the National Security Strategy process safeguards the currency of its agenda, which lays down how we can mitigate those threats and improve our resilience.

Digital Trust Centre **

The Digital Trust Centre (DTC) was set up in 2017 as part of the Ministry of Economic Affairs and Climate. The DTC supports SMEs and self-employed individuals with,

[95] https://blog.networking4all.com/owasp-top-10-is-vernieuwd/?gclid=CjwKCAjw2P-KBhByEiwADBYWCvWHQBMhYOXxVvO7Wy4djpryGjlKVZqNnp8GP0XbBs1vFOaviyC5jxoCNWQQAvD_BwE

[96] https://www.nctv.nl/organisatie/documenten/publicaties/2020/12/14/integrale-aanpak-nationale-veiligheid

[97] https://www.nctv.nl/onderwerpen/nationale-veiligheid-strategie

among other things, five basic principles for secure digital enterprise.[98] The goal is to increase businesses' cyber resilience. To start, business owners can perform a Basic Cyber-resilience Scan.[99] The DTC also provides advice and in the fourth quarter of 2021 started a pilot whereby companies that have signed up receive information on threats.[100]

Platform for Information Security *

The Platform for Information Security (PvIB) profiles itself as an independent knowledge centre for professionals in the digital security domain.[101] To that end it provides its members with information, for instance via a journal, website, other publications, by organising conferences and through cooperation with other national and international organisations.

Royal Association of Information Professionals *

The KNVI is a broadly composed professional association for anyone involved with information, whether that be information storage, processing, use or security. The KNVI brings together professionals with a varied background from the world of IT, archiving and library science. They find each other in a number of Interest Groups (IGs) that organise physical, digital and hybrid sessions for members and other interested parties.[102]

The KNVI also publishes three professional journals and a newsletter.[103] In mid-2021, the KNVI concluded a cooperation agreement with the central government to improve the government's information management.[104]

Dutch Association of Registered IT Auditors **

NoREa is a legally regulated and academic professional organisation for registered IT auditors (abbreviated in Dutch as REs). [105] On the one hand, a RE advises on the

[98] https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

[99] https://www.digitaltrustcenter.nl/tools/doe-de-basisscan-cyberweerbaarheid

[100] https://www.digitaltrustcenter.nl/zoeken?trefwoord=adviezen

[101] https://www.pvib.nl/algemeen/over

[102] https://www.knvi.nl/agenda?regionId=&groupId=&queryString=&listView=1&cardView=

[103] https://www.knvi.nl/vakbladen

[104] https://www.knvi.nl/nieuws/360240/PERSBERICHT-Rijksoverheid-en-beroepsvereniging-slaan-handen-ineen-om-informatiehuishouding-te-verbeteren

[105] https://www.norea.nl/?page=5776

setup and structure of information provision, and on the other a RE can play a certifying role in assessing information systems. An RE can never perform both these roles at once, but may, under certain conditions, do so successively.

Just as a registered accountant issues an opinion on the financial reporting (on the financial statements, for instance), the RE does so for all IT-related reporting. Given the importance of reliable, available and secure IT systems, it was recently argued that an IT report also be required alongside the report already required to the financial statements.[106] NoREa publishes guides for users of IT systems, taking into account the legislation and regulations related to these.[107]

ISACA_NL chapter **

The ISACA professional association is an internationally organised collaboration of IT auditors and related professionals.[108] Each country has a chapter; the Dutch chapter regularly provides lectures and training courses in preparation for examinations for one of the eight certificates issued by the ISACA.[109] The ISACA shares its knowledge via, among other things, White papers and a journal[110].

The ISACA is best known from its COBIT framework, which has for decades provided a constantly updated 'toolkit' for adequate IT governance.[111] This framework serves as an excellent instrument to bridge the gap between general managers or board members and the professionals responsible for IT. To do this, it is necessary, however, to perform a risk analysis to determine what threats and corresponding measures are relevant for one's own organisation.

ECP | Platform for the information society **

As Platform for the information society, ECP occupies a strictly neutral and independent position in the midst of government, science, the business sector, education and social organisations.[112] ECP, in the form of PPPs (Public Private Partnerships), offers cooperation and connection between all stakeholders in the digital society in an open and transparent way. ECP facilitates and sets up working

[106] https://www.norea.nl/nieuws/10188/nieuw-de-it-auditverklaring

[107] https://www.norea.nl/handreikingen

[108] https://www.isaca.org/why-isaca/about-us/purpose-and-strategy

[109] https://www.isaca.org/credentialing

[110] https://www.isaca.org/resources

[111] https://www.isaca.org/resources/cobit

[112] https://ecp.nl/over-ecp/onze-visie/

groups in areas where digitalisation plays a role and functions as a driver of discussions on 13 topics.[113]

At present, ECP has specific platforms in the areas of healthcare, energy, ethics, artificial intelligence, data sharing, internet security and quantum technology. A summary of the annual plan[114] provides insight into how ECP acts and what it does. All of ECP's publications are available digitally on its website for interested parties.[115]

International Standardization Organisation **

The International Standardization Organisation (ISO) is an independent organisation with which 166 national standardisation bodies are affiliated. In the information security world, ISO is mainly known for its 27000 series.[116] ISO27001 sets out the standards and requirements for an ISMS[117] (Information Security Management System): leadership, implementation, maintenance and constant improvement of the management system. An approach that is based on Charles Deming's Plan-Do-Check-Act quality circle aimed at the constant improvement of organisations. ISO27002 is also very important because it gives a total overview of guidelines, principles and possible security measures.[118]

The standards mentioned complement each other and are both used in practice. The starting point is always a formal risk analysis (risk assessment). The standards provide a toolbox that IT professionals and their principals (administrators and/or board members) should use with caution and responsibly. Over the years, ISO27002 has also given rise to the development of industry-specific sets of measures, such as for production companies, the healthcare sector, and more.

Dutch Standardisation Institute *

The Royal Dutch Standardisation Institute, better known as NEN, manages more than 34,000 different standards: Dutch, European and international. The standards relate to a multitude of topics, including the NEN7510 and NEN75xx standards

[113] https://ecp.nl/themas/

[114] https://ecp.nl/publicatie/ecp-in-2021/

[115] https://ecp.nl/publicatie/

[116] https://www.27000.org/iso

[117] https://www.27000.org/iso-27001.htm

[118] https://www.27000.org/iso-27002.htm

developed specifically for Dutch healthcare and derived from the ISO2700x standards.

The NEN has also formulated certification schemes that independent third parties can use in performing audits to assess whether an organisation, institution or business satisfies a particular standard. These third parties must in that case be accredited to perform audits. These audits can result in the granting of a quality mark. From the perspective of segregation of duties, the NEN itself does not grant certification. Worth noting is the specialist course[119] offered by the NEN to make the link between the Dutch GDPR and the implementation of an ISMS (Information Security Management System) for information security clear.

Conclusion

In the constantly and rapidly changing digital world, securing information has become a concern for the highest levels of management. That is why executives who are ultimately responsible, i.e. administrators and directors, but also non-IT professionals, and politicians, for instance, must be able to form an opinion on the quality and security of their digital information. This calls for the development and maintenance of adequate basic knowledge to be able to ask internal and external IT security experts the right questions.

The ultimately responsible individuals in an organisation must also be able to correctly evaluate the answers they receive to their questions, whether or not in the form of IT Assurance statements. In addition to statutory requirements, a risk analysis always underlies the set of security measures taken. The organisations mentioned offer support with this in various ways.

[119] https://www.nen.nl/leergang-iso27701-van-informatiebeveiliging-naar-avg

Recommendations

- Within any private, public or social organisation, the responsibility for information security must be vested at the highest level.
- The responsible board members, directors, politicians and non-IT professionals must periodically assess or commission an assessment of whether the security measures chosen and the standards applied in that context are still appropriate for the risks deemed relevant for their organisation.
- Just as for financial and policy information, there must also be accountability for the security of digital information. After the fact, but certainly also looking forward in order to be able to assess the adequacy of the measures for the future.
- An Assurance statement on the IT security must not only concern the past period, it must emphatically also be forward looking. Independent third parties can issue this kind of statement periodically.
- The weighing of the relevance of threats and the security measures taken to mitigate the risks identified must take place at the highest level.
- Information security must always be ‘a top-level issue’.

4. Making sense of certifications for security professionals

Rosanne Pouw, MSc, MPIM, MBA, CIPM

In the Wild West of the cybersecurity field, it is fashionable as a security professional to attain and list certifications, usually after your name. But what does such a certificate say about the qualities of the person in question? Furthermore, the jungle of certifications has made it difficult to assess whether the content and context of the certification is relevant for the assignment this person is supposed to perform. Demanding requirements are stipulated for the knowledge and skills of experts and professionals, in part because there are so many rapid changes taking place in the field. It is certain that the US certifications such as CISA, CISSP, CISM and others have become an important component in formulating job vacancies and selecting cybersecurity professionals worldwide and in the Netherlands. This chapter concisely explains the advantages and disadvantages of certifications for security professionals, then discusses the most popular certifications and finally concludes with a few considerations.

Popularity

Cybersecurity certifications[120] are popular because a large volume of subject-matter information can be learned in a relatively short period of time. While a bachelor's degree takes two years and a master's degree four,[121] a certification can be attained in mere months. Certifications furthermore stipulate different entrance requirements than traditional degree programmes, making them accessible for many people.

An additional advantage is that job vacancies may cite degrees as a preference, but certifications are often mentioned as conditions or prerequisites. A

[120] https://alpinesecurity.com/blog/history-of-cybersecurity-certifications/

[121] https://www.rijksoverheid.nl/onderwerpen/hoger-onderwijs/vraag-en-antwoord/wat-zijn-de-bachelor-master-en-associate-degree-in-het-hoger-onderwijs

professional with a master's degree in some other field and supplementary certifications can therefore compete with a professional with a master's degree in cybersecurity. Whether this is rightly the case depends on the qualities of the individual. While a bachelor's or master's programme is intended to produce broadly developed critical thinkers, the aim of a certification is to combine broad knowledge of the field with the most recent developments. Certifications are aimed at professionals who have already gained practical experience or who are ready to take the leap to start working in this field. There is something to be said for the idea that a cybersecurity professional should be both a critical thinker and someone who has broad, up-to-date knowledge.

Complexity

This is not to say that attaining certifications is substantially easier than completing a degree programme. Achieving certification requires taking an examination. The applicant must also have sufficient work experience in the field, which often needs to be endorsed by another professional who already holds the same certification. To retain the certification, a contribution must be paid annually per certification to the relevant organisation and the professional must demonstrate they have spent at least a certain number of hours per year on professional development. For example, by attending trade fairs, following training courses or contributing in some other way to developing the cybersecurity field.

Certifications require a different method of studying and assessment than a regular degree programme. The path towards passing the examination is less straight forward compared to a regular study programme. There are multi-day so-called 'bootcamps' in which participants are bombarded with the material, accompanied by examples to bring the material to life. There are study groups, various books and online platforms. The world of certifications is also a revenue model with many options for those who wish to attain a certification.

A closer look at certifications

Going by job listings on LinkedIn,[122] the three most requested certifications in the field of cybersecurity are CISSP, CISA and CISM. What is the essence of these three certifications?

[122] https://www.coursera.org/articles/popular-cybersecurity-certifications

CISSP

CISSP stands for Certified Information Security Systems Professional and was developed by the American organisation (ISC)2,[123] founded in 1989. This certification forms the basis for positions like Security Officer, Security Manager, Security Consultant or Cybersecurity Specialist. According to the Regulated Qualifications Framework of UK NARIC, the CISSP certification is the equivalent of a master's degree.[124] All the information tested on the examination is contained in the almost 1,200-page CISSP Official Study Guide. ISC2's certifications are moreover accredited under the ANSI/ISO/IEC Standard 17024, the worldwide benchmark for certifications.

After the CISSP examination

In order to attain certification, the applicant must successfully pass an examination, have at least five years of relevant work experience and be endorsed by someone who already holds a CISSP certification. The required knowledge is divided into eight domains, including operational topics such as network security and security in software development (but not in programming as such, because CISSP does not deal with programming languages or secure ways of describing code). Strategic topics like governance and auditing are also included. In that respect, the knowledge required to pass the CISSP examination is 'a mile wide and an inch deep'.

What is special about CISSP is that the exam adapts to the knowledge level of the person being tested. The general knowledge level is assessed with the first ten questions. The next questions zoom in on any gaps, thus calculating whether the participant's knowledge is sufficient or not. The questions often combine several domains and contain contradictory or misleading wording. The examination takes a maximum of 4 hours and contains 125 to 175 questions.

In order to maintain certification, the professional must pay an annual membership fee to ISC2 and achieve at least 120 Continuing Professional Education points (CPE) every three years. That means at least 120 hours demonstrably spent on activities to maintain cybersecurity knowledge and skills.

[123] https://www.isc2.org/Certifications/CISSP

[124] https://www.infosecurity-magazine.com/news/cissp-equal-masters-degree/

CISA

CISA stands for Certified Information Systems Auditor and is issued by ISACA.[125] This certification is regarded worldwide as the standard for those who audit, manage, monitor and assess information systems and technology. This certification creates a solid foundation for becoming an auditor.

The material for this certification is developed and updated by ISACA and emphasises audit skills. Important topics include the auditing process, IT management and governance, acquiring, developing and implementing information systems, business resilience and protecting information assets. The recommended learning material is the approximately 500-page CISA Review Manual. The examination takes a maximum of 4 hours and contains 150 questions. Examinations are taken at official testing centres to prevent fraud.

After the CISA examination

Like the CISSP certification, the CISA certification is accredited under ANSI/ISO/IEC Standard 17024: 2012. After passing the examination, the applicant must also go through a process to demonstrate at least 5 years of recent experience in auditing and information security, and a membership fee must be paid. To maintain certification, a contribution must be paid annually and at least 120 CPEs must be achieved every 3 years.

CISM

The ‘Certified Information Security Manager’ certification is also developed and managed by ISACA. This offers advantages when it comes to maintaining certifications, since a discount is given if someone maintains multiple certifications with ISACA. With this, security professionals can demonstrate that they have knowledge of information security governance, programme development and management, incident management and risk management. CISM is often requested for positions like Security Officer, Security Consultant or Security Specialist. The material here is also contained in a CISM official study guide, comprising approximately 300 pages. The examination takes 4 hours and contains 150 questions.

[125] https://www.isaca.org/credentialing/cisa

After the CISM examination

After passing the CISM examination, the same steps must be taken as for the other certifications. Demonstrating at least 5 years of recent experience by means of an endorsement, staying up to date on membership fees and attaining at least 40 CPE per year, or 120 CPE every three years. The ANSI/ISO/IEC Standard 17024: 2012 for accreditation also applies to CISM.

The comparison

A brief overview comparing the certifications side by side is provided below. The number of pages contained in the official study guides represents the study load. It is striking that the CISSP certification, involving the highest study load, is also the most frequently requested in job listings on LinkedIn.[126] Because the CISSP covers eight domains, it is logical that this certification is also requested for more positions in different domains.

	CISSP	**CISA**	**CISM**
Number of pages	+/- 1,200	+/- 500	+/- 300
Type of positions	Operational/tactical positions	Auditor	Strategic/tactical positions
Requested in job vacancies on LinkedIn	48,711	12,466	8,860

Conclusion

Educational certificates can provide a practical point of reference for organisations seeking to fill vacancies in the broad cybersecurity domain. The system behind the three most commonly requested certifications ensures that they cannot be attained or maintained without effort. In that sense, they serve as a hallmark for quality. It provides insight into the extent to which candidates invest in themselves by attaining and maintaining certifications. It would be unwise, however, to put blind trust in such certifications. A good strategy could be to state in the vacancy that the candidate must be willing to attain a certification, if they are currently not certified, thus attracting a higher number of suitable candidates. In order to make a considered choice, a candidate must have not only substantive knowledge, but also the necessary soft skills and be a good match for the business or organisation.

[126] https://www.coursera.org/articles/popular-cybersecurity-certifications

Considerations

- All the generic certifications discussed here have been set up by US organisations. A number of large US providers also offer certifications *for their own products*, such as Amazon, Microsoft and CISCO. To what extent can the knowledge and skills tested be applied in the Netherlands? One example is the difference in governance, as it is often assumed by creators of certifications that an organisation is hierarchically structured. In the Netherlands we are accustomed to asking critical questions and weighing contributions based on expertise. Organisation and culture specific knowledge does not easily translate to other countries and cultures.
- The substantive knowledge that is assessed for certifications is certainly useful for security professionals, as shown by the large number of certafied professional worldwide. Certifications are primarily suitable for starting or mid-level positions. Once a professional has gained enough experience in senior positions, certifications are often no longer requested. It comes across as somewhat peculiar to ask a professional who has worked in the field of security for over twenty years for certification.
- In addition, certifications are *not* always the quality hallmark envisioned. Starters in the field can achieve several certifications relatively quickly, but they are lacking the experience to be able to apply this knowledge in practice. Despite this flaw in the system, attaining a certification demonstrates that the candidate is willing to invest time and effort, consciously wants to expand their skills and knowledge, and conform to the standards of the field. *A good way of testing whether you are dealing with a critical thinker is to engage in a discussion on the usefulness of certifications.*
- Finally, a consideration on certifications in the privacy field. The only position with duties defined by law[127] is the Data Protection Officer (DPO). Because of the DPO's special legal status, this position is, as internal supervisory officer, independent of the organisation's board. There is currently no certification for becoming a 'certified DPO'.[128] The privacy training courses that could culminate in a certificate have no formal status with the Dutch DPA. The certifications that come closest to a quality

[127] Laid down and described in the General Data Protection Regulation (GDPR).

[128] https://www.ictrecht.nl/blog/hoe-word-ik-een-gecertificeerd-fg-certified-dpo-cdpo

hallmark for privacy are the CIPPE and CIPM certifications from IAPP. These follow a format comparable to that of the security certifications mentioned, also encompassing the related requirements that experience must be endorsed by a third party and knowledge must be kept on level.

5. Information security: the key to digital security in a time of growing cyber threats

Hans de Vries

Information security, a term inextricably connected with digital security. Without reliable systems that enable you to take measures to safeguard information, it is simply impossible to have your digital security in order. This may seem obvious at first glance, but nothing could be further from the truth if you consider that many Dutch organisations do *not* have their information security - and therefore their digital security - in order.

Every organisation that fails to safeguard its cybersecurity is one too many, of course. But we are not talking about just one or two organisations, but about a significant number that take too few measures, if any, to avert today's digital threats. This obviously has implications for the digital resilience of the Netherlands as a whole, especially if you consider that the COVID-19 pandemic increased our dependency on digital processes. This means that the consequences of a digital attack could have unprecedented scope and could even disrupt society. In short, information security is undeniably important. As great as the damage could be if your organisation is not digitally resilient, you can make the risks as small as possible if you take the right digital measures.

This is according to the Cyber Security Assessment Netherlands 2021 (CSAN 2021) that the National Coordinator for Security and Counterterrorism (NCTV) prepared in cooperation with the National Cyber Security Centre (NCSC).[129] The CSAN 2021 reflects the current state of digital security in the Netherlands. What threats are there? How able are we to defend against these threats and how do they impact our national security? With reference to the answers to these questions, the CSAN 2021 shows how important information security is and how this security can be improved.

[129] NCTV, Cyber Security Assessment Netherlands (2021), https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

Importance of information security

Every one of the cyber incidents that occurred between March 2020 and the end of March 2021 demonstrates the importance of information security. From a number of businesses that were infected via a leak in Citrix to Dutch providers hit by DDoS attacks, and from a ransomware attack on the municipality of Hof van Twente to the theft of coronavirus data from the GGD: all of these had a significant impact on the organisations affected.

Although the incidents varied in nature and impact, they have one thing in common: the fact that an organisation's private information can become public and can be misused. This damages not only the particular organisation itself, but also people and other organisations affiliated with the affected organisation. This is certainly the case for government agencies, on which citizens rely and where citizens have no choice but to provide their personal details to these agencies. Information security is therefore not only important for yourself, but for others as well.

COVID-19 and our digital security

One factor that has played a role in cyber incidents since March 2020 is COVID-19. Not only have we become more dependent on digital processes as a result of working from home, malicious actors also took advantage of the pandemic to carry out cyber attacks. Take phishing emails that play on COVID-19, for instance. Or cybercriminals who carry out attacks on healthcare institutions which feel heightened pressure to pay up in ransomware attacks, so that they can continue to help fight the coronavirus. It is crucial that these parties have exclusive rights to the access to their own information, so that they can safeguard the continuity of their services. Working from home can also pose a heightened risk; employers often have not adequately provided for digital resilience at their employees' home offices.

Basics not in order

COVID-19 therefore increased the digital threat to a certain extent. The digital resilience is still lagging behind the increased risks, however. There are still many organisations in the Netherlands that do too little, if anything, to properly secure their information. These organisations are not taking the basic measures in this regard - such as using strong passwords and patching vulnerabilities on time. This makes them extra vulnerable and we also see that malicious actors actively exploit these vulnerabilities, if we look at the cyber incidents that have taken place over the past period. It is not only cybercriminals that are involved, but also state actors who exploit vulnerabilities in hardware and software in systems or installations for purposes of espionage or sabotage based on national (geopolitical) interests.

In other words, patching digital vulnerabilities on time is essential for protecting information. If you do not do this, malicious actors exploiting the vulnerability can install a backdoor which will continue to give them access to the organisation's data at a later point in time. Even if you have already patched the vulnerability. In this way, a malicious actor can make sensitive business information public worldwide or promise not to do so in exchange for ransom.

If you have failed to immediately patch a vulnerability, the best option is still always to do so as quickly as possible; patching late is always better than not patching. This in order to make the likelihood of abuse as small as possible. It remains a fact, however, that the safest option is to patch as quickly as possible because vulnerabilities are being abused faster than ever.

Big helps small

Especially among SMEs (small and medium-sized enterprises), digital resilience is lagging behind the threats, partly because these businesses often do not have sufficient resources to optimise their resilience. There is not always a designated person with responsibility for back-ups and patches, for instance. This makes these businesses vulnerable to cyber attacks.

In order to ensure that as many SMEs as possible increase their digital resilience and safeguard their precious assets, they can become part of the Nationwide System for sharing information on cyber threats (abbreviated in Dutch as LDS).[130] This is a system in which information about digital threats and vulnerabilities is shared with individual organisations via linking organisations. The NCSC is the central information hub in this system. For SMEs, the NCSC passes information on to the Digital Trust Centre (DTC), which focuses on these businesses and self-employed individuals. In this way, we can ensure that SMEs are not left behind big business and providers of vital social services in terms of digital resilience. By making sure, among other things, that they receive the information they need to take measures to prevent or prepare for incidents on time.

[130] NCSC, Landelijk Dekkend Stelsel [Nationwide System] (2019), https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds

Chart out the risks

Another step that would be advisable for any organisation is to investigate what digital risks are unacceptable, for instance because they can disrupt the continuity of the organisation's core business. This consideration determines which measures an organisation must take to contend with the biggest risks. In order to provide more insight into the risks, there is an instrument for translating them into concrete scenarios, so that not only cybersecurity experts, but also others in the organisation - such as directors or board members - can better situate the risks and act accordingly.

In short, it is very important for organisations to take measures that are appropriate to the heightened digital threats of today. The use of strong passwords and prioritising patches and risk management are just a few examples of measures that can help organisations stand up to the higher threat level. The NCSC has fortunately also picked up on positive developments in increasing digital resilience among organisations. A growing number of organisations are using multi-factor authentication, for instance, and have improved their response to cyber attacks. Nonetheless, these efforts have not yet caught up with the increased digital threat.

Conclusion

To give organisations a hand in making their organisations more secure digitally, step by step, the NCSC has prepared the Guide to Cybersecurity Measures.[131] This contains a more extensive overview of measures and a five-step plan for organisations to strengthen their resilience. With the cyber risks of today, the likelihood of damage and disruption of an organisation's continuity is simply too great not to take these steps. This produces a lot of benefit for digital resilience. Because an organisation that has its digital security in order also strengthens the digital resilience of our country as a whole. This is precisely how we make the Netherlands digitally secure together, because only if we take the necessary cyber measures to protect our valuable information can we protect ourselves against today's digital threat.

[131] NCSC, Guide to Cybersecurity Measures (2021)

https://www.ncsc.nl/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen

Points for attention

- Our digital security is under pressure on a daily basis. Every day, vulnerabilities in hardware and software are actively taken advantage of. Large-scale digital attacks are growing worldwide. As are attempts at sabotage, espionage and theft. Especially by state actors and criminals.
- The Netherlands is increasingly digitalising, so our dependency on digital facilities continues to grow. Among other things, the Citrix and the coronavirus crisis demonstrated how dependent the Netherlands has become on good and above all secure digital facilities.
- Our digital infrastructure is therefore increasingly the lifeline for our economy, social interaction and innovation. Protecting our digital lifeline is vital.
- Because if a major ICT disruption causes outages in the drinking water supply, or power failures, or trains to stop running, or payment terminals to go offline, then the Netherlands will come to a standstill and social unrest and disruption will undoubtedly ensue.
- The task of keeping the Netherlands digitally secure therefore requires a responsible government that is capable of protecting our digital interests smartly, quickly and decisively, now and in the future. The National Cyber Security Centre (NCSC) carries out this task by:
    1. Having at its disposal the right knowledge and information in relation to digital threats and vulnerabilities
    2. Sharing this information with vulnerable businesses and organisations as quickly as possible
    3. Providing (preventative) advice on risks
    4. Playing a coordinating role within the national crisis structure if a serious ICT incident or crisis (or threat thereof) arises.
- The government has a responsibility, but organisations, businesses and citizens themselves also bear responsibility for their own cybersecurity. It is the government's job to enable them to fulfil these responsibilities. From tech giants and government authorities to start-ups - we must all work together to help secure our digital world.
- That is why we, as the NCSC, actively work as part of a public-private system of parties. We call this the Nationwide System (in Dutch: *landelijk dekkend stelsel*). In this system we share threat information with parties for whom it is relevant. After a legislative amendment that will be realised soon, there will be

more possibilities for the NCSC to share this kind of information more broadly.

- It is also important that senior management at businesses and organisations feel a sense of responsibility for digital resilience. We, the NCSC, have identified eight basic measures you must take at bare minimum and how you can best assign responsibilities within an organisation.
- Only if we all take up our role can we improve the digital resilience of the Netherlands.

6. Supporting cyber security skills and professionalism in the UK

Steven Furnell

A key focus in the United Kingdom in recent years has been professionalisation in cyber security and improving the related understanding of the topic and the sector. In common with other countries, the UK has seen significant recognition of a cyber security skills shortage, with related evidence[132,133] repeatedly suggesting a lack of practitioners (including experienced staff and new entrants), as well as a lack of clarity around the knowledge and skills that are needed to address the demands. As a consequence, various activities have been undertaken to improve the understanding of the topic, enhance the recognition of practitioners, and bring wider visibility and clarity to the sector.

Recognising security professionals and skills

Looking at some of the key developments in chronological order, a relevant starting point is the Chartered Institute of Information Security (CIISec). This was founded in 2006 as the Institute of Information Security Professionals, but changed its name in 2018 having been granted Royal Charter. The Institute was founded by leaders of the profession, drawn from industry and academia, and their motivation was their question of how to recognise a competent information security practitioner. As a professional body, CIISec has an individual membership scheme from student to fellow, and at the time of writing represents over 10,000 members across the sector, with an extensive range of corporate and academic partners.

However, the contribution goes beyond this and has also been relevant in guiding and shaping the profession itself. For example, CIISec has devised a Capability

[132] McHenry, D., Borges, T., Bollen, A., Shah, J., Donaldson, S, Crozier, D. and Furnell, S. 2021. *Cyber security skills in the UK labour market 2021 – Findings report*. Department for Digital, Culture, Media and Sport, March 2021. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021

[133] Wilson, P. 2021. The Security Profession 2020-2021. Chartered Institute of Information Security.

Development Methodology[134], which is designed to help organisations to develop, recruit and retain cyber security talent. This notably includes the *CIISec Skills Framework*[135], which provides a means of identifying and measuring different skills relating to cyber security, and enabling individuals and roles to be profiled accordingly. The Framework identifies a set of 11 Security Disciplines (denoted A-K) as follows:

A. Information Security Governance and Management
B. Threat Assessment and Information Risk Management
C. Implementing Secure Systems
D. Assurance, Audit, Compliance and Testing
E. Operational Security Management
F. Incident Management, Investigation and Digital Forensics
G. Data Protection, Privacy and Identity Management
H. Business Resilience
I. Information Security Research
J. Management, Leadership, Business and Communications
K. Contributions to the Information Security Profession and Professional Development.

These disciplines are then further decomposed into a total of 36 underlying Skills Groups (e.g. Discipline B includes: B1 – Threat Intelligence, Assessment and Threat Modelling; B2 – Risk Assessment; and B3 – Information Risk Management). The skills associated with each of these groups can then be assessed at six different levels, ranging from basic knowledge to lead practitioner. As a result, individuals and teams can be assessed against the framework in order to demonstrate their skills profile, and roles/vacancies can be similarly assessed in order to enable employers to understand their skills needs.

Establishing a national centre

[134] See www.ciisec.org/Capability_Methodology

[135] CIISec. 2019. *CIISec Skills Framework*, Version 2.4, Chartered Institute of Information Security, November 2019. https://www.ciisec.org/CIISEC/Resources/Capability_Methodology/Skills_Framework/CIISEC/Resources/Skills_Framework.aspx

While notable in supporting professionalism in the sector, CIISec is far from the only significant player in the UK context. Indeed, a clear sign of the recognition and significance of the issue was the launch of the National Cyber Security Centre (NCSC) in 2016. Part of the UK's Government Communications Headquarters (GCHQ), it has initiated and supports a wide range of activities, with examples being public-facing advice via the Cyber Aware campaign[136] and a variety of business-focused guidance, including the *10 Steps for Cyber Security*[137] and the *Cyber Essentials* certification scheme[138].

From the perspective of supporting the development of the sector, two of the NCSC's notable contributions have been supporting the creation of the *Cyber Security Body of Knowledge (CyBOK)*[139] and the introduction of a certification scheme for academic degrees.

Defining a body of knowledge

First launched in 2019, the CyBOK aims to provide a guide to the body of knowledge in the topic area. It does so by drawing upon material that is already available in other sources and mapping this into a structure involving 21 Knowledge Areas (KAs) that collectively span a breadth of cyber security issues. These are grouped into five broader categories, and the resulting structure is summarised as follows:

- Human, Organisational and Regulatory Aspects (Risk Management & Governance;; Law & Regulation; Human Factors; Privacy & Online Rights)
- Attacks and Defences Malware & Attack Technologies ; Adversarial Behaviours; Security Operations & Incident Management; Forensics)
- Systems Security (Cryptography; Operating Systems & Virtualisation Security; Distributed Systems Security; Formal Methods for Security; Authentication, Authorisation & Accountability)
- Software and Platform Security (Software Security; Web & Mobile Security; Secure Software Lifecycle)

[136] See www.ncsc.gov.uk/cyberaware

[137] See www.ncsc.gov.uk/collection/10-steps

[138] See www.ncsc.gov.uk/cyberessentials

[139] Rashid, A., Chivers, H., Lupu, E., Martin, A. and Schneider, S. 2021. *The Cyber Security Body of Knowledge. Version 1.1.0*, 31 31 July 2021. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf.

- Infrastructure Security (Applied Cryptography; Network Security; Hardware Security; Cyber-Physical Systems Physical Layer & Telecommunications Security)

The resulting material represents a considerable reference resource, with the KAs materials collectively covering over 700 pages and citing over 2,200 related sources.

Certification of academic degrees

The NCSC's degree certifications were first introduced in 2014, in recognition of the potential difficulties facing prospective students in terms of identifying courses to suit their interests, as well as the challenge for employers in recruiting talent from relevant sources. Key elements considered as the basis for certification are the topic coverage of the degree, the assessment materials, and the academic team involved in the delivery, with applications being considered by panel of experts drawn from academia, industry and government.

The certification programme was initially targeted towards Master's level degrees in general cyber security, and was then later extended to cover undergraduate degrees at Bachelor's and Integrated Masters level[140]. More recently the scheme has been adapted to utilise the CyBOK KAs as the basis for mapping programme coverage, providing a consistent and comprehensive reference point against which to compare and understand the focus of different degrees. At the time of writing this has led to the certification of over 50 degree courses at over 30 universities

Self-regulation and career pathways

The most recent UK development has been the creation of the *UK Cyber Security Council*, a self-regulatory body for the cyber security education and skills sector. The Council was launched in May 2021, following on from an 18-month formation project, itself involving contributions from a consortium of 16 existing organisations and professional bodies within the Cyber Security Alliance[141]. The stated mission of the Council is "to be the self-regulatory body for, and voice of, the cyber security

[140] Furnell, S. K, M., Piper, F., E2, C., H2, C. and Ensor, C. 2018. "A National Certification Programme for Academic Degrees in Cyber Security", in *Towards a Cybersecure Society: Education and Training*. L. Drevin and M. Theocharidou (eds.), IFIP Advances in Information and Communication Technology, Springer, pp133-145.

[141] IET. 2021. "About The UK Cyber Security Council", Institution of Engineering and Technology. https://www.theiet.org/impact-society/uk-cyber-security-council-formation-project/

profession" and "to develop, promote and provide stewardship of the highest possible standards of expertise, excellence, professional conduct and practice in the profession, for the benefit of the public"[142].

One of the key contributions in this respect is the provision of a Careers Route Map, identifying the pathways for 16 specialisms within the cyber security field (with examples including Cyber Threat Intelligence, Digital Forensics, Incident Response, Secure Operations, and Security Testing). Each specialism is described in terms of working life, responsibilities, and progression opportunities, as well as details of how to join the area and the indicative job titles and salaries that may be expected. It also considers the relevant qualifications and experience, and the underlying knowledge and skills that would be applicable for practitioners in each of the areas. The latter are notably specified with reference to Knowledge Areas from the CyBOK and Skills Groups from the CIISec Skills Framework, thus providing clear linkage and ongoing relationship with the earlier contributions in the topic.

Conclusions

While the issue of developing cyber security capabilities and skills in the United Kingdom cannot be considered to have been solved, the various initiatives outlined here have certainly made a significant contribution in terms of providing clarity and structure. Collectively, they offer means of understanding knowledge and skills, as well as the qualifications and career paths into which they can be incorporated. As such, they provide a solid foundation for practitioners and a reference point for employers, with organisations such as CIISec, the NCSC and the UK Cyber Security Council all set to play a part in further development as things move forward.

Insights

- The cyber security sector requires professional practitioners, supported by appropriate recognition of knowledge and skills.
- National initiatives help to provide visibility and also serve to signal the recognition and importance of the cyber security to those within and outside the sector.
- Integration of different components into a coherent overall approach provides a credible basis for providing clarity and supporting growth.

[142] UK Cyber Security Council. 2021. "Out Vision and Mission".

https://www.ukcybersecuritycouncil.org.uk/about-the-council/vision-and-mission/

7. The CISO as security officer and his arsenal

Brenno de Winter

Keeping the digital environment safe is undoubtedly a task for which many parties in an organisation are responsible. To name a few examples, we expect a user not to share his or her login details, to report suspicious situations, not to share information outside the organisation without permission and to follow the organisation's guidelines - or better: instructions – meticulously. We expect system administrators, as dedicated IT professionals, to configure the information systems securely, regularly implement updates, monitor the systems and assign user accounts and authorisations responsibly. We expect the management to offer an environment *and* the corresponding conditions that enable secure behaviour and also that they convey that expectation broadly. Many of these duties come together in the Chief Information Security Officer or CISO, who must be more of a manager than an adviser. And: not infrequently, the position must be fought for in an organisation.

Pivotal role

The CISO plays a pivotal role in an organisation's information security policy. In an ideal world, this person would bring together different disciplines, ensure that the likelihood of risks materialising is limited and mitigate the effects if incidents occur. In practice, this means that the role involves not only organisational aspects, but that insight into risk management and technology is also indispensable. For success, risks in all layers of the organisation must be translated. That requires a jack-of-all-trades in fact, which is hard to find these days. In practice, we often see that performance of the role is dominated by one of these aspects. For a more specific role description, the Centre for Information Security and Privacy Protection (CIP) wrote a paper to clarify the position.[143]

[143] https://cip-overheid.nl/media/1167/bid-operationale-producten-bir-011-ciso-functieprofiel-10.pdf

Organisational embedding

But the role of CISO is just not as clearly delineated as that of the Data Protection Officer (DPO), for instance, who, like a Works Council member, cannot be dismissed. Thanks to the General Data Protection Regulation (GDPR), the DPO has an independent role, a right to an adequate budget and must be consulted for the mandatory data protection impact assessments (DPIAs). Because this position reports to the data controller, usually the highest 'boss' in an organisation, there is a direct line to the boardroom. Such a role is not automatically reserved for a CISO, as the role is not defined in legislation. The fact that embedding information security is part of data protection law usually ensures that the issue is considered from a legal perspective rather than a technical one. You could take the position that the position of CISO is being undermined over the long term. After all, it can be skipped over.

This certainly does not mean that there is no place for a CISO, but rather that the position must be fought for. Although organisations are required[144] to provide for security - 'taking into account the state of the art' - how they arrange that is up to them. The role is indeed mentioned in ISO-27001 and the Government Information Security Baseline.[145] That means that governments and organisations that satisfy the ISO standard must have one. With a bit of skill, one could argue that this role is required under the Networks and Information Systems (Security) Act (Wbni) because it makes it mandatory to comply with international standards,[146] but that is not a robust foundation on which to firmly anchor the role.

Budget is crucial

Without clear anchoring, there are multiple ways in which the role can be embedded in the organisation. *In practice, the role in its weakest form emerges to be mainly advisory in nature*. The operational duties are invested elsewhere, if at all, which means the influence is very limited and the security policy lacks cohesion. Especially the absence of a budget for the role means it is difficult to achieve anything. In such a construction, budget is sometimes still available, but experience teaches that this is mainly intended for awareness-raising campaigns. There is little if any overriding authority. The fact that this is a big problem is evident from

[144] Article 32 GDPR – https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679

[145] Government Information Security Baseline (BIO) – https://www.bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf

[146] Wbni – https://wetten.overheid.nl/BWBR0041515/2019-01-01 – Article 7(2)(e)

research by Kaspersky[147] which makes it clear that a third of CISOs have a structural budget deficit and that CIOs and CISOs do not have enough access to the 'boardroom'. A picture that is, for the rest, in line with other studies.

In a more ideal situation, this kind of staff position would be decked out more by giving the advisory function a stronger role in an organisation's strategy and policy. Organisations that put more weight in the advisory function are more likely to have a budget and a CISO that can not only advise, but also test against the practice. This somewhat sturdier configuration does provide the space to develop and roll out a policy. Properly established, it is possible to approximate the independent position of a DPO. It does make a difference in this context whether the role is a staff position under the board or a staff position under the Chief Information Officer. If the role falls under the board, it is easier to exert influence on the whole organisation and, for example, to enable information security to better come into its own in the line organisation. If the position is under the CIO, the role is more limited to the systems and the rest of the organisation will be more likely to interpret this as a mere 'ICT matter'.

Indispensable coordination

For years now, information security has no longer been concerned with the security of a computer system alone. It concerns a broad spectrum of aspects ranging from system security to monitoring systems, or from protecting personal data to safeguarding business continuity. ICT now has a significant impact on the physical world, so security involves more than just computers. The deluge of ransomware incidents with significant impact makes it crystal clear that many organisations are in any event falling short in terms of proper access management, systems monitoring, network segmenting, fall-back arrangements and securing back-ups. If the position of a CISO is in fact embedded, this individual can play a key role in bringing the right disciplines together and giving direction to the strategy and policy, from security handling through to final resolution of the ultimate incidents.

Another problem immediately arises. A 2019 survey[148] by the Centre for Information Security and Privacy Protection among 100 CISOs and 40 administrators in government indicated that there is a lack of experience in the field. Some 40 percent of respondents emerged to have been working in the field for between zero and two years. A similar percentage had been active in the field

[147] https://go.kaspersky.com/BNL_CISOrapport_NL.html

[148] Survey: https://www.cip-overheid.nl/media/1363/ciso-enquete-2019-definitieve-versie-11.pdf

for between three and five years. The average age emerged to be 55 years. Despite the seniority, around 80% percent has less than six years of experience in the information security field and is *therefore at most mid-level*.

This broadly conjures up an image of CISOs who have moved into the position as a career switch rather than after a long period in the field. What is problematic with this is the lack of relevant training in many cases. That need not be a problem in and of itself, but in combination with a lack of experience it is problematic. In a playing field which requires understanding of the available technology, organisational knowledge and experience in the information security domain, this makes the officer vulnerable. In practice, it emerges that preventing many vulnerable situations depends entirely on identifying the danger in time and selecting the right measures. Performing effective coordination becomes difficult in that case.

That the same survey shows that 69% of the CISOs say they perform their job part time. That impression is not made any rosier when it emerges that 77% has no team around them and that a base on which to fall back is also lacking. This inevitably prompts the conclusion that it is precisely in the area of coordination and management that the officer is often flying solo, with a lack of experience and expertise. Despite much good will and skill, embedding information security policy is an uphill battle.

Conclusion

Anyone who wants to comply with the duty to organise information security well cannot avoid properly embedding the coordination and management in the organisation. That means not only giving the CISO a robust role in the organisation, but also organising knowledge and skill so that the job can be performed well. Those who do not do this will manage to do something about information security on some points. But there can only be an effective security strategy if the measures are geared to the organisation and the risks at play for the organisation. Investment in knowledge, training and equipment for a CISO office is also unavoidable. Only then can a coordinating role be performed. Anyone who doubts whether the benefits outweigh the costs need only look at the enormous damage caused by an incident or draw lessons from safety management: 'If you think safety is too expensive, try an accident'.

Points to consider

- Organise proper dissent with respect to a CISO Office
- Embed the role of the CISO
- Aim for a comprehensive policy instead of solutions for individual points
- Verify whether the officer is actually in charge

8. Digital crime has become a business model

Serge Wallagh

In the 1980s, hacking was a cult. Small groups of nerds in their attics with beeping modems, rifling through computer systems where they were not supposed to be. United with one another by a strong sense of hacking ethics and a fascination for technology. A bygone world brilliantly described in the classic 'Hackers: Heroes of the Computer Revolution' by Steven Levy. Cybercrime has since become hard crime. The rise of globally connected systems, the increased complexity of systems and with that also often the vulnerability of society and the insight that a lot of money can be made from computer crime prompted an explosion. On the one side are the 'good guys': the specialists, legislators, managers and well-meaning computer users. On the other is a growing legion of criminals who are trying in every conceivable way to make money from their ruthless digital crime. If cybercrime were a country, it would be the third largest economy in the world in 2021, with a loss item of almost 6 trillion dollars annually. That is more than the total illegal drug trade worldwide. Fighting this therefore requires major investments and global coordination: a War on Computer Crime. How do these criminals make money? We take a look at some of the most common means of abuse, roughly in order of increasing damage, to get a good picture of what we are actually up against.

Sextortion

Digital crime comes in all shapes and sizes these days. A relatively new form of making money from cybercrime is 'sextortion'. Victims - usually minors - are seduced into sharing compromising photos.[149] The extortionists then threaten to disseminate the photos if they are not given money, and sometimes other services. In terms of sums of money worldwide, not a major area of crime, but one that has

[149] https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime

an enormous impact on the individual. Enough reason for the FBI to start up a special campaign.[150]

Twilight zone

A diffuse area between legal and illegal is that of espionage software, now a business involving millions. A key country in this regard is Israel. Israeli ex-military experts often working at commercial organisations are developing world-class offensive and defensive cybersecurity software. The Pegasus spyware from the Israeli NSO Group can be used by investigative authorities and governments to remotely monitor the phones of targets and harvest data. Espionage organisations can read out *all* the data from a mobile phone, including calls and data stored in the cloud. The spyware can then deinstall itself to delete any traces of data theft. NSO claims the purpose of its software is to track down terrorism and serious crime, but in practice the software emerges also to be used to monitor politicians, activists, lawyers, journalists, religious leaders, etc. NSO itself says that it has no direct insight into the use of the products. [151]

You're a winner

A textbook computer crime, but one that is steadily evolving, is 'phishing': a method of using misleading emails and websites to get a hold of people's personal data.[152] Many of us may smile remembering the time of poorly written emails from Nigerian princes wanting to transfer funds, lotteries in which we had won fantastic monetary prizes or unknown Bitcoins that it turned out we owned. The emails have now become more professional and targeted.

They play on current issues (COVID, parcel deliveries at home, etc.) and make use of credible data obtained from public and semi-public sources. This 'spear phishing' is thus specifically targeted to an individual. Studies show that 1 in 5 people is (ultimately) caught by this kind of spear-phishing email.[153] Sometimes it involves an immediate gain through the securing of bank details, but usually it involves installing malware (software that does something malicious), which is then

[150] https://www.fbi.gov/news/stories/stop-sextortion-youth-face-risk-online-090319

[151] https://www.nrc.nl/nieuws/2021/07/19/pegasus-verschaft-zichzelf-toegang-tot-alles-op-je-mobiel-a4051651

[152] https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

[153] Whitepaper 'What we learned from sending millions of phishing emails', phished.io

the prelude to much greater misery: the beginning of ransomware. I will return to this later.

Better well stolen than poorly invented

Simply stealing information is of course still an extremely important source of income for cybercriminals. Stolen commercial data, patents and other trade secrets are big business. Sometimes this still takes place relatively amateurly, by the combination of insiders and poorly secured systems. The recent theft of GGD data is an example of this. Two GGD employees stole personal data from the GGD's coronavirus test registration system and offered these data up for sale.[154] A low-tech data theft, with a high chance of being caught.

An incident that took place in March 2021 was already a bit bigger. It emerged at that time that personal data, possibly from millions of Dutch car owners, had been stolen and were for sale online.[155]

But it can also be done much more professionally. The best known recent example of this is the SolarWinds hack. In this incident, malware was spread via the update software of the SolarWinds software company, without it knowing. This enabled hackers to gain access to thousands of systems, including US government systems. The attack went unnoticed for months, allowing it to spread worldwide. The US Cyber Command, whose job is to protect US networks, was 'caught unawares' by the attack. It was a private company (FireEye) that discovered the attack after its own systems were hacked. Some organisations are probably still unaware that they were victims and that their data may potentially have been stolen.[156] It is therefore not clear what precisely was stolen in this worldwide hack, where the data went and for how much money. What makes this attack all the more interesting is that there are strong indications that the Russian government was behind it.

Your money or your data

Ransomware is the undisputed money-maker of the cybercrime world. A hyper-professional billion-dollar business with far-reaching specialisations, intensive

[154] https://www.ad.nl/binnenland/verdachte-ggd-datadiefstal-was-op-zoek-naar-gegevens-bners-ik-heb-echt-domme-dingen-gedaan~ab25d295/

[155] https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

[156] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?international=true&r=US&IR=T

international collaborations, the use of the latest technology and often an interplay between governments and the private sector.

What exactly is ransomware? In essence, it is very simple. You manage to gain access to another party's systems, on which you install software which encrypts all the files. You then demand money from the affected party in exchange for decrypting the files. As a secondary source of income, you can also blackmail the victims: if they don't pay up, the secret, commercial or privacy-sensitive data will be disseminated on the internet unencrypted.

The biggest name in ransomware is Revil: a hacker's group suspected to have ties with the Russian government.[157] Revil proved capable of injecting its malware into the software of (innocent) company Kaseya. Kaseya provides software that allows ICT companies to manage their clients' systems.[158] This kind of software needs to have many permissions on the clients' systems and is thus ideal for spreading malware. Within a brief period, thousands of companies worldwide turned out to be infected. Revil's Russian ties were obvious in this spread: as soon as the malware registered that it had infected a Russian company, the malware deactivated itself.

The large sums of money involved became clear at the beginning of June when the gang collected 11 million dollars from the world's biggest meat processor, Brazilian company JBS. Revil recently demanded as much as 70 million for the release of the data.

An interesting Dutch twist to this ransomware attack involves the Dutch volunteer organisation DIVD (Dutch Institute for Vulnerability Disclosure). A vulnerability used in the hack had already been discovered by this group prior to the attack. DIVD worked with Kaseya on a solution[159] but it turned out that the damage had already been done worldwide, unfortunately.

Revil is not the only player in this area, however. DarkSide is another active ransomware gang. In May 2021, the FBI managed to seize its servers and a large part of the ransom money collected by DarkSide, after it had extorted 4.4 million dollars from US fuel pipeline company Colonial Pipeline. The US Justice Department

[157] https://www.rtlnieuws.nl/tech/artikel/5240065/revil-ransomware-evil-rusland-amerika-hackers-gijzelsoftware-losgeld

[158] https://tweakers.net/reviews/9204/wat-weten-we-over-de-kaseya-ransomwareaanvallen.html

[159] https://fd.nl/ondernemen/1390703/grote-russische-hack-treft-ook-nederlandse-bedrijven-mzg1cakCgzGI?utm_medium=social&utm_source=email&utm_campaign=earned&utm_content=20210726

decided to henceforth give ransomware the same investigative priority as terrorism.[160]

Ransomware has become an ecosystem, with various specialised 'companies'.[161] The first are the software developers, who develop the ransom software. They lease out their software ('Ransomware as a Service') to the real hackers who use it to commit the actual breaches. With the software, the hackers get 24/7 support, bundled offers, user reviews, forums and other functions that are identical to those of legitimate software providers.[162] The developers often get a percentage of the takings. After the hackers have broken into a company, they hand over access to data managers, who are specialised in tracking down valuable data in an organisation and then encrypting this.

Then the extortion begins. This is done by special negotiators, possibly assisted by 'chasers', a sort of second-line negotiator that puts extra pressure on the client. Finally, there are also financial experts involved to securely get control of and launder the money.

Revil has since disappeared entirely from the world front.[163] Its servers are offline. It is not clear why this happened, but it is strongly suspected that this was due to the influence of the US government.

The Good Guys

Finally, there are also *good* parties who make a great deal of money from cybercrime, albeit much less than the criminals. Firstly, the technical specialists and IT security companies earn a good living, of course. A much larger earning market is now that of digital-related insurance, including crime as an uncertain event. Cyber insurance is becoming increasingly advanced, so that companies have a one-stop shop for responding to hacks. Insurance companies work with enormous teams of lawyers, technical and forensic experts and negotiators to help victims manage and recover from a ransomware attack,[164] all parties who also make money from this. A lucrative business.

[160] https://www.nrc.nl/nieuws/2021/07/10/cyberbende-revil-verslikt-zich-in-te-grote-prooi-a4050602

[161] https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

[162] https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

[163] https://www.volkskrant.nl/nieuws-achtergrond/plotseling-is-de-russische-hackgroep-revil-van-de-aardbodem-verdwenen-maar-waarom~b4cab740/

[164] https://edition.cnn.com/2021/07/13/tech/ransomware-negotiations/index.html

Conclusion

It is no secret that the world is becoming more and more dependent on ICT. It is therefore logical that this attracts crime, unfortunately. The coming together of hard crime, geopolitical support and limited manpower and knowledge at investigation services and victims means that to date, there has been a growing illegal industry with many branches. There are big opportunities to make money, the profits are enormous and the chances of getting caught especially small. The only way to put a stop to this is to invest substantially in knowledge, education, investigation and damage control on the 'good side'. Whilst coordinating worldwide, because no single country is strong enough (in terms of knowledge and money) to protect itself in isolation. What is needed is a worldwide War on Computer crime.

Points for attention

- In terms of scope, cybercrime is comparable to or bigger than drug crime.
- Cybercriminals are becoming increasingly professional and specialised.
- There are strong suspicions that state actors are involved as well.
- Fighting cybercrime is becoming an increasingly extensive ecosystem of specialists and parties. A worldwide War on Computer crime.

9. Digital Security at municipalities: A top-level issue!

Kato Vierbergen

The responsibility for digital security at municipalities touches on multiple domains, each of which generates its own risks and calls for different solutions. Firstly, municipalities are responsible for the continuity of the municipal service provision and operations (information security). Secondly, they are facing incidents in the public space that arise from digital disruption. Thirdly, based on their responsibility for public order and safety, they play a role in fighting digital crime. This article describes the manifold administrative responsibility that municipal governments have in this, what room for manoeuvre the administrator already has and what fundamental questions are now being investigated.

Manifold administrative responsibility

The thinking on digital security is broadening both inside and outside of city halls. The development of 'smart cities' is raising new questions. For example, who, on the basis of what legitimacy, may monitor residents online, collect data or decide how the citizen can be protected against privacy violations or against unsecure technology? Technology can also cause a city to in fact become less safe or less democratic. Administrators are being called to account for their responsibility in the event of outages or disruptions to the digital society. The openness shown by the administrators of Lochem[165] and Hof van Twente[166] makes it clear that an incident directly touches on their responsibility. Safeguarding the digital security of the

[165] https://www.lochem.nl/laatste-nieuws/nieuwsbericht/gemeentenieuws/gemeente-lochem-door-het-oog-van-de-naald-bij-hack-2553

[166] https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2021/03/artikel/hof-van-twente-cyber-hack-stevige-les-voor-ons-1872

municipality requires efforts from the municipal governments on multiple terrains.[167]

Still important to have one's own house in order

A reliable and secure government calls for thorough information security and privacy protection of the municipal information management. It is still necessary to have and keep 'one's own house in order'. The municipality itself will have to remain sufficiently resistant to ever-evolving digital threats, for instance. The threat assessment of the Information Security Service (IBD) 2021[168] of the VNG; the cybersecurity assessment of the Netherlands[169] and the increasingly serious ransomware attacks like at Hof van Twente make that clear. Municipalities are working to constantly improve that digital resilience and spoke out on this unanimously in the Digital Security resolution in February 2021.[170] They also see that it requires a great deal from the administration, the civil service, IT facilities, providers, as well as in the cooperation between municipal partners and coordination between the various existing digital and regular security structures. The risk management at the municipalities will have to be aligned with these digital risks and the risks of chain partners must be charted out. For the municipalities and government organisations in the chain, the Government Information Security Baseline (BIO) serves as the basis for information security and privacy protection, both in the organisation itself and in the cooperation and data exchange as part of municipal schemes, with other chain partners and for outsourced private-law tasks or services. This requires insight into the degree to which the service provision of the organisation itself, its supplier or chain partner is vulnerable to breach or disruption at the interface and demands openness from both sides. The Information Security Service (IBD) for the municipalities is the sectoral Computer Emergency Response Team (CERT), [171] with its specialised team of ICT professionals who are able to act rapidly in the event of a security incident involving computers or networks. The IBD supports municipalities with their information security, both by

[167] https://vng.nl/sites/default/files/2021-01/08_resolutie_digitale_veiligheid.pdf

[168] https://www.informatiebeveiligingsdienst.nl/nieuws/dreigingsbeeld-informatiebeveiliging-2021-2022/

[169] https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

[170] https://vng.nl/nieuws/meer-prioriteit-voor-beveiliging-digitale-systemen-gemeenten

[171] https://www.informatiebeveiligingsdienst.nl/ibd-cert/

providing advice and warnings about vulnerabilities, and by taking on a role as a supporting 'digital fire brigade' in the first response to incidents.[172]

The municipalities are supported in their reporting on digital security, the BIO and various government-wide standards with a Single Information Audit Unified Norm (ENSIA).[173] Provinces, water boards and a few divisions in the national government also use ENSIA to render account. The reports on the state of information security form a good basis for a periodic discussion between administration, management and the organisation's own Chief Information Security Officer (CISO). This helps to increasingly get a better grip on digital security and the way in which digital resilience and capacity for recovery is set up.

Preventing digital disruption[174]

In addition to responsibility for the security and continuity of the municipality's own municipal processes and chain processes, municipal governments are also responsible for any consequences of digital insecurity that could disrupt society. Together with (social) partners, they are involved in various socially relevant processes the loss or disruption of which could cause social disruption. Municipalities have an interest in these processes continuing undisturbed but are not responsible for all aspects. They can stipulate digital security requirements for events and business activities that are subject to permits. It is relevant in this context that the municipality knows how to enforce these requirements and how, together with the organisation or other municipalities and/or the security region, it can act to make a cyber incident or crisis manageable and resolve it. This became clear during the hack at Senzer[175] and IJmond werkt!,[176] public employment services that implement the Participation Act for the labour market regions for multiple municipalities, which also jeopardised the payment of social assistance benefits and the temporary bridging scheme for independent entrepreneurs (Tozo). Apart from the fact that a business or the institution may be able to resolve the incident itself

[172] In 2019, BZK/DGOO/DO, in the guise of the Joint Government Security Operations Centre (GOV-SOC), handed over the results of its inquiry to the administrative layers that utilise the outcomes to strengthen the incident response capacity of their own administrative layer.

[173] https://www.vngrealisatie.nl/ensia

[174] The WRR report 'Voorbereiden op digitale ontwrichting' [Preparing for digital disruption] of 20 March 2020: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.

[175] https://www.senzer.nl/netwerkinbraak

[176] https://www.ijmondwerkt.com/2021/10/04/uitbreiding-veelgestelde-vragen-30-9/

in first instance, it could also have an effect on the social living environment, as a result of which the municipality or municipalities may be affected. In addition to ensuring the continuity of service provision and communication to persons involved from the affected organisation, further containing the impact could be one of the tasks of the municipality. All in all, data security goes beyond the responsibility of the municipal CISO and is by its nature an administrative issue.

Does the analogy with physical security work in all respects?

This manifold responsibility brings with it complex governance. It requires a different view on the existing administrative responsibilities, in order to identify these socially relevant processes with the corresponding relevant (chain) partners, from the perspective of digital security.

In the physical security chain, industrial sectors such as water, transport and energy are currently designated as vital sectors. There the link with the security of digitally-managed operational technology and measurement and regulation systems has already been made. Here, 'safety' and 'security' coincide and are already 'a top-level issue'. As socially relevant processes are worked out, the thinking about digital security will have to be further integrated with the regular conceptions in relation to security. From the policy departments of Justice and Security and Home Affairs and Kingdom Relations, research is being carried out together with the VNG into the most important local processes that are crucial in the event of social disruption.[177] Following on from the perceptions of the vital sectors, a municipal map of socially relevant processes, possible effects of digital disruption, the possible (digital) interventions and the appropriate perspective for action will be developed. This produces a top 10 of the key socially relevant processes in which municipalities have an interest, but in which they might not be responsible for implementation. Focused on the potential incidents in those processes, an (administratively) adequate crisis role[178] and approach can be

[177] Investigation was promised by the Minister of Justice and Security in the government response to the WRR report 'Preparing for digital disruption' https://www.digitaleoverheid.nl/document/kabinetsreactie-op-het-rapport-voorbereiden-op-digitale-ontwrichting-wrr/.

[178] In 2020, the Digital Government department of Home Affairs performed the *Quick scan preparation for digital disruption*. https://www.rijksoverheid.nl/documenten/rapporten/2021/01/31/quick-scan-voorbereiding-op-digitale-ontwrichting. Preparation for digital disruption is defined herein as: *'Being prepared to combat*

developed. For municipal responsibility in combatting the effects, optimal connection will need to be sought with the National Digital Crisis Plan (NCP-Digitaal).[179] The NCP-Digitaal offers rapid insight and an overview of the possible effects of measures, roles, tasks and authorities on the national level at the time of a digital crisis. A number of municipalities have appointed a so-called 'resilience officer'. The cooperation with the Institute for Physical Security (IFV) and the Security Regions, as professionals in crisis management and consequence response,[180] is important so that a relevant and up-to-date programme of drills can be coordinated for the municipal digital domain, one set up from the basis of both areas of responsibility. Drills are a tried and tested means of determining whether incident and crisis management are properly set up. In the physical domain, this is a 'no brainer' and common practice; in the digital domain it will first have to be worked out when local and when regional response is appropriate, and what specific digital crisis structure will be necessary.

Digital public order and security

A genuinely new development is the attention to public order disturbances instigated online,[181] whereby social media is used to incite people to quickly organise to disturb the public order. Disinformation is actively disseminated with the goal of pitting people against each other, casting doubt on information from the government and thus putting pressure on democratic values. Online, people seem less aware that they are committing criminal offences. Residents also come in contact with radical groups more easily online and hate crimes take place in the digital world, with repercussions in the physical reality, as occurred in Bodegraven.[182]

At the same time, residents and businesses are increasingly online. Different forms of crime take place primarily online, from bank fraud to child abuse.

the effects of a serious "local" disruption to social core processes, which is related to cyber incidents whereby the continuity of service provision and/or crisis management falls under the responsibility of local governments in connection with existing crisis structures.'

[179] https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal

[180] https://www.ifv.nl/kennisplein/Paginas/bestuurlijke-netwerkkaarten-crisisbeheersing.aspx

[181] https://hetccv.nl/onderwerpen/cybercrime/cyberweerbaarheid-gemeenten/online-aangejaagde-ordeverstoringen/

[182] https://www.ad.nl/binnenland/burgemeester-bodegraven-als-het-nodig-is-laten-we-complotverspreiders-gijzelen~a0c62a93/?referrer=https%3A%2F%2Fwww.google.com%2F

This also calls for attention to safety and enforcement so that residents can feel safe online as well. The Rathenau Institute indicates in its research into harmful and immoral behaviour online that even online behaviour that is not directly illegal can still be harmful and immoral.[183] They argue for a more proactive government. *'A government that not only responds once behaviour has already been detected, but which also intervenes proactively in the online environment, so that damage is prevented and constitutional rights of citizens are protected.'* For mayors, it is relevant to know whether, after people are incited, the public order is actually jeopardised and what perspective for action is available for (proactive) intervention in these security issues. The digital security operating framework[184] can help administrators prepare for digital security problems.

In the fight against digital crime, the municipality supports vulnerable residents and businesses. The parallel with the division of responsibility and room for manoeuvre of the municipal administrators in the physical world is also being investigated here. Cybercriminals do not adhere to municipal boundaries in this context. They are persistent and have plenty of time and money to put into targeted attacks on digitally vulnerable spots for the municipality, business owners and residents. Cybercrime and cyber-enabled crime[185] are growing concerns in the city's security policy. 'Digitalised crime', 'healthcare and security' and 'information position' were added to the Core Security Policy in 2021.[186] It is important to each time sharpen the interaction between the powers of the police, Public Prosecutor's Office and the municipality so that they can continue to respond adequately. The VNG is therefore working with the ministries, Security Regions and police, the Centre for Crime Prevention and Safety (CCV) and the IFV on a number of cyber resilience projects in the municipalities.

Conclusion

An outage in socially relevant processes as the result of digital incidents in the municipal service provision, public order disturbances incited online or digital crime

[183] At the request of the Research and Documentation Centre (WODC), the Rathenau Institute carried out a study into harmful and immoral conduct online. https://www.rathenau.nl/nl/digitaal-samenleven/online-ontspoord

[184] https://vng.nl/nieuws/handelingskader-lokaal-bestuur-in-een-digitale-samenleving

[185] Explanation on the distinction in the letter to parliament from the Minister of Justice and Security: https://www.rijksoverheid.nl/documenten/kamerstukken/2021/06/28/tk-integrale-aanpak-cybercrime

[186] https://vng.nl/artikelen/kernbeleid-veiligheid-2021

can cause social disruption, possibly with effects in the physical realm. The mayor is responsible for maintaining public order and safety and, together with the security region, for crisis management in the event of major incidents, in the digital domain as well. It is being investigated where the analogy with the room for manoeuvre that administrators have in the physical domain fails to apply for digital security. The responsibility for that broader digital security reaches beyond the responsibility of the municipal CISO. Digital Security is a public administration issue, 'a top-level issue'. The manifold responsibility brings with it complex governance, which, in addition to requiring substantive knowledge, is a difficult subject for administrators to adequately manage. Digitalisation and cybercrime reach beyond borders and the complexity of the issue is too big for every municipality to process on its own.

Points for attention

- Current events mean that digital security issues are addressed in different forums, from the basis of different policy responsibilities at the Ministries of Justice and Security, Home Affairs and Economic Affairs. From the VNG Digital Security Agenda, this is channelled to the various relevant municipal officials and VNG regulates the administrative burden. This makes it more manageable for the municipalities so that it has an effect in implementation.
- There is scarce capacity for Public Order and Security and information security in the Netherlands, and it is difficult to attract suitable people; for research, policy and at municipalities. Fundamental research is still needed for many policy questions. The scarce capacity in this digital security domain can be optimally deployed through targeted connection with research initiatives and the administrative strengthening of coalitions focused on research and development of the field.

10. Security by Design: new buzzword or the magic word in the fight against cybercrime?

Natascha van Duuren

Cyber attacks and data leaks top the list of risks that worry administrators the most. And for good reason. Data leaks have become commonplace and cyber attacks are becoming more prevalent. 'Privacy by Design', 'Privacy by Default' and 'Security by Design' are terms that are often used in this context. What do these terms mean exactly and what concrete significance do these terms have for organisations and businesses? And, last but not least, is Security by Design the solution for our (justified) concerns about cybercrime? A brief explanation.

Initial introduction to Privacy by Design

The concept of Privacy by Design was introduced in the 1990s by the Canadian privacy regulator Ann Cavoukian. The term 'privacy-enhancing technologies' (PETs) already existed. Ann Cavoukian felt that 'a more substantial approach' was required. In other words, not only technical, but also organisational and physical measures. Ann Cavoukian introduced the 7 foundational principles:

- Proactive not reactive - preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality - positive-sum instead of zero-sum
- End-to-end security - full lifecycle protection
- Visibility and transparency — keep it open
- Respect for user privacy — keep it user-centric

The 7 principles of Privacy by Design in effect also introduced Privacy by Default (by way of the principle 'Privacy as the default setting') and Security by Design (by way of the principle 'End-to-end security - full lifecycle protection'). According to

Ann Cavoukian, powerful security measures from start to end are essential for maintaining privacy.

Implementation of privacy by design in our legislation and regulation

Ann Cavoukian's view caught on. The principles of Privacy by Design have since been codified.

For instance, the General Data Protection Regulation (GDPR) imposes Privacy by Design (Article 25(1) GDPR) and Privacy by Default (Article 25(2) GDPR) as requirements, although these terms are not explicitly stated. There have been comments in the literature about the abstract character of Article 25 GDPR. It has been said, for instance, that the requirements contained in this article occupy a middle ground between an abstractly formulated principle and a more or less concrete assignment. [187]

This criticism is justified, in my opinion. Read carefully, Article 25(1) GDPR mentions just two concrete obligations:

- Data minimisation (also see Article 5(1)(c) GDPR): collect only strictly necessary data
- Pseudonymisation (also see Article 4(5) GDPR)

The GDPR also contains a number of separate provisions with obligations closely related to Privacy by Design & Default. You could also put it differently: in order to satisfy these obligations, it is necessary to apply Privacy by Design:

- Encryption (Art. 6(4)(e), Art. 32(1)(a) GDPR)
- Storage (Art. 5(1)(e) GDPR)

Interpretation in practice

The question is: How must these (to some extent abstract) obligations be implemented in practice? What footing do businesses and organisations have in this respect?

In 2015, even before the introduction of the GDPR, ENISA[188] endeavoured in its report 'Privacy and Data Protection by Design – from policy to engineering'[189] to build a bridge between 'the legal framework' and 'the available technologies

[187] See, for instance, H.J. Bolte in 'EDPB richtlijnen over Data Protection by Design en Default' in Privacy & Informatie (P&I),

[188] European Union Agency for Cybersecurity

[189] https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

implementation measures'. Four years later, the EDPD[190] published guidelines[191] on the use of data protection by design and default. Despite the well-meaning attempts, the guidelines do not provide the starting points envisaged. An examination of the guidelines, in my view, prompts the conclusion that just a few examples and points of reference are given, but that the guidelines remain relatively abstract. The same applies for the ENISA report published earlier.

ENISA incidentally reached this conclusion as well. In its report 'Guidance and gaps analysis for European Standardisation',[192] it arrives at the following observations, among others:

- Despite a general common agreement on the value of privacy by design, the concept and its implementation are still not clearly elucidated in standardisation activities;
- Proving compliance with privacy standards in information security is not as straightforward as one would expect. While there are some approaches for conformity assessment available in specific sectors, others are still lacking appropriate mechanisms;
- A consistent analysis of sector-specific needs for privacy standardisation is essential, especially in the context of information security;
- Since the references to standards in the Union legislation are becoming more regular, and there are considerable differences of Union privacy and security regulations with other jurisdictions, the need for analysis of mapping of international standards and European regulatory requirements is intensified.

ENISA broaches an important point with this last observation. Privacy and cybersecurity standards will have to be developed on the European level and not just on the level of an individual country.

Security by Design and the Dutch government

An interesting question in this context is: how does the Dutch government deal with Privacy by Design, more specifically Security by Design? Digital security is, after all, inextricably bound up with national security. The importance of Security by Design in government automation is undisputed and was recently underscored once again when a data leak was found in the GGD's systems. The letter to

[190] European Data Protection Board

[191] Guidelines 4/2019 on Article 25 Data Protection by Design and Default

[192] https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation

parliament from State Secretary Knops of the Ministry of Home Affairs in response to the motion from Kröger et al. explicitly mentions 'Privacy by design', as well as the 7 principles from Ann Cavoukian. This letter refers to the government-wide measures already taken, including the instrument Government Cybersecurity Procurement Requirements (ICO). At the same time, the State Secretary indicates that these measures must be further supplemented based on the seven principles.[193] It is also explicitly cited in the Cyber Security Assessment Netherlands 2021[194] from the NCTV[195] and the NCSC[196] that a baseline[197] is not sufficient and the need for further regulation is acknowledged.

Responsibility for Security by Design

Assuming that the European and Dutch intention to further flesh out Privacy (and therefore Security) by Design is actually realised, the question is: who is responsible for correct application of that? Based on the GDPR, Privacy and Security by Design is an obligation of the data controller (who is in many cases the principal). The practice is, however, that data controllers do not develop software themselves and that too few requirements are often stipulated for security by the principal. As a result, the vulnerabilities in the software often do not come to light until the use phase, and sometimes not until the moment a cyber incident occurs. That is an undesirable situation, of course.

It would therefore be good if the obligation of Security by Design were to be also addressed directly to developers and software providers. Particularly for standard software, it should be the case, in my view, that a purchaser should be able to trust that Security by Design was applied in the development of the software: End-to-end security, full lifecycle protection (whereby the application and use of standard software is likewise decisive for security and these factors naturally lie outside the control and responsibility of the developers and software providers). This brings us back to another point, specifically that further fleshing out will first have to take place on the European level with respect to the obligations that Security by Design entails. (To avoid making it even more complex, and to keep it

[193] This is expected to be filled in in the course of 2021.

[194] https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

[195] National Coordinator for Security and Counterterrorism

[196] National Cyber Security Centre

[197] https://www.ncsc.nl/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen

somewhat manageable, we leave the global character of digitalisation outside of consideration for the time being).

Conclusion

Security by Design is not a new buzz word. It has been around since the 1990s and has since been codified. The importance of Security by Design as part of Privacy by Design in the fight against cybercrime is undisputed. The lack of a definition and concrete fleshing out of Security by Design on the Dutch and European level means, however, that it is at present not adequately clear for administrators and developers what precisely is expected of them. To withstand cyber risks, it is important that this concept be further fleshed out in the short term.

Points for attention

- Security by Design is an important instrument in making an organisation resilient in the face of cybercrime; the earlier security issues are included in the development process, the more impact the measures will have;
- The GDPR takes accountability as a basic premise. It is therefore important to document how the obligation of Privacy & Security by Design is complied with;
- In the absence of concrete points of reference for the specific details of Privacy & Security by Design, organisations and businesses would be wise, for the time being, to follow the existing guidelines/baselines closely, supplemented with a risk analysis on the organisational level;
- Directors and administrators at data controllers are responsible for dealing with digital risks adequately;
- As long as the obligation of Privacy & Security by Design is not (also) addressed to developers and software providers directly, it is important to impose concrete requirements on developers and software providers (and to document these requirements in turn in the context of accountability).

11. Bulgaria and artificial intelligence in cybersecurity

Dimiter Velev and Plamena Zlateva

The contemporary world relies - more than ever before - on an exponential scale of the recent advances of information and communication technology (ICT). Naturally, the ICT developments bring a new quality of life and business but they also carry new possibilities of misuse. The growing number of users, devices and programs in today's complex technological environment, together with the large volumes of data generated in all computing and communication processes, increase the risk of cyberattacks and their possible negative consequences substantially. Traditional approaches, which use conventional security techniques and systems against defined and well-known threats, are no longer reliable enough. Hence, a more active, adaptive and intelligent approach is necessary. One viable solution could be the use of artificial intelligence (AI) in cybersecurity.

Basic principles: cybersecurity

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Cybersecurity measures are designed to combat threats against networked systems and applications in the cases such threats originate from inside or outside of an organisation[198]. The measures are used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems[199]. The cybersecurity term applies in a variety of contexts, from business to mobile computing, and it can be divided into a several common categories[200]:

[198] IBM (2021) *What is cybersecurity?,* https://www.ibm.com/topics/cybersecurity

[199] Shea Sh., Gillis A. S., Clark C. (2021) *What is cybersecurity?*, Tech Accelerator https://searchsecurity.techtarget.com/definition/cybersecurity

[200] Kaspersky (2021) *What is Cyber Security?*, https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

- Network security – protects computer networks from intruders.
- Application security - keeps software, its data and devices free of threats.
- Information security - protects the integrity and privacy of data.
- Operational security includes the processes and decisions for handling and protecting data assets.
- Cloud security - encrypts cloud data at rest, in transit and in use to support customer privacy, business requirements and regulatory compliance standards.
- Internet of Things security – provides protection to critical and non-critical appliances such as sensors, WiFi and other communication channels.
- Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data.

The aim of cybersecurity is to fight the following major threats[3]:

- Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.
- Cyberattack involves politically motivated information gathering.
- Cyberterrorism has the aim to undermine electronic systems to cause panic.

The most common types of cybersecurity threats are divided into the following categories[201]:

- Social engineering - trick the user into revealing sensitive information, which could lead to monetary payments or gaining access to user confidential data.
- Malware - software designed to gain unauthorized access or to cause damage to a computer.
- Ransomware - type of malicious software to extort money by blocking access to files or the computer system until the ransom is paid.
- Phishing - sending emails that mimic emails from trusted sources to steal sensitive data such as login information or card numbers.

[201] Cisco (2021) *What Is Cybersecurity?*, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Basic principles: AI

Intelligence concerns the human brain, mind, involvement, logical thinking, understanding, and applicability. In general, intelligence can be well defined as an individual's capability to do things effectively by using own knowledge, interpretation, and insight. The term 'artificial intelligence' (AI) was defined by John McCarthy, a Stanford University emeritus professor of computer science, "as the science and engineering of making intelligent machines", particularly intelligent software programs. Artificial intelligence leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind. AI combines computer science and large datasets to enable problem-solving[202].

Various AI domains of are defined[203]:

- Machine Learning teaches a machine how to make inferences and decisions based on past experience by evaluating data.
- Deep Learning teaches a machine to process inputs through layers in order to classify, infer and predict the outcome.
- Neural Networks represent algorithms that capture the relationship between various variables, and processes the data as a human brain.
- Natural Language Processing reads, understands, and interprets a language.
- Computer Vision identifies an image by decomposing it and studying different parts of the objects.
- Cognitive Computing mimics the human brain by analyzing text, speech, and images in a way the human does and tries to give the required output.

Three types of AI are expected to fully develop in time[204]:

- Artificial Narrow Intelligence (ANI) – existing AI systems solve a single problem in a better manner than a human can, but they generally have narrow (limited) capabilities. They come close to human functioning in specific contexts, surpassing them in many instances, but only excelling in very controlled environments with a limited set of parameters.

[202] Copeland B.J. (2021) *Artificial Intelligence*, Britannica https://www.britannica.com/technology/artificial-intelligence

[203] Wikipedia (2021) *Artificial intelligence*, https://en.wikipedia.org/wiki/Artificial_intelligence

[204] Advani V. (2021) *What is Artificial Intelligence? How does AI work*, Types and Future of it?, https://www.mygreatlearning.com/blog/what-is-artificial-intelligence/

- Artificial General Intelligence (AGI) is still a theoretical concept, defined as AI which has a human-level of cognitive functions, such as language and image processing, reasoning.
- Artificial Super Intelligence (ASI) is expected to surpass all human capabilities in the near future. This will include decision making and taking rational decisions.

AI in cybersecurity

The AI can quickly analyze millions of events and identify many different types of threats, ranging from malware exploiting daily vulnerabilities to identifying risky behavior that lead to phishing attacks or malicious code download. The technology has the ability to learn constantly in time to identify new types of attacks. AI is able to detect and respond to deviations from established norms based on existing profiles of users, assets and networks.[205,206]

With the help of AI the following cyber threats can be handled:[207,208]

- Password Protection and Authentication – AI can be used to improve biometric authentication and eliminate any weaknesses.
- Credit card fraud prevention - Unusual activity, such as purchases made from a different device or unusual transactions can be instantly detected using AI services that help verify the user.
- Phishing Detection and Prevention Control – AI can understand all types of phishing attacks despite their geographic origin.
- Vulnerability Management - multiple factors can be examined and analyzed to determine when a threat is pending.

[205] Balbix (2021) *Using Artificial Intelligence in Cybersecurity*, https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

[206] European Union Agency for Cybersecurity (ENISA) (2020) *AI Cybersecurity Challenges*, https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

[207] Stefanini (2021) *The New Role of Artificial Intelligence in Cybersecurity: How Can It Protect Your Business?*, https://stefanini.com/en/trends/news/role-of-artificial-intelligence-in-cybersecurity-to-protect-busi

[208] Kaspersky (2021) *AI and Machine Learning in Cybersecurity — How They Will Shape the Future,* https://www.kaspersky.com/resource-center/definitions/ai-cybersecurity

- Network Security – AI monitors and learns network traffic patterns. Thus, the creation of security policy and definition of network topography in an organization are enabled successfully.
- Behavioral Analytics – AI algorithms can learn and create a pattern of a user behavior by analyzing how he uses his device and online platforms. When the AI algorithm notices unusual activities that are outside the typical behavior, it can flag it as suspicious or block the user.
- Breach Risk Prediction - AI systems help determine the IT asset inventory which is an accurate and detailed record of all devices, users, and applications with different levels of access to various systems.

Despite those promising possibilities, it should be noted that AI can be used by adversaries - cybercriminals can take advantage of the same AI systems for illegal purposes. Research shows that protection against AI attacks is a complex challenge requiring multiple approaches to ensure security. Adversarial AI causes machine learning models to misinterpret inputs into the system and behave in a manner which is favorable to the attacker[209]. Therefore, secure AI solutions must be a top priority for all organizations.

Bulgaria

A fully integrated National Cybersecurity Ecosystem with the ability to adapt to the dynamics of global cyber threats and to respond to large-scale attacks on Bulgarian information resources, including integration into the European Union's cybersecurity system is a *strategic goal* defined in the National Development Program ‘Bulgaria 2030’. The Cybersecurity Act defines cybersecurity as a state of society and the state in which, by implementing a set of measures and actions, cyberspace is protected from threats related to its independent networks and information infrastructure or which may disrupt their work.

The updated National Strategy for Cybersecurity ‘Cyber Resilient Bulgaria 2023’ guarantees that the Republic of Bulgaria will be a reliable and sustainable partner and participant in common networks and systems and collective security

[209] Accenture (2019) *The new cyberattack surface: Artificial Intelligence*, https://www.accenture.com/us-en/insights/artificial-intelligence/adversarial-ai

with our Euro-Atlantic partners, with the capacity and ability to participate in preventing and overcoming evolving cyber threats and crises[210].

The concept for the development of Artificial Intelligence in Bulgaria until 2030 proposes a comprehensive vision for the development and use of AI. It is based on the strategic and programming documents of the European Commission, which consider AI as one of the main drivers of digital transformation in Europe and a significant key factor in ensuring the competitiveness of the European economy and a high quality of life. The main areas of impact and specific measures have been identified: building a reliable infrastructure for AI development; development of research capacity for scientific excellence; creating knowledge and skills for the development and use of AI; support for innovation in order to implement AI in practice; raising awareness and building trust in society; creating a regulatory framework for the development and use of reliable AI in accordance with international regulatory and ethical standards; creating conditions for financing and sustainable investments for the development of AI, use of AI in cybersecurity[211].

Conclusion

The world moves fast to a fully digitalized environment through a myriad of advanced information and communication technologies and concepts – Cloud Computing, Mobile Computing, Social Networking, Big Data, Internet of Things, Autonomous Vehicles, Industry 4.0, Society 5.0, et cetera., where colossal volumes of data are generated by the industrial systems that deploy those technologies, as well as of result a the active user collaboration over networks. Cybersecurity is at risk with those developments and new advanced security measures should be looked for to replace the traditional ones. The application of Artificial Intelligence techniques, algorithms and tools in cybersecurity are highly recommended, Managers and users must be aware of their potential use and benefits.

[210] Council of Ministers of the Republic of Bulgaria (2021) National Strategy for Cybersecurity "Cyber Resilient Bulgaria 2023", https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=5878

[211] Ministry of Transport, Information Technology and Communications of the Republic of Bulgaria (2020) *Concept for the development of artificial intelligence in Bulgaria until 2030.* https://www.strategy.bg/PublicConsultations/View.aspx?@lang=bg-BG&Id=5396

Points for attention

Artificial Intelligence in cybersecurity is a hot and emerging topic nowadays and some of the main advantages of its application can be defined:

- AI offers advanced password protection since it secures account authentication. AI uses various tools to improve biometric authentication and to eliminate any weaknesses.
- AI can process large volumes of data, which are exchanged between businesses and users; hence, it is able to detect any threats that are masked as normal activity. AI can identify unknown threats, since it successfully recognizes and stops them.
- AI accelerates detection and response time since it scans the entire information system and checks for possible threats, identifying them in advance and thus simplifying all security tasks.
- AI achieves better overall security, since its deployment can prioritize cybersecurity threats and tasks, and optimizes the order to process them.
- AI improves its performance in time since it constantly learns business network and user behavior through its application in cybersecurity domains. It recognizes the corresponding behavioral patterns, so it can stop any potential threats at an early stage.

12. Digital Security Risk Management for data centres

Raymond Bierens and Sander Nieuwmeijer

New digital technologies are increasingly transforming the way organisations work. Data centres play an important role in this transformation and are therefore considered critical national infrastructure in a growing number of countries. Without data centres, online digital services as we know them are unavailable, digital devices cannot be operated without connectivity and big data cannot be exchanged. But, like any organisation, data centres are also undergoing the same digital transformation themselves, which makes it very important to map and manage the corresponding risks. What exactly is the impact of the growing connectivity in the control and operations of these data centres?

The Netherlands a frontrunner in digital infrastructure

The Netherlands was the first country in the world linked up to the American internet as we now know it. As European initiator, and because of our favourable location, the Netherlands has always remained a frontrunner in digital infrastructure and is still a springboard to the rest of Europe. Because of its stable political climate and reliable power network, the Netherlands has an extremely favourable business climate for data centres. As a result, the Amsterdam Internet Exchange (AMS-IX) is one of the largest internet hubs in the world. This digital oasis also entails risks, however, which are still not always recognised or understood by everyone within organisations. The awareness of digital risks within organisations is therefore an important point for attention. Despite the fact that 63% of organisations are actively working on a digital transformation,[212] just 23% of the C-level devotes adequate attention to the digital risks arising from that.[213]

[212] https://www.rsa.com/content/dam/en/white-paper/rsa-digital-risk-report-2019.pdf

[213] https://www.rsa.com/en-us/offers/rsa-digital-risk-report-second-edition

Growing risks for data centres

Cloud computing, growing automation and remote working have increased the possibilities of attack. Hackers have seized on this to carry out waves of cyber attacks, which means the risks for data centres have grown. Cyber attacks on data centre control systems can cause system outage, production loss, injury or even loss of human life and have a major impact on a data centre’s reputation. The facilities infrastructures underlying the functioning of data centres are controlled using OT (operational technology). The OT ensures the proper functioning, security and availability of, among other things, the cooling equipment, power distribution and connectivity.

Merging the worlds of IT and OT

Diagram 1 provides a visual representation of the merging of the two previously distinct worlds of information technology and operational technology. With a view to efficiency, major steps have been taken by enabling IT and OT to communicate with each other. The Industrial Internet of Things (IIoT) is an expansion of the Internet of Things (IoT) for industrial applications.

IIoT components are intended for machine-to-machine communication. IIoT is used in data centres and is at the cutting edge of IT and OT. The use of smart sensors and actuators has brought about drastic improvement in the monitoring and control of physical infrastructures, and in remote access and control. But the digital threats are also increasing and the security risk is greater than ever before.

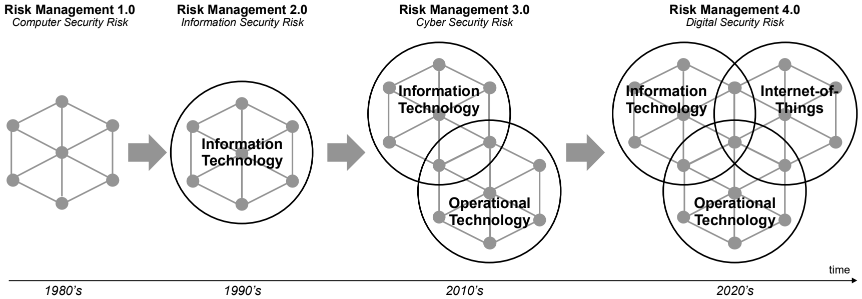


Diagram 1: Historical overview of the development to digital security risk management © Bierens 2020

In order to gain a good understanding of the impact of a data centre’s digital transformation, the dependencies inside and outside the data centre must first be mapped out. This encompasses more than requiring that a supplier holds an ISO certificate. It involves obtaining a comprehensive overview of all the technologies that are directly or indirectly connected with each other. More than 98% of all processors can be found in embedded systems (OT), not in PCs or servers (IT).[214] OT is connected to IT and IT is connected to the internet. In a world where IT technology is used by a Network Operations Centre, where the (OT) cooling equipment, for instance, is controlled remotely and sensors are increasingly connected to suppliers, mapped out this attack area requires the first step of digital security risk management. After all, if something has an IP address, the digital risks must be managed. Attackers could activate sprinkler systems, for instance, and destroy thousands of servers, or deactivate or tamper with cooling and/or energy systems to cause a fire or explosion.

Once mapped out, the attack area provides a comprehensive overview of all the connected technology used in the data centre. The second step is how the providers of all these technologies can be managed. It was not for nothing that the NIST framework was expanded from v1.0 to v1.1 to include, among other things, the topic of supply chain management. At the same time, supply chain management is a term that corresponds to the outdated cybersecurity risk management, while digital risk management 4.0 assumes that this supply chain concerns many more dimensions. After all, every connected technology has all sorts of hardware and software components that have been purchased from different suppliers and put together. As the 2020 SolarWinds hack demonstrated, these days even security software modules are programmed based on material acquired externally, which means that corrupted software (updates) already arises in the programming phase. In the event of digital security risk, therefore, we no longer talk about a supply chain, but rather an ecosystem of suppliers, which have been mapped out behind each of the connected technologies in the first part of digital security risk management 4.0. Simply assigning these risk management responsibilities to the supplier has proved to be inadequate too often in the past.

Complex ecosystem as the starting point for digital risk management

Taking the ecosystem as the starting point for digital risk management also makes clear how quickly the risks grow as technologies become more connected with each other. An unmanageable architecture quickly arises from this, in which the digital security is much more difficult to guarantee, as became visible in May 2021 in, among others, the ransomware attack on Colonial Pipeline in the US. The rapidly

[214] Cybervision 2025, United States Air Force Cyberspace Science and Technology Vision

growing number of devices in a network makes keeping a real-time overview of the dynamic attack area a necessary second part of digital security risk management. Good end-to-end network segregation and access management are essential parts of reducing the risks and their impact. This is easier said than done, because a segmentation within the data centre does not mean a segmentation of the suppliers of that connected hardware and software. It is precisely the growing desire on the part of suppliers for, among other things, energy efficiency and remote maintenance of operational technology that creates a risk for the continuity of that same technology. The question is justified, therefore, whether organisations have sufficiently considered whether the cost advantages and efficiency improvements generated by connectivity outweigh the risks.

At the same time, the ecosystem has become so complex and contains so many interdependencies that an outage is increasingly likely if one of the components in the ecosystem is hit. Take the Kaseya software hack in July 2021, which forced all the Coop supermarkets to close, for instance. And what to make of the collateral damage, like that at Maersk in 2017 as the result of the hacking of the accountancy software used by the port in Odessa? Not to mention the acceptable number of programming errors in software before it is released.[215]

The final component that makes digital security risk management unique is the starting point that it not only defines defined risk appetite, but also makes the residual risk explicit in order for it to be managed. What are the residual risks that could cause the operations to come to a standstill and what mitigating measures can be come up with to counter those? Because the fact that it will happen is a statistical certainty, the only question that remains is whether the data centre itself has given this enough thought in advance.

Conclusion

Data centres pose a double risk in terms of digital security. Firstly, for the organisation's own operations, which are increasingly connected internally and externally, as a result of its own digital transformations. Secondly, for the growing dependencies of the users of these data centres who will see their operations come to a standstill without the data centre. For this reason alone, data centres can and should be expected to set an example when it comes to digital security.

[215] Steve McConnel – Code Complete 2 (A Practical Handbook of Software Construction)

Points in conclusion

- Approaching risk management from the perspective of a dynamically evolving ecosystem connected internally and externally to the organisation, in combination with explicitly identifying and managing residual risks, makes digital security risk management uniquely suited to the business operations of data centres.
- Through early adoption in this regard, data centres can distinguish themselves within their own sector and provide clients with a higher degree of continuity assurance.
- Waiting too long will only make the risk of outage more likely, resulting in societal disruption, so there is no time to lose.

13. The unavoidable widescreen view of digital threats

Victor de Pous

Digital security makes the headline news on a daily basis, mainly because of large international incidents or limited events with drastic consequences. At the same time, a debate arises. About paying ransom to digital criminals or the use of multifactor authentication via sms. Other discussions pertain to back-ups: when is this the responsibility of the ICT service provider? Or what to make of tech companies that want to autonomously scan the encrypted files of their customers, for example to check for child pornography? The diverging views on the position of the Chief Information Security Officer (CISO), the usefulness and necessity of an independent ICT certificate and the legal enforcement of minimum security requirements for computer programs also remain as topical as ever. In contrast, there has been little discussion so far about digital threats, because a more traditional approach to the threat assessment and network and information security prevails. That view is too narrow. The enemy is not only lurking in the power outlet, and the threat actors are not limited to 'the usual suspects'. Today the uncomfortable truth is that no one can be trusted.

Siege

It is good to realise the flipside of the digital transformation. At a certain point, the status quo of digital threats shifted: from incidental and monolithic to permanent and diverse. That means that today, the individual, organisation and sovereign state is 'under siege' and will remain so for the time being. Speaking of a radically altered world view. In addition to the traditional notorious threats, like espionage, crime and terrorism (from - organised - criminals, activists and state actors) and fire and water damage and power outages (now also caused by climate change, incidentally), there is also the danger of poor quality information technology or cheating software, for example.

The oft-praised innovative but at the same time *socially* disruptive business models of Big Tech and the platform economy, like that of Airbnb in an urban conurbation with an acute shortage of affordable housing, might also fall under the heading of digital threat. Or take Facebook, which European Commissioner Verstager (Competition) alleges can threaten the mental health of users and the development of our democracy.[216]

We also see fining decisions and caselaw being decided in the Netherlands on account of the increase in government organisations that use ICT *unlawfully* and violate citizens' rights in doing so. The cases involving bonuses (Tax and Customs Administration), SyRi[217] (Tax and Customs Administration), automated fining system[218] (Municipality of Amsterdam), Land Information Manoeuvre Centre[219] (Defence) and the Fraud Detection Facility (once again the Tax and Customs Administration) speak volumes. The blacklisting of individuals by the tax authorities was deemed by the Dutch Data Protection Authority (DPA) to be a 'serious' violation of GDPR.[220] 'Over a quarter of a million people were kept — often wrongly — on this fraud list for much too long, without them knowing this. This meant they could not defend themselves, nor could they get themselves off the list. This gave rise to a gap in the protection under the law. Caused by the government no less!'

Another possible category. Consumers are being misled by careless business owners, who, for a start, provide inaccurate information online. Supervisory body ACM imposed millions of fines on KPN, Tele2, T-Mobile and Vodafone, each individually, at the end of 2019.[221] Booking.com had to make major changes to its websites in Europe on the same grounds - violation of consumer protection law.[222] Video-calling company Zoom is under fire in the United States. On further study, it emerged that the company was not employing end-to-end encryption, despite having initially stated that it did. Personal data were also being

[216] https://www.dw.com/en/eu-top-antitrust-official-margrethe-vestager-talks-to-dw/av-59633111

[217] *Cooperating parties v State of the Netherlands*, District Court of The Hague, 5 February 2020, ECLI:NL:RBDHA:2020:865.

[218] *Resident v Municipality of Amsterdam*, District Court of Amsterdam, 9 March 2021, ECLI:NL:RBAMS:2021:1169.

[219] https://www.nrc.nl/nieuws/2021/11/01/waarom-greep-niemand-in-bij-defensie-a4063866

[220] https://autoriteitpersoonsgegevens.nl/nl/nieuws/zwarte-lijst-fsv-van-belastingdienst-strijd-met-de-wet

[221] https://www.acm.nl/nl/publicaties/vier-telecomaanbieders-beboet-voor-onduidelijke-websites

[222] https://www.acm.nl/nl/publicaties/booking-past-website-aan-na-optreden-van-de-europese-consumententoezichthouders

secretly provided to third parties, such as Facebook, on commercial grounds; even from users who had no Facebook account.[223] Can we classify this type of deviant commercial practice as a digital threat? There will be little discussion about the creation of fake profiles by regular dating sites,[224] or the running of fake websites.[225]

Hunt for personal data

A specific modus operandi pertains to the use of so-called pixel espionage. Investigation by the Dutch programme Reporter Radio (NCRV-KRO) in 2019 indicated that the lion's share (21 of the 26) of the Dutch healthcare insurers investigated was using controversial tracking software, hidden in emails to their customers.[226] This tracking software can be used to check whether a person has read their email, without that person having direct knowledge of this. The sender can also see where and when the email was opened. Someone's IP address can also be unlocked.

Although the above is an unlawful commercial practice - there is no legal basis for the data processing - supervisory authority the Netherlands Authority for the Financial Markets (AFM) warns about the *legal* hunt for financial personal data.[227] This behaviour is explicitly encouraged because of the opportunity that the Community legislator provides entrepreneurs via the new EU Payment Service Directive (PSD2). Since 19 February 2019, new parties in our country can offer payment initiation services and account information services. The emphasis is therefore on competition and innovation and elimination of the obstacles to new entrants on the financial market. In that context, there has evidently been no or insufficient attention paid to the possible side effects observed by the AFM. With the result that some innovations of both financial start-ups and the big tech companies 'undermine the customer interest'.

[223] https://www.govinfo.gov/app/details/USCOURTS-cand-5_20-cv-02155/USCOURTS-cand-5_20-cv-02155-1/context

[224] https://www.acm.nl/nl/publicaties/toezegging-online-dating-met-right-link-godai-green8group-boost-web-activities en https://www.acm.nl/nl/publicaties/datingwebsites-moeten-stoppen-met-misleiden-met-nepprofielen

[225] In 2019, SIDN took down 4,340 fake online stores, in cooperation with the .nl registrars and others. https://www.sidn.nl/nieuws-en-blogs/bijna-4-500-nepwinkels-offline-gehaald-in-2019-dankzij-detectie-sidn

[226] https://radar.avrotros.nl/nieuws/item/zorgverzekeraars-volgen-klanten-met-e-mailcookies/

[227] https://www.afm.nl/nl-nl/nieuws/2020/november/trendzicht-2021

Zero trust

Several years ago, a delivery van from security service provider Fox-IT used to drive around the Netherlands with the slogan 'Who you gonna call?' — playful marketing alluding to the successful 1984 film Ghostbusters. Knowing who to call if a serious disaster occurs can't hurt. The overriding question, however, is otherwise. 'Who you gonna trust?' That is true for user organisations - think of the recent software problems of providers like Citrix,[228] SolarWinds,[229] and Microsoft,[230] with many users worldwide - and for us as an individual.

In fact, *trust in digitalisation is crucial for the society that relies on it.* Former Minister De Jonge (Public Health, Welfare and Sport) said on 24 January 2021 in response to the breach at a GGD call centre which resulted in the illegal selling of the address details, phone numbers and citizen service numbers (BSNs) of tested people from two COVID-19 systems:[231] 'This must not hurt people's willingness to get tested'.[232] But how do you restore digital trust once breached?

Today the inconvenient truth is that no one can be trusted. The National Cyber Security Centre (NCSC, part of the Ministry of Security and Justice) emphatically advises organisations to opt for a 'Zero Trust model'. 'The traditional security model, also called the castle or coconut model, has structural vulnerabilities and has become untenable because of modern malware and ransomware attacks. The model falls short when it comes to changing technologies and threats from within, the NCSC concludes.'[233] But does the new approach actually result in resilience to different types of deviant behaviour (so alongside espionage, criminality and terrorism) in relation to digital technology and data processing, such as misleading, privacy violation and defects in the information technology?

[228] https://www.ncsc.nl/actueel/nieuws/2020/januari/16/door-citrix-geadviseerde-mitigerende-maatregelen-niet-altijd-effectief

[229] https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

[230] https://www.ncsc.nl/actueel/nieuws/2021/maart/16/schade-microsoft-exchange

[231] https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-database-coronit-hpzone

[232] https://nos.nl/artikel/2365961-arrestaties-voor-handel-in-persoonsgegevens-uit-coronasystemen-ggd

[233] https://www.ncsc.nl/actueel/nieuws/2021/augustus/18/publicatie-factsheet-bereid-u-voor-op-zero-trust

Quality shortcomings

History is constantly repeating itself. At the beginning of March 2021, the NCSC warned about vulnerabilities in Microsoft Exchange Server and the urgent need to install the updates as quickly as possible. Rising estimates indicated 60,000 hacked servers worldwide at the time. On 16 March 2021, 1,200 of the email servers in the Netherlands had not yet been patched;[234] three days later only 75 data leaks had been reported to the DPA. Fingers were pointed at hackers affiliated with the Chinese government. Although the jargon is not unequivocal and formal definitions are usually lacking (generally: a vulnerability is a weakness in software which can be exploited and a (security) bug is a software error[235]), it concerns a defect in digital quality. Generally speaking, this creates an independent security risk that cannot be limited or prevented, or more conservatively, by definition cannot be limited or prevented by the appropriate technical and organisational measures of the GDPR or security rules from other regulations. And: a patch, even if it is implemented immediately, does not help if systems have already been compromised.

The Rutte III cabinet wanted to introduce into Dutch law a special legal liability for unsecure software. Neither this agreement, laid down in the coalition accord of 10 October 2017,[236] nor the plan of the Minister of Justice and Security two years later to be able to intervene at digitally unsecure companies were implemented.[237] *Both are sorely missed legal measures*. Digital quality defects - in designing, programming, securing, configuring, testing and maintaining - make individual users, organisations and society as a whole more vulnerable than necessary and make it easier to commit digital crime.

Artificial intelligence

Among others, scientist Stephen Hawking, philanthropist Bill Gates and entrepreneur Elon Musk have warned about the dangers of artificial intelligence (AI).[238] Unchecked application of AI could ultimately mean the end of our

[234] https://www.ncsc.nl/actueel/nieuws/2021/maart/16/schade-microsoft-exchange

[235] https://en.wikipedia.org/wiki/Vulnerability_(computing)

[236] 'An ambitious cybersecurity agenda is being drawn up which includes, among other things, (..) encouraging companies to make more secure software via software liability (..).'

[237] https://fd.nl/ondernemen/1318504/justitie-wil-ingrijpen-bij-bedrijven-die-digitale-beveiliging-niet-op-orde-hebben

[238] https://observer.com/2015/08/stephen-hawking-elon-musk-and-bill-gates-warn-about-artificial-intelligence/

civilisation. In the Netherlands, citizens are concerned about discrimination and privacy breaches, but also that inaccurate data could result in incorrect decisions and that decisions taken by AI systems are generally difficult to reverse.[239] This fear seems to be well founded. There is a threat to democracy, the rule of law and our freedoms, and the potentially irreversible nature of the effects that the smart technology could cause.

Properly considered, international bodies, including the OECD, G20 and European Commission, are on the same page. Artificial intelligence can pose a threat and needs to be curbed. Together with the dominant sentiment on 'the silent power of AI' (*improving* our welfare), the - draft - ethical and legal standards frameworks for human-centred AI have a complementary common thread: *safeguarding* our welfare.[240]

In conclusion

The individual, the organisation and society have in fact become entirely dependent on the availability, proper functioning and further development of digital technology and what it does: automated data processing. 'The enemy is lurking in the power outlet', was the one-liner from 2016, attributed to the CEO of Siemens AG at the time, but the threat actors are no longer limited to 'the usual suspects', as emerges from practice. Even digital technology can pose an autonomous threat.

In the meantime, we see that legislators are supplementing legal rules with sanctions with a strong deterrent effect via high administrative fines that supervisory bodies can impose. Consider privacy law, economic law, consumer protection law and environmental law. Unsecure digital products and services make us more vulnerable than necessary and make it easier to commit digital crime. In fact, you could say that digital resilience starts with adequate quality, particularly of software code. Anyone who wants to protect themselves well and at the same time manoeuvre optimally in the digital space cannot avoid taking a broad view of digital threats as the starting point for taking measures.

[239] Yolanda Schothorst and Dieter Verhue, *Nederlanders over Artificiële Intelligentie* [The Dutch on Artificial Intelligence], Kantor Public, 2018 (commissioned by the Ministry of the Interior and Kingdom Affairs).

[240] See, among others, the proposal for the EU AI Regulation (COM(2021) 206 final) of 21 April 2021 as well as Natascha van Duuren and Victor de Pous, *Multidisciplinaire aspecten van artificial intelligence*, Amsterdam, 2020.

Analyses

- On the *global level*, the international security climate is worsening and according to the Dutch Minister of Defence has changed the nature of conflicts. 'The dividing line between war and peace is often diffuse and conflicts are increasingly being fought with (dis)information, irregular military forces and cyber attacks,' according to the 2021 Annual Plan Letter from the Military Intelligence and Security Service (MIVD) sent to the Dutch House of Representatives on 15 December 2020.[241]
- Zooming in on the *country level*, the Netherlands has now lost a large part of its digital sovereignty, the Cyber Security Council observed and warned on 14 May 2021.[242] One of the concrete issues that now demands action is the 'implementation of a digital autonomy cybersecurity assessment framework'. And on the *organisational level*, the NCSC advises businesses and government organisations to opt for a 'Zero Trust model'.
- It should also be considered here that the dividing line between regular entrepreneurship and sham practices is sometimes diffuse and the competition is sometimes waged with digital technology used in a questionable manner. The examples are possibly as diverse as they are numerous, whereby damage also arises on the *level of the individual*. This latter point is also true for the citizen if government organisations use ICT unlawfully, for example by employing unverifiable ICT systems and bases for data processing.
- The justified attention to combatting espionage, crime and terrorism must not be at the expense of the primary need for adequate digital quality, without overlooking the security aspect. Solid legal safeguards - in line with the prevailing legislative sentiment - supplemented with proportionate and deterrent sanctions has become unavoidable, given the society-wide importance.

[241] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z25043&did=2020D52574

[242] https://www.cybersecurityraad.nl/actueel/nieuws/2021/05/14/%E2%80%98digitale-autonomie-nederland-staat-onder-druk%E2%80%99

14. Cybercrime and Cybersecurity in South Africa

Basie von Solms, Rossouw von Solms, Sune von Solms and Elmarie (von Solms) Kritzinger

In this chapter we evaluate the situation as far as Cybercrime and Cybersecurity in South Africa (SA) is concerned. This evaluation will include aspects like the present state and experience of citizens in SA as far as Cybercrime is concerned, the latest developments concerning Cybersecurity in SA, including developments in the legal area and educational environment. We will also highlight some problems experienced as far as these matters are concerned, with reference to the situation regarding transfer of Cybersecurity knowledge and skills. We also review developments in the area of Cybersecurity Awareness, with the focus on the involvement from the side of the Government, Educational bodies and Community groups. The experience of the authors reflects the fact that an increase in Cybersecurity knowledge and skills, and specifically Cybersecurity Awareness, will definitely have a positive effect on lowering Cybercrime and helping to establish a better cybersecurity culture in SA. All authors are therefore involved in activities to increase such Cybersecurity knowledge, skills and awareness to help fight Cybercrime.

Cybercrime in South Africa

In a research report published in 2020[243], the company Accenture states that South Africa has the third-highest number of cybercrime victims worldwide, losing approximately R2.2 billion (US$147 million) a year to cyber-attacks. The report also provides a timeline for cyberattacks in SA during 2019. One of the conclusions in this report is that one reason for this high number of cyberattacks, is that South African Internet users are inexperienced and less technically alert than users in other nations. In 2020 some more serious attacks have taken place in SA, for example

[243] Insight into the cyber threat landscape in South Africa, 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa

the Experian data breach in which personal information of about 24 million was leaked to a fraudulent client[244].

Cybersecurity developments in the legal and capacity building areas in SA

Two important developments are the new Protection of Personal Information Act (POPIA)[245] and the Cybercrime Act[246] – which both became operational in 2021. Both these Acts are in principle based on international standards, and may help to improve the image of SA as far as being a big target for cybercrimes is concerned. However, both Acts depend on skilled people to implement and enforce the relevant Acts. It is well known that SA, as all over the world, has a lack of Cybersecurity knowledge and skills[247].

Therefore, for these Acts to really show their teeth, SA needs more cybersecurity capacity. Fortunately, a significant number of cybersecurity knowledge and skills creating initiatives have started in the country over the last few years. Examples are the Cybersecurity Short Learning Courses offered by the University of Johannesburg, specifically directed towards people working full-time and who wants to improve their cybersecurity skills in a part time mode. The University also has a 4 year BSc degree with specialisation in Cyber Security[248]. The University of South Africa has three Short Learning Courses that is offered through Open Distance Learning[249]. The Nelson Mandela University introduces a formal master's program, the MPhil in IT Governance, which places a huge emphasis, amongst others, on IT and cyber risk, security, assurance and law[250]. The focus of this qualification is predominantly to teach more security-related knowledge and skills in the public sector. Another recent development is the establishment of the

[244] Experian Security Breach in South Africa, 2020 https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/experian-security-breach-in-south-africa

[245] Personal Information Act (POPIA), 2021 https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

[246] Cybercrime Act, 2021 https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

[247] Mind the Gap: Addressing South Africa's cybersecurity skills short age, 2018, https://www.dailymaverick.co.za/article/2018-07-13-mind-the-gap-addressing-south-africas-cybersecurity-skills-shortage/

[248] Website of the Centre for Cyber Security, www.cybersecurity.org.za

[249] School of Computing Short Learning Programmes (SLPs), http://cs-cert.unisa.ac.za/

[250] Nelson Mandela University, https://mphilitgov.mandela.ac.za

Cybersecurity Capacity Centre of South Africa in Cape Town[251]. Most Universities in SA offer some form of knowledge and skills development initiatives in Cybersecurity, and many private companies in SA also offer such knowledge and skills development courses.

Even though these initiatives all advance the level of Cybersecurity knowledge and skills in SA, the implementation of the two Acts mentioned above will need a special effort from the SA Government, and especially the SA Police Service in developing the required knowledge and skills to support these Acts. The private industry has indicated that they are more than willing to be involved through Public-Private Partnerships (PPPs). As the private industry is basically running many of the critical Information Infrastructures in the country, they have far more knowledge and skills in the cyber area than the Government itself has. It is therefore extremely important that such PPPs are implemented with the greatest speed – if not, the chances are very good that these two very important Acts, will not have a significant effect in lowering Cybercrime. It is critical to note that even though the one pillar of formal legislation is critical within Cybersecurity, the other pillar of Cybersecurity knowledge and skills transfer, as well as Cybersecurity Awareness, is just as critical to promote a culture of cybersecurity in SA.

Cybersecurity Education

There exist limited initiatives to educate communities (school learners, educators, parents) on cybersecurity across Africa - only a handful of African governments currently have active formal national cybersecurity education and awareness initiatives. Although several South African Universities offer formal Cybersecurity education and training, South Africa does not have a formal nationwide Government-driven initiative for cybersecurity awareness. Nevertheless, the cybersecurity awareness in schools cannot lie dormant until effective government initiatives are implemented, as children regularly fall victim to cyber-attacks and threats. Several Initiatives from the private sector, NGOs and universities aim to equip children and students with the knowledge to use the Internet safely and responsibly[252].

A cybersecurity curriculum, based on open educational resources, was developed by the Nelson Mandela University and the CSIR some years ago for primary school

[251] Cybersecurity Centre for South Africa, http://www.c3sa.uct.ac.za/

[252] University of Johannesburg, https://www.bcs.org/deliver-and-teach-qualifications/university-accreditation/practice-highlights/university-of-johannesburg-cyber-security/

learners[253]. A final curriculum of 33 lesson plans for three age groups were developed. These lesson plans and associated worksheets for learners were distributed and used by numerous schools. A cybersecurity children's book, containing poems and short messages, was written by the University of Johannesburg and the African Centre of Excellence for Information Ethics aimed at teaching small children the basics of cybersecurity[254]

Another cybersecurity education initiative is the Cyber Security Challenge, hosted annually by the National Integrated Cyber Infrastructure System (NICIS). The Cyber Security Challenge targets university students and aims to improve security education, focussing on network security and hacking challenges to improve cybersecurity skills and knowledge. This competition is held annually and open for all Southern African university students[13].

Cybersecurity Awareness - Training the trainers

It is critical that community members and educators have proper cybersecurity, specifically Cybersecurity Awareness knowledge and skills to be able to assist communities, educators, parents and school learners to grow a cybersecurity culture. One initiative within South Africa is to provide cybersecurity awareness knowledge and skills to communities which otherwise have no access to cybersecurity education.

The University of South Africa (UNISA) offers MOOCs (Massive Open Online Courses) on the UNISA MOOC platform for free to all communities[14]. The main purpose of the Cybersecurity MOOCs is to provide anyone with the foundational cybersecurity understanding to improve the overall cybersecurity awareness knowledge and skills in South African schools and communities. Participants who complete such a MOOC will gain basic knowledge of cybersecurity and help to contribute to a safer cyber culture within South Africa. Some MOOCs use the Cyber Safety Awareness Toolkit[15] that was developed in 2020, in partnership with the British High Commission and Department of Communication and Digital Technologies (DCDT). The Toolkit consists of a workbook, guide, posters, cartoons, videos, a pledge and more to assist teachers and school learners to become responsible cyber citizens in South Africa. Most of the Toolkit has been translated

[253] S. von Solms, R. von Solms, "Towards Cyber Safety Education in Primary Schools in Africa", HAISA, 2014, pp 185-197.

[254] S. von Solms, R. Fischer, "Digital Wellness: Concepts of cybersecurity presented visually for children", HAISA, 2017, pp 156-166.

into different South African languages to address the language barriers in schools to ensure inclusiveness.

Conclusion

Significant developments have taken place in South Africa during the last few years. These developments are related to new cybersecurity legislation, which includes the Protection of Personal Information Act (POPIA) and the Cybercrime Act. Cybersecurity degrees on tertiary level as well as Cybersecurity Awareness initiatives offered by different role players in the country, including the private sector, NGOs and universities. However, these Awareness initiatives are not coordinated on a national level, and there is no national portal providing a single entry point to all these initiatives. This is sorely needed.

Insight

South Africa has started on the daunting and ongoing task of improving the culture of cybersecurity within SA. A number of initiatives have been implemented in the government, education and the community sectors. SA has indeed a number of very good cybersecurity initiatives, however these initiatives are operating in silos spreading over different organizations and institutions with no clear vision of integration. Some thoughts on the way forward:

- SA needs a holistic and integrated approach to Cybersecurity, with an emphasis on Cybersecurity Awareness, supported by a National Cybersecurity Awareness Portal providing a single point of entry to all initiatives, led by the Government.
- SA needs sufficient cybersecurity knowledge and skills to support the enforcement of the new legislation
- SA needs additional cybersecurity culture enrichment programs for employees in all organizations, especially SMMEs.
- SA needs integration of cybersecurity courses within all Higher Education courses (university level)
- SA needs the formal inclusion of cybersecurity courses into the school curriculum
- SA needs open access to cybersecurity awareness for all communities (no matter of prior knowledge, access or standing).

15. Better security testing via procurement and reporting requirements

Brenno de Winter

The results of a penetration test, or pen test, are often argued as proof that an organisation or division thereof has its information security in order. 'We have had hackers test the system and they gave their approval', is the reassuring message. If things go wrong, the tired saying that 'there is no such thing as 100% security' or that the incident 'could happen to anyone' is marched out. Over the past years there have been frequent examples of major hacks that were in fact very basic and that a simple 'sanity check' should have uncovered. But the recent penetration tests gave no indication that the organisation should be concerned. Fortunately, digital security tests can and must simply be performed better.

Periodic vehicle inspection

Imagine that you pick up your ten-year-old car from the garage. 'We serviced it, replaced a few parts and carried out a periodic inspection. Everything is perfectly in order. That'll be €962.87 please,' says the employee. If you ask what precisely was done and what is tested as part of the periodic inspection, the employee cheerfully explains that the testing involves trade secrets and what is tested is not shared with you. You are only told if something is not in order and fortunately that is not the case. With the inspection certificate in hand and almost a thousand euros lighter, you leave the garage.

Such a thing would be absolutely unacceptable in the physical world. The inspection requirements[255] for the periodic vehicle inspection are, after all, public, so that one knows what is tested, how this is done and what the result of the test is. It is just as unacceptable to simply replace 'a few parts' and charge for that. The practice in the digital world is very different. Many pen tests do not make clear what

[255] https://apk-handboek.rdw.nl/

exactly is tested and what is not, what result the test produced and what conclusions can be drawn from this. There is no access to how the test is performed because it is classified as a trade secret and therefore what has been done cannot be verified. Some pen test providers even go so far as to actually report only findings which they deem relevant or not report how much energy was put into the search. That fuels the statement 'hackers had a look at it and couldn't get in'.

Incident

How problematic this approach is, becomes clear if we extend the parallel to the periodic vehicle inspection. A day after the inspection, on a rainy morning, you drive onto the motorway and while merging, you tap the brakes as you pull in behind another car. Your car suddenly veers to the left and hits a car in the left lane, which bumps the guardrail. A technical investigation indicates that a blocked brake was the cause of the accident and the slippery tyres meant you did not have any traction. The conclusion is that your car is in poor repair. A few months later you must face the consequences: being held accountable before the judge in a criminal court.

RIVM

On 6 June 2020, broadcaster NOS[256] revealed that a website of the RIVM had proved vulnerable to URL manipulation. That is a complicated way of saying that changing a number in the web address provides access to other data. In this case, the personal data of someone else. Someone cleverly exploiting this would be able to access the data of 60,000 people. The error was very basic and simple to test. Previously, the budget memorandum[257], a Christmas address from Queen Beatrix[258] and later an address from King Willem-Alexander[259] had been leaked via URL manipulation. The penetration test from Infectieradar did not pick up on this basic error. After remedying the problem, more tests were carried out.

[256] https://nos.nl/artikel/2336416-lek-in-rivm-coronasite-gegevens-van-gebruikers-makkelijk-in-te-zien

[257] https://www.nu.nl/politiek/2616614/miljoenennota-gelekt-onbeveiligde-site.html

[258] https://www.nu.nl/internet/2990747/kersttoespraak-koningin-beatrix-gelekt.html

[259] https://www.nu.nl/binnenland/3662226/kersttoespraak-koning-willem-alexander-lekt.html

On 1 December 2020, the municipality of Hof van Twente discovered[260] that it could no longer access its files. A large part of its network had been taken hostage. Investigation[261] indicated that a penetration test had been performed on the infrastructure in the months prior to the attack. This test did not reveal that the municipality was providing access to the network in an undesirable manner. That if a user account is hacked into, this account would work across the municipality, *no* multi-factor authentication was in use, and there was insufficient segregation in the network. All indicators that attackers would be very successful if they managed to hack in via a ransomware attack. It is precisely this warning that had been given at a neighbouring municipality a year earlier[262] after a similar hack with less drastic consequences.

Perform an audit or look for errors?

Confusion arises in relation to many penetration tests[263] because the expectation of what one is purchasing is often far removed from what is actually being offered. The test provider offers a service whereby a number of tests are performed, either in a structured way or otherwise. The reports then show the findings with a weighting, determined by the tester. It can happen that a finding at one company is considered critical while the same finding at another company is deemed no more than average. The test methodology also varies, with not every penetration test provider testing in as structured or in-depth a manner. The way in which a test is performed can vary, for example. One tester might only use software packages to carry out the tests, while others may use automated scanning as well as develop their own attacks and provide a lot of manual work. Even when the same object is being tested by several companies, it is possible that different assessments as to security could arise.

[260] https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2020/12/artikel/systeem-hof-van-twente-platgelegd-door-onbekende-derde-1773

[261] https://www.hofvantwente.nl/fileadmin/files/hofvantwente/inwoners/actueel/Te-goed-van-vertrouwen.pdf

[262] https://www.lochem.nl/fileadmin/internet-doc/Bestuur-Organisatie-Nieuws/Nieuws/2019/hack/Duidingsrapportage_Lochem-WHITE.pdf

[263] https://nl.wikipedia.org/wiki/Penetratietest

Container concept

Differences also arise because a penetration test is really a collective term for all testing aimed at uncovering vulnerabilities. This distinction arises with the level of knowledge available while performing the test attacks. In the most basic form, there is a so-called 'black box' test. The only information provided for the testing is that which is strictly necessary, such as the targets to be attacked, the IP address or a URL. As in the case of a random attack, no information is given.

In the event of a 'grey box' test, on the other hand, more information is available, such as some details about the underlying systems and a user account to the environment. This imitates the situation in which an attacker has already made their way in, or the situation of a malicious insider. In a 'white box' or 'crystal box' test, the tester has access to a great deal of information, such as detailed information about the networks, the source code for software, and advanced access rights. This tests the situation in which a hacker has already been in for some time, or the situation of a malicious employee. The more knowledge made available to the tester, the more there is to test and try out, which means more will be found.

Groping in the dark

For many organisations looking to purchase penetration testing, without this knowledge it is difficult to understand why one penetration test is more expensive than another and what exactly can be expected on the basis of a test. It may feel like the organisation has undergone an audit (digital periodic inspection, like for vehicles), from which assurances can be derived. It does not seem logical then that this is not the case based on a penetration test, or even an audit. The gap between what is being offered and what the customer thinks they are getting is therefore enormous. For the rest, there is often reason to suspect that a penetration test does not offer the certainties hoped for. Many reports do not make clear what exactly has been tested and the document contains reservations. Such reservations are not made in the event of a periodic vehicle inspection, because there a detailed description is given of what has been tested, and with what result.

Audit value

In order to nonetheless be able to derive assurances from a penetration test, one must inevitably seek connection with frameworks that provide a certain degree of uniformity. The disadvantage of a framework is that just as with a periodic vehicle inspection, a selection of components are examined. The advantage, however, is that certainty arises as to what, at a minimum, has been tested and that the report provides sufficient transparency to support the aim of the audit: to obtain a reasonable degree of assurance or confidence that the security has been adequately implemented at a certain level. Uniform documentation helps in this respect because then the reporting at least contains a certain amount of transparency about the situation on one's own systems.

When the CoronaMelder was being developed, the issue of penetration testing flared up in full force. How do you eliminate societal concerns about security and reliably serve MPs if they ask for a penetration test as if it were a periodic vehicle inspection? On the other hand, you yourself seek certainty in predictability in finding possible problems, making the picture presented normatively correct. No matter who performs the test, the results should be given the same weighting and every tester should reach the same findings on the most important points. Uniformity also introduces a level playing field for the procurement of penetration testing and uniformity in the reporting introduces a debate based on objective criteria instead of opinion.

Conclusion

An important lesson from this process is that testing providers often hide behind their own methodologies and find open standards difficult. The search revealed, however, that it is possible to arrive at meaningful *procurement requirements*. First of all, the Open Web Application Security Project (OWASP)[264] offers a collection of standards that answer the question of *what* should be tested. There is a top 10 of common security vulnerabilities, for instance, the OWASP TOP 10[265] (there is a separate TOP 10 for APIs[266]). Based on this list, a penetration test can no longer suffice with a scan because errors are also identified that necessitate asking the client about the available monitoring, for instance. Other OWASP standards describe in detail what must be tested for web applications (WSTG[267]) and mobile applications (MSTG[268]). Simply making inquiries to the senior management, in combination with the standards, ensures a minimum level of testing is performed and assumes a ‘white box’ or ‘grey box’ test.

[264] https://owasp.org/

[265] https://owasp.org/www-project-top-ten/

[266] https://owasp.org/www-project-api-security/

[267] https://owasp.org/www-project-web-security-testing-guide/

[268] https://owasp.org/www-project-mobile-security-testing-guide/

Points for attention

- While the OWASP provides a list of standards that indicate *what* the subject of digital testing is, for the reporting there is the Penetration Testing Execution Standard.[269] This meticulously describes *how* a penetration test should be recorded. It involves attaining a defined, careful and also very detailed working method. In combination with the requirement that the testing be carried out such that it is reproducible, it is possible, if there are doubts, to get a second opinion on (parts of) the testing.
- When reporting on vulnerabilities, the Common Vulnerability Scoring System[270] provides uniformity in the seriousness of a finding on a scale of 0 (informative) to 10 (very serious). It is very helpful that the seriousness can be related to the organisation's specific situation, so that the relevance of findings for your situation is also considered. A number of organisations consider a CVSS score of 4 or higher as a block to going live. This also makes the score a crystal clear measuring stick.
- Using standards guarantees a minimum level of security. Uniformity helps settle disagreements. Applying a firm limit for what is acceptable for going live prevents serious deficiencies from being ignored. After a successful retest of any problems, the results of the test can be shared in order to give the stakeholders confidence in a penetration test. In the event of the penetration test for CoronaMelder[271] that was the public at large, which is why this was published as if it were a periodic vehicle inspection.

[269] https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf

[270] https://www.first.org/cvss/v3-1/

[271] https://github.com/minvws/nl-covid19-notification-app-coordination/blob/master/privacy/Duidingsrapportage/Bijlage%20K%20-%20Rapportage%20Penetratietest.pdf

16. Cyber attack & emergency response

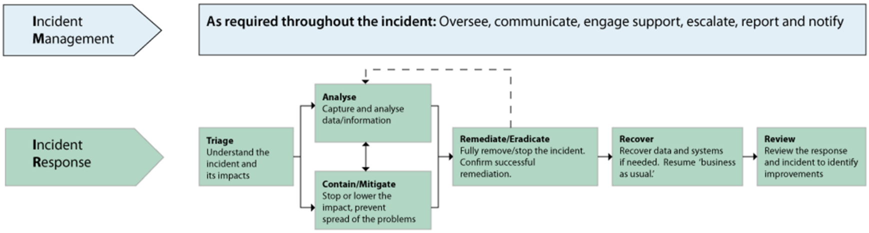
Steven Dondorp

We live in a reality where the world's biggest meat processor JBS, the Port Authority of Rotterdam, and pipeline operator Colonial Pipeline have all been hit by cyber attacks. But it is only when medium-sized companies like Bakker Logistics are hit that we really notice it ourselves, when there is no cheese on the supermarket shelves. What process are these kinds of companies dealing with in such a situation? How does it work and what decisions and considerations play a role in this? A simplified account will be given of what phases an organisation goes through during a cyber incident, with the assistance of an Incident Response Team, forensic investigation and recovery procedure.

Cyber Emergency Response as part of Incident Management

Although the terminology is often used interchangeably, it is convenient to think of Emergency Response as part of Incident Management.

Emergency Response is the practical process in the event of an Incident which - translated freely - has already been identified as: A 'severe and impactful problem that requires immediate action'. Incident Management is much broader than that. This concerns the entire process for minor and serious incidents alike.


Incident Management
As required throughout the incident: Oversee, communicate, engage support, escalate, report and notify
Incident Response
Triage Understand the incident and its impacts
Analyse Capture and analyse data/information
Contain/Mitigate Stop or lower the impact, prevent spread of the problems
Remediate/Eradicate Fully remove/stop the incident. Confirm successful remediation.
Recover Recover data and systems if needed. Resume 'business as usual.'
Review Review the response and incident to identify improvements

Illustration[272]

Incident Management also encompasses the communication, media handling, escalations and reporting problems, for instance. It includes the policy, the

[272] https://www.ncsc.gov.uk/collection/incident-management/incident-response

playbooks and the training courses and ensures that everything in a context is managed and carried out coherently. Incident Management could be seen as the best prevention and also ensures that the organisation learns from incidents.

Cyber threats and incidents for organisations

The most oft-heard comment from directors when a cyber attack happens: Why us? Surely we're not the most interesting organisation? What they are actually saying is that they (consciously or unconsciously) underestimated the likelihood of a cyber attack and did not really consider Incident Management a necessity for their organisation. The reality is that cybercriminals do not pay much attention to whether an organisation is interesting, but rather to how likely they will be able to easily break into an organisation digitally and, for instance, steal (privacy-sensitive) information or blackmail the organisation. After all, virtually everyone has sensitive information and critical business information. There are various examples of cyber attacks and incidents:

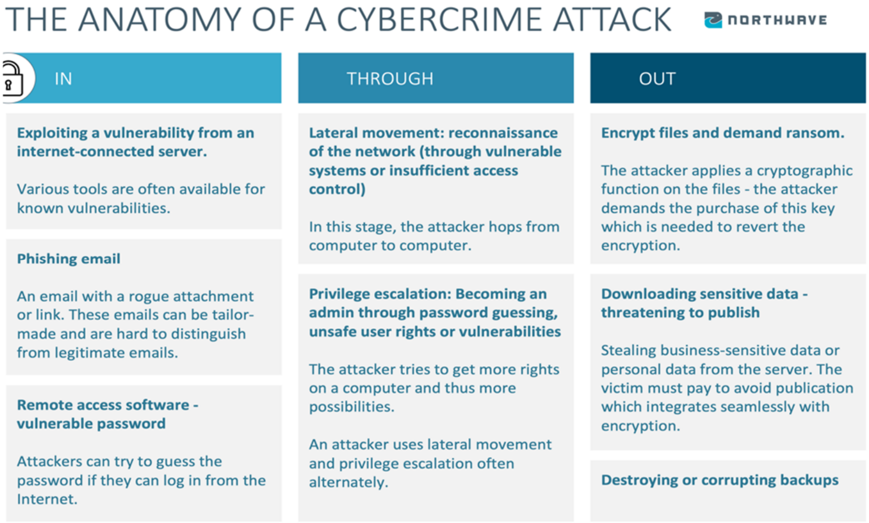
- Theft or interception of information (industrial espionage, privacy-sensitive information, customer information, etc.)
- Breach of the computer network and abuse of user accounts by another
- Malware outbreak (a worm or virus disrupts the normal business operations)
- Distributed-Denial-of-Service (DDOS) attack (overloading digital traffic so that systems no longer work)
- Destruction and sabotage of systems or critical information (an attacker tries to cause destruction and disturbance for political, social or personal reasons, vandalism or otherwise)
- Corruption of digital information (documents become damaged and can no longer be opened because of an attack)
- Exposure and leaks of sensitive company information or privacy-sensitive information
- Encryption or destruction of critical information (also called a wiper attack. This deletes critical information entirely in order to disrupt businesses)
- Ransomware attacks (encrypting information for the purposes of extortion)

Analysing the steps of an attack

A cyber attack on an organisation can be roughly divided into three steps [273]: 1) The preliminary phase; 2) the phase in the organisation; and 3) the phase outside of the organisation. In the preliminary phase, the attacker prepares for the organisation. They explore vulnerabilities from the outside and via social engineering[274] and figure out the best possibility for getting into the organisation. In this phase, the hacker creates attack techniques and the technology they will use to break in. Once they have penetrated the organisation, the attacker often keeps a low profile, remaining unnoticed for days or even months. In this phase, the hacker thoroughly but circumspectly surveys the environment, figuring out which information is crucial and how the organisation works. Based on these experiences, the next steps involve exploitation and installation of, for instance, malware, backdoors, or ransomware, in order to then leave the organisation again unnoticed. In the final phase, the attacker, having established a Command and Control (C&C) environment, has control over the organisation and over certain information. The malware installed communicates back to this C&C and the attacker can now finally start the actual attack and achieve the objectives of all the preceding actions. The hacker completes their attack plan, which could consist of damaging, destroying or stealing information or the disruption or extortion of the organisation for a substantial ransom.

[273] www.northwave-security.com Anatomy of a Cybercrime attack

[274] Social engineering is a technique whereby an attacker obtains information from people by playing on human traits such as curiosity, trust and ignorance. The attacker manages to secure confidential or secret information as a result, which enables the hacker to get closer to the digital object they are attacking.



THE ANATOMY OF A CYBERCRIME ATTACK

IN	THROUGH	OUT
Exploiting a vulnerability from an internet-connected server. Various tools are often available for known vulnerabilities.	**Lateral movement: reconnaissance of the network (through vulnerable systems or insufficient access control)** In this stage, the attacker hops from computer to computer.	**Encrypt files and demand ransom.** The attacker applies a cryptographic function on the files - the attacker demands the purchase of this key which is needed to revert the encryption.
Phishing email An email with a rogue attachment or link. These emails can be tailor-made and are hard to distinguish from legitimate emails.	**Privilege escalation: Becoming an admin through password guessing, unsafe user rights or vulnerabilities** The attacker tries to get more rights on a computer and thus more possibilities. An attacker uses lateral movement and privilege escalation often alternately.	**Downloading sensitive data - threatening to publish** Stealing business-sensitive data or personal data from the server. The victim must pay to avoid publication which integrates seamlessly with encryption.
Remote access software - vulnerable password Attackers can try to guess the password if they can log in from the Internet.		**Destroying or corrupting backups**

Understanding the anatomy of the cyber attack helps in investigating the primary cause of the incident and in proactive Incident Management, in order to preventatively arm yourself against attackers.

The Emergency Response rollercoaster

The Emergency Response process is complex because of two main reasons. Firstly, no two incidents are ever the same. Also, every response requires that people, processes and technology be attuned to each other.

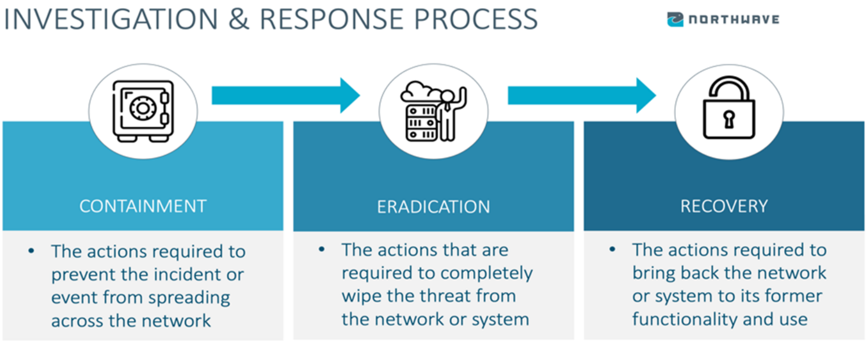
Once an incident has been identified as an emergency, the process begins. This takes place in triage, where the impact of the incident is estimated by experts and by the organisation itself. Then analysis, mitigation and containment takes place in combination with eliminating and uprooting the malware. These phases can be repeated until the problem has been removed from the organisation. Finally, the recovery process takes place in relation to all clean information, such that the organisation can resume its normal processes and business. The Emergency Response process concludes with a review, in which - based on the knowledge and experience gained - improvements can be made to prevent issues and ensure an even better response if a new Emergency Response is required. This entire process involves many stakeholders. From directors and employees of the organisation, to angry customers, IT and Telecom providers to whom processes are outsourced and often an external expert team of Incident Responders and Forensic Investigators that has been brought in (CERT teams).[275] In many cases, sooner or later external stakeholders become involved as well, such as local or regional authorities, police, supervisory bodies, insurers and the media. Working in this complex force field requires navigation, knowing that speed is one of the most crucial matters in Incident Response.

The investigation and recovery process

During the Incident Response investigation, digital forensic analysis tools are used. Forensic investigation is deployed to gather evidence in order to determine activities in individual systems. This enables a (backward) recreation of what has happened, how it happened, what has been affected, and where (looking forward) one could start the recovery process in a focused way.

Before proceeding to that, however, it is first important to go through the containment phase. This makes sure that the situation does not escalate further and any new attacks are picked up on. These containment actions usually consist of enclosing the problem so that it cannot spread. (Temporarily) heightened defences are also created by the deploying of additional monitoring, detection and logging. In this phase, one cannot yet be certain whether what has been observed thus far is the extent of the problem, or if more (or different) attacks are yet to follow.

The containment phase and analysis via forensic investigation then herald in the recovery phase. This consists of two parts: eradication and recovery. Eradication involves the actions needed to fully clean up the malware or causes of the disruption. Recovery involves the actual restoration of the systems and software.



- The actions required to prevent the incident or event from spreading across the network
- The actions that are required to completely wipe the threat from the network or system
- The actions required to bring back the network or system to its former functionality and use

[275] https://northwave-security.com/cert/

Forensic investigation

There are roughly two practical variants of the forensic investigation: 1) collecting and forensically recording events and 2) collecting and forensically recording legal evidence. With the first, you want to know as quickly as possible what actually happened. With the second, you want the process to take place such that the material will suffice in court as legal evidence to be able to convict a person. To gather material to serve as legal evidence, more documentation criteria apply, the process consequently takes longer and as a result is often more costly. It must be decided in advance which variant will apply. If, for example, there is a suspicion in advance that an employee has committed criminal acts, it makes sense to collect and forensically record legal evidence. In many other cases, organisations opt for regular forensic recording. This decision is usually informed by the desire for speed, the desire to avoid publicity and the fact that hackers usually operate in far-off countries in different jurisdictions and are therefore more difficult to prosecute. It is important to properly safeguard the chain-of-custody [276] in both variants, however. These are the forensic rules for identifying and describing the evidence obtained, the storage requirements, and the analysis of documentation and analysis of recording.

Recovery phase

The recovery phase is often very extensive in operation and can sometimes reverberate for months to years after the incident. Think of huge server and system washing lines to clean up all the servers, clients, computers and laptops, smartphones, etc., in a company. Also consider the reinstallation of operating systems and applications with modified configurations, passwords, agents and antivirus software to prevent new outbreaks. This is why some organisations decide not to clean up their infrastructure, systems and software at all, but to purchase all of this entirely anew. Sometimes this solution proves to be more cost efficient.

The post-incident phase

This phase is often neglected in the process. Many organisations proceed to business as usual, without providing good aftercare. This aftercare consists of: Actually implementing all the preventative measures to prevent new or different

[276] CISA ISACA Certified Information Systems Auditor, Common Body of Knowledge, Page 446

attacks, documenting the lessons learned in the Incident Management, creating policy for new processes and actually practising these.

Suggestions and recommendations

As director or supervisory director, ask the question: What still works in my company if the IT fails?
If one has the luxury of never having been affected by a cyber attack:

- Start by setting up Incident Management (with or without external assistance)
- Put together a playbook and actually practise this
- Decide: what can I do myself, what am I willing to do, what do I need to get others to do?
- Can I call on the right expertise immediately?

If one has already been affected by a cyber attack:

- To what extent did a good post-review actually take place and what could be improved moving forward?
- Have all the preventative measures been properly taken and actually implemented?
- Continue to expect that it could happen again. Keep practising. What areas of expertise do you want to be able to call on immediately?

Directors are often surprised that their organisation is the one that was targeted by an attack, they are then relieved to put it all behind them and carry on as normal, but then quickly lose sight of directing and monitoring the actual realisation of the proactive preventative recommendations. The director who does distinguish themselves in that respect will indirectly become more competitive as a result of cybersecurity.

17. The added value of sectoral cyber response teams

Wim Hafkamp

The Netherlands has a great many Computer Security Incident Response Teams (CSIRTs). The bigger multinationals have them, as do many government organisations. The best known is the National Cyber Security Centre of the Ministry of Justice and Security. Often referred to as a 'Computer Emergency Response Team' or CERT, these teams play an important role both in warning about new cyber vulnerabilities and threats and coordinating the response to cyber incidents. Over the past five years, sectoral CERTs have also been set up, which sometimes provide hundreds of organisations with relevant information. Alongside SURF-CERT (colleges and universities) and IBD (municipalities), Z-CERT was set up in 2018 as a sectoral CERT for healthcare by a number of umbrella organisations, with support from the Ministry for Public Health, Welfare and Sport. In addition to tasks relating to the response to vulnerabilities and incidents, these teams increasingly also take on other tasks to improve the resilience and knowledge on cybersecurity in their sector. They organise cyber drills, for instance, and themed sessions in relation to information security. This chapter provides insight into the world of Z-CERT and a view on the nationwide system for cybersecurity that is taking shape.

Life cycle

The large majority of cyber incidents are the result of deficiencies in the vulnerability or patch management policy of organisations. An important foundation of the Information Security Management process is identifying and managing security vulnerabilities. But how do you do that precisely and where do these vulnerabilities even come from?

Vulnerabilities are often found by (scientific) researchers, by security companies or by the provider themselves. Sometimes the vulnerabilities are accidentally uncovered when someone is investigating an error and consequently stumbles upon a bug in the software. Vulnerabilities that are discovered and reported to The Mitre Corporation in the US are assigned a unique identification number, the so-called Common Vulnerabilities and Exposure (CVE) number. This organisation has been doing this since 1999. In addition to The Mitre Corporation, there are also designated CVE Numbering Authorities who - within their own scope, often in relation to their own product - can assign CVE numbers to vulnerabilities. In 2020 alone, 18,352 CVEs were registered!

Distinction

Vulnerabilities vary in their seriousness. This is why in 2005, a method was developed by the US National Infrastructure Advisory Council to transparently and unequivocally indicate the seriousness of a vulnerability. The worldwide Forum of Incident Response and Security Teams (FIRST) adopted the method that same year and developed it further in the years that followed. The method is called the Common Vulnerability Scoring System, whereby the seriousness is indicated by assigning a number on a scale of 0-10. Of the over 18,000 registered vulnerabilities mentioned above, approximately 15 percent had a score of 9 or higher.

Vulnerabilities with such a high score are often easy to exploit and sometimes enable attackers to gain full control of a system or component. Calculating the end score is no simple matter and involves a combination of factors.[277] First, the attack sector is considered (physical access, locally or via a network). It is also determined how complex it would be to exploit the vulnerability, in other words: how much of an expert does the attacker need to be to exploit this vulnerability in practice? It is also determined whether interaction from the user is required and whether the attacker needs to have certain authorisations to be able to successfully carry out an attack. Finally, the consequences of the vulnerability for the aspects of availability, integrity and confidentiality of the information on the system where the vulnerability is located are considered.

Method

Although the CVSS method is standardised worldwide, organisations often perceive it to be very time consuming and complex to calculate the score for their own organisation. The system also sometimes proves difficult to use in specific contexts. For example, in the medical sector. Because how do you weigh the impact of being able to change the monitoring data on a medical device, such as a blood pressure meter or heart monitor? At the end of 2020, the US Food & Drug Administration

[277] Van Baardewijk, S. [2021]. Digitaal pleisters plakken: kaf van koren scheiden. ICT & Health no. 04/21

(FDA) approved a method developed by Mitre[278] enabling the CVSS method to also be applied to medical equipment. Time will tell whether this modification of the CVSS method will garner support in the healthcare sector.

In the Netherlands, the National Cyber Security Centre uses a simplified version to determine the likelihood and impact of a vulnerability. Many sectoral CERTs have adopted this simplified presentation. To judge the likelihood of exploitation, it is considered whether there is a patch available. It is also monitored whether active exploitation can already be observed and how difficult it is to exploit the vulnerability.

Cyber chain risks

Multiple definitions of 'risk' can be found in the literature. Looked at from a distance, these definitions contain a number of commonalities. For instance, risks always concern 'uncertain events' with a potentially 'negative effect'.[279] These events could have internal or external causes. Another common denominator is the (qualitative) value of the risk that is usually calculated with reference to the formula likelihood x impact. If both are high, the risk is also high of course.

Digitalisation has increased enormously in virtually all sectors over the past twenty years. If we look at the healthcare sector, for instance, we see various examples of the intensive use of digital resources. All healthcare institutions use electronic patient or client dossiers (EPD/ECD) to record medical data. But the use of sensors and apps to monitor patients remotely, the use of artificial intelligence for diagnoses, the provision of information to patients and clients via online portals, and the personal health environment are all commonplace these days.

Visible risks

Digitalisation has therefore become of strategic importance in keeping healthcare in the Netherlands accessible, affordable and of good quality. Still there are also concerns about the risks of far-reaching digitalisation in healthcare. On 13 February 2020, for instance, the Dutch Safety Board (OVV) published a report[280] arguing for

[278] MITRE [2020]. Rubric for Applying CVSS to Medical Devices.
https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

[279] COSO [2012]. Enterprise Risk Management, Understanding and communicating risk appetite. The Committee of Sponsoring Organizations of the Treadway Commission (COSO)

[280] Dutch Safety Board [2020]. Patient safety under pressure from ICT outages in hospitals.
https://www.onderzoeksraad.nl/nl/page/4980/patientveiligheid-bij-ict-uitval-in-ziekenhuizen

a better identification of the risks of ICT outages in hospitals. According to the Dutch Safety Board, the dependency on ICT can result in unsafe situations for the patient, such as misdiagnosis based on incomplete information. The Board focused mainly on ICT outages resulting from disruptions in the ICT management processes. However, the availability, integrity or confidentiality of essential information systems could also be affected by growing cyber threats. Advanced ransomware attacks in particular are extra cause for concern because these sometimes hinder primary care processes and ultimately risk compromising patient safety.

Supplier management

Another somewhat overlooked aspect in the entire discussion about cybersecurity in healthcare is the issue of supplier management. From the security perspective, there are, in my view, two primary risks:

1. Dependency on the supply of products and services (chain dependency) and
2. A cyber attack on one's own infrastructure via the 'trusted supplier' (supply chain attack).

The preferred supplier model is used throughout the healthcare sector. These are suppliers who, with their products or services, play an important role in one or more healthcare processes. Healthcare institutions have often built up a strategic relationship over many years with such a supplier, and made substantial investments to ensure that the product or service sets the standard. Agreements are also often made with the supplier on the (remote) technical management of the product or service. This is often the case for advanced, expensive medical equipment, such as MRI scanners.

But we also see these kinds of agreements with suppliers of large EPD systems. Which is understandable, since new links are constantly being made with different information systems. The supplier is closely involved in the required customisation in that case. For instance, consider the linking of a radiology system with PACS images (x-ray, MRI) to a central EPD system, so that a treating physician also has instant access to this kind of information. There are a great many EPD suppliers who provide their products 'on premises' and/or in a SAAS solution. Switching EPD supplier is often a complex matter and not one that is undertaken frequently.

In 2018, the journal Zorgvisie[281] commissioned M&I Partners to investigate what EPD system is used at hospitals and how long they had been using this product. Of the total of 77 hospitals surveyed, it turned out that 50 hospitals were using the system supplied by the same supplier! The list contained two other suppliers. There is clearly a situation of market dominance. With all the risks that entails. After all, if a serious zero-day vulnerability were to arise in the particular EPD system, the potential impact on secondary care in the Netherlands would be enormous.

Supply chain

The other security risk concerns an attack on a healthcare institution via the 'supply chain'. A recent example of a worldwide supply chain attack was the hack of US company Kaseya, which provides IT management software. The hack enabled the criminals to roll-out ransomware on a large scale, to hundreds of organisations worldwide, via Kaseya's regular and legitimate software distribution channel. In this case, mainly IT services providers were hit, including several in the Netherlands.[282]

The big question, of course, is who has an accurate and up-to-date overview of the various links and components of crucial or vital (supplier) chains in the Netherlands? In the United States, the identification and analysis of 16 critical, vital sectors is assigned to the National Risk Management Center, part of the Cybersecurity and Infrastructure Security Agency (CISA). The Netherlands does not have such a national agency.

Conclusion

The Network and Information Systems (Security) Act (Wbni) has been in force since 9 November 2018. This law stems from the European NIS directive and provides for the statutory duties of the National Cyber Security Centre (NCSC) in the cybersecurity domain. Organisations in vital sectors – so-called providers of essential services (AEDs) - are required to report serious digital security incidents to the NCSC. The law mandates the NCSC to assist these vital organisations in

[281] M&I Partners [2018]. The complete EPD overview. https://mxi.nl/kennis/298/het-complete-epd-overzicht-welk-ziekenhuis-heeft-welke-leverancier

[282] Computable [2021]. Mass ransomware attack via Kaseya. https://www.computable.nl/artikel/nieuws/security/7210136/250449/massale-ransomware-aanval-via-kaseya.html

taking measures to safeguard the continuity of their services and inform and advise them on threats and incidents for their network and information systems.

The law also gives the NCSC a legal basis to share vulnerability and incident data with other designated organisations or crisis teams.[283] The Nationwide System (LDS) is an existing structure in which public and private parties, such as CERTs (computer crisis teams), sectoral and regional collaborations, the NCSC and the Digital Trust Centre (DTC), work together to exchange information and knowledge with the aim of preventing digital disruption and making the Netherlands more cyber resilient.[284]

On 1 September 2021, the Netherlands had four crisis teams and six linking organisations that are officially designated as partners in the nationwide system. With these linking organisations and crisis teams, the NCSC can share information about new, current vulnerabilities and threats which it in turn has been informed about by other (international) sister organisations, by cybersecurity researchers or by security services.

Best practices can also be shared. This strongly increases the reach of the NCSC, as central hub. After all, this means that not only government organisations and vital organisations are informed directly about acute threats, but via the nationwide system linking organisations and crisis teams, hundreds if not thousands of other organisations also receive this information, including municipalities, colleges and universities, healthcare institutions, etc. These linking organisations are in close proximity to their own 'constituencies', speak the same language and are often very familiar with the (cybersecurity) problems faced by their affiliated organisations. A nationwide system of linking organisations and crisis teams gives rise to a 'hub and spoke' model so that information on vulnerabilities and other security issues can be transported quickly and adequately down to all levels.

Analyses

[283] Government Gazette [2020]. Regulation for designation of computer crisis teams. Government Gazette of the Kingdom of the Netherlands, 13 January 2020, number 4420

[284] NCSC [2020]. Connection to the nationwide system. https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds

- Unfortunately, a genuine vision on the nationwide system has not yet taken off and mainly existing linking organisations and crisis teams constitute part of the system at present. In short, more direction is needed with respect to the system. The preparation of an overview of gaps and a multiyear implementation program could be considered in this respect. The Netherlands currently has only a few sectoral CERTs; important sectors like the energy sector, the telecom sector and the transport sector do not have one, for instance. Umbrella organisations can play an important role in setting up sectoral CERTs because they represent the interests of many organisations in a sector and can engage in dialogue with them on this. Umbrella organisations also often have good insight into the cyber-related problems of their members and of the sector as a whole. Both the CERT of the Dutch municipalities and Z-CERT were set up with the assistance and efforts of umbrella organisations.
- There must also be financial support to start up sectoral CERTs. If the CERT becomes an independent legal undertaking and must support itself financially, a start-up subsidy will be required, at least for the first year, for recruiting cyber specialists, purchasing hardware and software, and for its accommodation, among other things.
- The Nationwide System is not only the responsibility of the Ministry of Justice and Security, all departments must commit to this and contribute to making the Netherlands more cyber resilient in the future. The NCSC functions as a hub in this context, in an extensive and expansive network of spokes which can quickly and adequately respond to national cyber crises and which informs all vital and crucial organisations in a timely manner about new cyber threats and adequate response measures. A legal framework must be introduced to mandate the sectoral CERTs for their task so that they can - in close cooperation with the NCSC - track down vulnerabilities and incidents in the sector and provide perspective for action and follow-up.

18. Digitalisation of education requires the protection of public values

Bart Bosma and Iris Huis in 't Veld

Education is digitalising, with ICT support becoming increasingly important as a result. Over the past several years, many institutions have switched to cloud-based providers for their data storage, email, collaborative environment and other (educational) applications. The question is whether this is compatible with the public values that educational institutions seek to protect.[285] Cloud-based providers offer excellent platforms for developing and making learning materials available, but apply their own standards, on which educational institutions have little or no influence. Furthermore, the providers gain access to — commercially — very interesting data of pupils, students and teachers. It is not clear what they do with those data outside the context of the educational platform. Public values such as autonomy, accessibility and inclusivity are, alongside security and privacy, fundamental aspects for shaping a robust social and technical educational environment.

Move to digital

Dutch educational institutions are currently going digital *en masse*. This digitalisation contributes to the institutions' ambition to organise top-quality education in a flexible manner that is consistent with the modern way of working of organisations, teachers and students. The fact that higher education sees digitalisation as an important priority is illustrated by, among other things, the Educational Innovation with ICT Acceleration Plan.[286]

The digitalisation has also been accelerated as a result of the coronavirus crisis. At a dizzying pace, educational institutions ensured that all education could be provided online. In a short time frame, important choices were made, technology was purchased and teachers set about teaching online. The rapid transition also

[285] https://link.springer.com/content/pdf/10.1007/s10997-021-09596-4.pdf (30 Aug 2021)

[286] https://www.versnellingsplan.nl/

prompted discussions: some institutions initially opted for Zoom as an online platform, for instance, because of the user-friendly interface, while security and privacy aspects of this provider were initially somewhat overlooked, which caused many institutions to ultimately choose a different solution. Another example is the use of online proctoring tools because examinations had to be administered online and surveillance was required. Students objected because of the privacy-sensitivity of these kinds of tools, which even resulted in some students bringing legal action against their institution.[287]

Vulnerabilities

The fact that digitalisation introduces vulnerabilities is no surprise, especially when undertaken at a rapid pace or on a large scale and in a sensitive context. On Christmas Eve 2019, the education sector in the Netherlands got a rude awakening. Maastricht University was attacked with the Cl0p ransomware.[288] Systems and data were no longer accessible and education and some research came to a standstill. The university decided to pay the ransom to safeguard the continuity of education and research. It quickly became clear that earlier that year, Antwerp University had been hit by a similar ransomware attack and afterwards it turned out that a number of other institutions in the Netherlands had made a narrow escape. Thanks in part to the openness that Maastricht University immediately provided via the cooperation of educational and research institutions in SURF,[289] they were able to take countermeasures on time. This likely prevented a great deal of damage at other institutions.

Since that time, educational institutions, both individually and in cooperation with SURF, have been working hard to further improve the security of their digital infrastructure, better chart out where their vulnerabilities lie and take their cooperation to the next level.

Platformisation

Security and privacy are fundamental in protecting digital infrastructure. Institutions of higher education have therefore made significant moves towards

[287] https://www.scienceguide.nl/2020/06/uva-mag-van-rechter-gebruikmaken-van-online-proctoring/

[288] Cl0p ransomware is a virus that encrypts files, making them inaccessible for the user, after a system has become infected. In order to get the key that makes the files accessible once again, ransom must be paid.

[289] https://www.surf.nl

more professionalisation in this regard over the past years. At the same time, organisations are increasingly joining up with various platforms that facilitate education, simplify management, are secure and also seemingly cost-effective.

But the challenges of 'platformisation' (see below) and the dependency on (large) tech companies raises a great many new questions, in which public values play an important role: how do you ensure that educational institutions retain sovereignty over study data generated on platforms that are in the hands of commercial providers? How do you organise that educational institutions retain enough control over the development of technology that determines how education is designed? How do you retain freedom of choice and prevent vendor lock-ins that can be accompanied by exorbitant price increases? How do you ensure that the use of technology remains transparent for users? How do you make optimal use of technology to increase efficiency without simultaneously losing sight of the human dimension?

These questions are increasingly urgent because educational institutions are becoming more and more dependent on a limited number of digital service providers for both their organisation and the delivery of education. This growing dependency is driven in part by the platformisation. The major tech companies like Apple, Google and Microsoft each have their own digital ecosystems, in which services link up seamlessly with each other. While this offers a great deal of convenience for users, it also causes lock-ins and compartmentalisation. Users cannot work easily with others outside their own ecosystem and - unless they can work together without restrictions - services from outside automatically are at a disadvantage, because they do not function well in the ecosystem of the dominant parties.

Moreover, the tech giants are gaining more and more influence in education itself because of the possibilities that the platform does or does not offer. This is not only making educational institutions more dependent on the platforms, but the choice for a particular platform also determines how the education itself is organised: an undesirable development.

Public values

In 2018, in response to the Gerkens motion[290] in the Dutch Senate, the Rathenau Institute called for targeted digitalisation, i.e. value-driven innovation and

[290] The motion from Gerkens (SP) et al. concerning a study by the Rathenau Institute into the desirability of an advisory committee on the ethical side of the digitalisation of society.

reconsideration of the social and ethical aspects of digitalisation.[291] The government, business sector and social organisations must shape and direct the digital society in such a way that people and public values are the priority. They should not leave the digital transformation to commercial parties.

This awareness has also reached the education sector. At the end of 2019, the rectors of the universities wrote a newspaper essay in which they sounded the alarm about the enormous dependency on the (US) tech giants.[292] In the meantime, these same institutions, perhaps for economic reasons, have diligently proceeded to switch to (cloud-based) solutions from these same tech giants. A number of professors united in the ACCSS (Academic Cyber Security Society) also recently called in an open letter for more reflection on the decision to transfer ICT services to the cloud or instead keep them under own management, for example together with SURF.[293] And the VSNU working group on public values published a recommendation in April 2020 arguing, among other things, that universities must work together on a digitalisation strategy and anchor their attitude, ambitions and actions in relation to digitalisation and public values in a Declaration.[294]

Standards

One of the dilemmas is that the tech giants use their own (closed) standards or, in some cases, do use open standards, but implement them in a vendor-specific way, so that interoperability remains difficult.

Interoperability means that services and products from different providers connect with each other and can work together without restrictions, allowing the user/purchaser to make his/her own choices instead of being dependent exclusively on what one provider offers. One of the possibilities for creating interoperability is using open standards.

For the education and research institutions to have influence on the platforms, they would have to embrace and develop (open) standards themselves, jointly promote these and impose them as a requirement when selecting platforms, preferably in an international context. Open standards ensure interoperability,

[291] Kool, L., E. Dujso, and R. van Est (2018). *Doelgericht digitaliseren – Hoe Nederland werkt aan een digitale transitie_waarin mensen en waarden centraal staan*. The Hague: Rathenau Institute

[292] https://www.volkskrant.nl/columns-opinie/digitalisering-bedreigt-onze-universiteit-het-is-tijd-om-een-grens-te-trekken~bff87dc9/ (22/12/2021)

[293] https://accss.nl/open-brief-overstappen-naar-de-cloud-bezint-eer-ge-begint (11/06/2021)

[294] https://www.vsnu.nl/files/Advies%20werkgroep%20publieke%20waarden%20onderwijs.pdf

prevent vendor lock-in and promote innovation. It also requires that education and research institutions cooperate and are willing to get off their own hobby horses.

Security architecture

The question remains how to increase the security of the digital infrastructure at education and research institutions without losing the open character of the institution. A number of joint initiatives have been set up to this end within SURF,[295] including the Higher Education Reference Architecture (HORA) and the Higher Education Sector Architecture (HOSA). There are also European initiatives coordinated and managed by GÉANT.[296] HORA focuses on the information management, including security and privacy aspects, of individual institutions, while HOSA focuses on joint facilities with due observance of public and educational values.

GÉANT provides for European cooperation between the Research & Education organisations in the European countries. There are various projects, of which the cooperation with the European Commission is an important one:

- 'The GÉANT project is a fundamental element of the European e-infrastructure. Through its integrated catalogue of connectivity, collaboration and identity services, GÉANT, together with its National Research and Education Network (NREN) partners, provides users with unconstrained access to communication, computing, analysis, storage, applications and other resources, whenever and wherever needed.'[297]

Conclusion

Digitalisation offers opportunities, but also brings with it risks. Educational institutions have matured significantly over the past several years when it comes to security and privacy protection. Nonetheless, there have been several incidents that call for an even more robust digital infrastructure. Because of, among other things, the growing influence of a few big providers in and on the education, it is important to broaden the perspective on the protection of the digital infrastructure from security and privacy to public values, in which security and privacy are indeed important components.

[295] https://www.surf.nl/werken-met-architectuur

[296] https://www.geant.org

[297] https://ar2020.geant.org/

To achieve *open and secure education* that upholds public and educational values such as transparency, privacy, security, reliability, accessibility, freedom of choice and high quality, educational institutions must work together to develop initiatives as quickly as possible to influence the standards used by the big cloud/platform providers and create their own open standards.

The digitalisation of education has been accelerated by the coronavirus pandemic, so time is pressing.

Analyses

- Strategic procurement: working together as a sector is crucial to be able to stand up to the tech giants. It is difficult for a single education and research institution to force changes to the platforms of a major player. Institutions must jointly determine what their precious assets are and decide what must remain under their own management and what can be outsourced. This is based on a fundamental decision: are the institutions willing to choose a less cost-efficient route in order to ensure that public values are safeguarded?
- The government contributes: the EU and the Dutch government can curb the power of the tech giants via legislation and regulations. The government can provide for the financing of solutions which may be less desirable in terms of cost efficiency, but which are indeed desirable from the perspective of protecting public values. The government can facilitate and encourage the creation of open standards and make the requisite knowledge and resources available for this.
- We are stronger together: cooperation is the only way to stand up to the cyber and other threats facing the education and research sector. There is a glaring shortage of information security expertise. Combining knowledge and resources makes it possible for the sector to act quickly and effectively. Cooperation is indispensable on the administrative level as well. Acting together requires letting go of individual preferences and going along with the others, even if that might not be the best solution for an individual institution in certain situations.

19. The human side of phishing

Patrick Borsoi

One's email inbox has started to resemble an aquarium more and more over the past few years. Among the bona fide emails there are always a few 'phish'. Anyone who thinks they have never had to deal with phishing is probably wrong and may well belong to the group of vulnerable users. Cybercrime — and with it, phishing as a way of obtaining confidential information by pretending to be a reliable entity — is one of the most democratic manifestations of crime. No distinction is made between poor and rich, it doesn't matter where you live, what the person in question looks like or how he or she behaves. Moreover, criminals use the shotgun approach on us. One almost cannot avoid facing this illegal phenomenon. Information security experts are happy to explain how to recognise phishing and how to handle it. We mainly address the other side: why do people fall for it and what can we do about that?

The Bol.com case

In November 2019, Dutch online retail service bol.com received an email supposedly originating from Brabantia, a household goods manufacturer, stating that payments for products sold would henceforth have to be paid into a Spanish bank account.[298] The text was written in abominable Dutch. And granted, this archetypal Dutch company actually has an office in Spain, but beyond that the request was devoid of any logic. Despite these red flags, someone at bol.com must have shrugged and made the change. Damage: over 750,000 euros. The court held that bol.com should have phoned Brabantia to ask whether that email actually came from them; the court then ordered bol.com to cough up the loss.[299]

[298] https://tweakers.net/nieuws/181152/bol-punt-com-trapte-in-phishingmail-en-maakte-750000-euro-over-naar-oplichters.html

[299] Judgment: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2021:1528

The directly measurable financial damage from phishing in the Netherlands in 2020 was calculated at €12.8 million.[300] Indirect damage also arises if criminals use the stolen information elsewhere, for instance by using hijacked accounts to send out spam.

Arms race

In most phishing, it's not laid on as thickly as in the bol.com case. There is a real arms race going on: the more security-aware people become, the more inventive criminals become. While a non-Dutch-speaking criminal could, in the beginning, get away with a simple email run through Google translate, these days you need to speak perfect Dutch, use the logo of the company you are impersonating, and sign the email with the actual CEO’s name. The sender’s address and link on which prospective victims are to click should preferably closely resemble that of the genuine company. It is therefore becoming more and more difficult to pick out that one false email from the daily mountain of bona fide messages.

Well-known company

A modest survey of my own from 2020[301] in response to a phishing email received by several employees prompted the insight that it is far too short-sighted to think: how could you be so dumb as to fall for it. The email in question had used a hacked email account, which meant the email had actually been sent from (but not by) the particular company. Some recipients knew the company by name, or did business with similar companies, so that it was not illogical that this company would be emailing them. There were also people, however, who said they thought it was very strange to be receiving the email but opened the attachment anyway. They lacked that extra bit of insight to arrive at the correct decision and ignore the email.

Phishing, vishing, smishing

Phishing occurs in a number of manifestations. The archetypal phishing would have been a telephone call that went something like this: “Hello, this is your bank. You reported your bank card as lost and we have good news: it has been found! To check that everything is in order, we do need your pin code.’ The telephone is still used these days as a means; just think of the countless cases of helpdesk fraud, whereby criminal call centres (usually in India) work through entire phone books

[300] https://www.betaalvereniging.nl/actueel/nieuws/schade-fraude-2020/

[301] https://securityblogpatrick.blogspot.com/2020/06/phish-gephileerd.html

pretending to be employees (usually) of Microsoft in order to 'help' their victim with computer problems.[302]

This form of phishing is also referred to as 'vishing' (voice phishing). Yet another form of phishing uses sms text messages. In essence, this 'smishing' works no differently than phishing via email, but is more compact. So it takes less work from the criminal (short and sweet, no logos required). Because of this compactness, the recipient has fewer opportunities to recognise the message as phishing.

Awareness

Anyone looking for a remedy for phishing mainly finds tips for recognising it. People must be made aware of the risk and they must learn to apply that knowledge each time. That will not always work, as the survey cited shows. The willing / able matrix of occupational consultant Hanneke Tijken,[303] with the willingness to do something along the one axis and the person's ability in that respect on the other axis can also be applied to this topic. People who are both willing and also able to apply the security guidelines need little attention. A person who is indeed willing but not yet able is part of the most grateful target group for awareness. And those who are not willing but who are indeed able may still be able to be persuaded. The last quadrant, people who are neither willing nor able, must largely be regarded as lost (or a disproportionate amount of time and energy must be put into them). The key target group for awareness training is therefore the people with 1 'yes' and 1 'no' in the matrix.

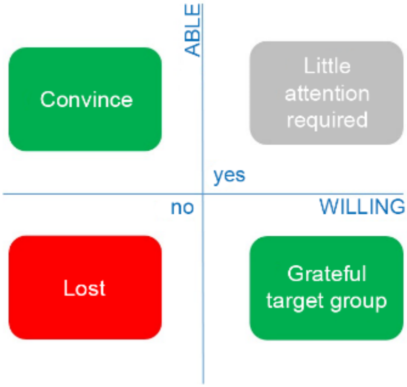


Figure 1. The willing / able matrix

[302] https://www.fraudehelpdesk.nl/fraude/ik-heb-contact-gehad-met-een-helpdesk/

[303] H. Tijken, *Aan het werk! Over trajectbegeleiding en re-integratie*, 2012

Secure email

Ideally, it shouldn't be necessary to position people in the frontline against phishing. Smart software should ensure that phishing emails never even make it to your inbox. Some of the email is already prevented by spam filters, because there are similarities between these two forms of malicious email. But that is not enough: while 'normal' spam mainly causes annoyance, one single phishing email, which for instance results in a ransomware attack, could mean the end of a company. There is an urgent need for new filters, therefore.

Although secure email gateways (SEGs) do exist, and are becoming better and better at detecting phishing, these are far from watertight. A SEG can filter for already known phishing sites, for instance. If an email contains a link to one of these sites, the SEG will refuse the email. To do that, a SEG creator must, however, keep a list of phishing sites, and even though this is done in an automated manner, of course, it is still a huge task, and by definition it is always behind the facts. SEGs can also use other techniques, such as recognising brand impersonation. Research firm Gartner says that a SEG should be able to recognise the 50 most commonly impersonated brands.[304] That still leaves plenty of impersonation opportunities for criminals.

There are also technical protocols[305] available to make email more secure. Their success relies entirely on the degree of penetration. It is difficult to find hard, recent figures on this, but the few sources that do exist paint the picture that these protocols will not be the salvation for now.

Smartphone lending a hand

An SEG does not help against vishing and smishing, after all that does not take place by email. Telecom companies evidently do not feel called on to take action against these forms of crime. The smartphone itself can help in the fight against smishing, fortunately. Android's sms app has a 'spam detection' option that can learn to detect known spam patterns. Apple leaves this to third parties, who develop apps that can connect with the Identity Lookup framework[306] and then filter for suspicious telephone numbers and links, for instance. Although these systems cannot stop all false sms messages, it is commendable that our devices lend us a

[304] Solution Criteria for Secure Email Gateways, Gartner, Published 1 March 2021 - ID G00734278, https://www.gartner.com/document/3998744

[305] DMARC, SPIF, DKIM

[306] https://developer.apple.com/videos/play/wwdc2017/249/

helping hand. Both the Google and the Apple approach require input, but both manufacturers insist they do not use privacy-sensitive information for that.

Artificial intelligence

So computers can learn to recognise false messages. With regard to email, however, this occurs only sporadically at the moment, because it is not easy to properly apply machine learning technology, mainly because criminals behave unpredictably. Criminals themselves are increasingly using this technology, which they use in attempts to circumvent counter measures.[307] It also turns out that computers can write better phishing emails than people.[308]

Conclusion

The user's inbox has become an aquarium these days, beyond the user's control, which the user him/herself must maintain. This is becoming more and more difficult; on the one hand because criminals are developing more sophisticated techniques, and on the other because the technology still does not provide enough assistance in preventing false messages and phone calls. This puts people from all segments of society in the frontline in the battle against these international criminal practices.

For consideration, some advice

Because of the sombre conclusion, it is important to nonetheless conclude this article with some advice to help you protect your personal and business environment.

- Use your common sense. If something sounds too good to be true, it usually is; you can't win a lottery if you haven't played.
- Activate 2-factor authentication[309] wherever possible. This minimises the likelihood that a criminal who has stolen your password can actually access an account.

[307] AI as a Target and Tool: An Attacker's Perspective on ML, Gartner, Published 19 June 2019 - ID G00381087, https://www.gartner.com/document/3939991

[308] AI Wrote Better Phishing Emails Than Humans in a Recent Test, WIRED, 08-07-2021, https://www.wired.com/story/ai-phishing-emails/

[309] https://veiliginternetten.nl/themes/situatie/wat-tweestapsverificatie/

- Use different passwords for different accounts. This limits the scope of a successful phishing campaign.

Specifically for organisations:

- Implement protocols that help combat phishing.
- Provide inbound email with a warning ('Beware. This email has come from outside our organisation. Be extra careful opening links and attachments.')
- Make sure that your outbound email does not inadvertently contain hallmarks of phishing, such as an impersonal greeting or links to a 'strange' domain. This prevents confusion.

Finally, a piece of advice to politicians and administrators: ensure more ICT expertise in your ranks. An understanding of this material and of the implications of cybercrime - and of cyber espionage! - is desperately needed if the Netherlands is to hold its own on the digital world stage in the coming years.

20. DPIA as an instrument for better digital information security

Michelle Wijnant

The performance of a so-called data protection impact assessment - or DPIA - is compulsory for every organisation on grounds of European privacy law if the envisioned processing of personal data involves a high risk to privacy. Looked at more closely, a DPIA is a written investigation in which the proposed processing is tested against the applicable privacy legislation and regulations. Since more and more processes take place online and organisations are moving 'to the Cloud' *en masse*, digital information security is becoming an increasingly important topic in DPIAs. DPIAs have to satisfy certain requirements and a certain process will have to be gone through in an organisation. Various models are available for performing a DPIA. From Dutch practice, it emerges that a DPIA is sometimes used retrospectively as well, as follows from the case that occurred at the central government.

When is it compulsory?

A DPIA is required by law for all processing of personal data that is likely to entail a high risk.[310] It is usually performed in advance, which, in principle, is required.[311] Performing a DPIA after the processing has already started, can also serve well, however. For example, the central government performed a DPIA on Microsoft Office 365 Online and mobile Office apps[312] even though it was already using these. The DPIA highlighted multiple high privacy risks, which the central government was able to mitigate after negotiations with Microsoft.

[310] Article 35(1) General Data Protection Regulation (GDPR).

[311] Article 35(1) and recital 90 GDPR. Of course, it is also relevant to still carry out a DPIA for processing that has already started and for which a DPIA is mandatory, if one has not yet been performed.

[312] URL: https://www.government.nl/documents/publications/2019/07/23/dpia-microsoft-office-365-online-and-mobile-slm-rijk-23-july, most recently accessed on 08/10/2021.

The privacy risk is assessed in a DPIA with reference to the event that will happen and the possible effects thereof, which are estimated in terms of seriousness and likelihood. It has been determined that the performance of a DPIA is always required for certain processing operations.[313] This could include profiling, the use of monitoring, camera supervision, blacklists, the (large-scale) processing of special personal data[314] or sensitive data,[315] the sharing of these data in collaborations, the merging of datasets or the use of new technological or organisational solutions.[316]

The obligation to perform a DPIA is borne by the controller. If a processor is involved, the processor is required to assist the controller with the DPIA in accordance with agreements from the processing agreement.[317]

Performance

For the performance of a DPIA, an organisation itself must choose or create a model and/or method. There are several different models in circulation. Models that could be used (as inspiration) are, for example:

- NOREA (very extensive and as such suitable for very high-risk processing operations, for instance);[318]

[313] These processing operations are designated as high risk in the ‘Guidelines for data protection impact assessments and determination whether a processing operation “likely entails a high risk” in the sense of Regulation 2016/679’, as most recently amended and adopted on 4 April 2017, from the Article 29 Working Group (now: European Data Protection Board) and *Government Gazette* 2019, no. 64418.

[314] These are data that say something about someone’s race, ethnic origin, political, religious or philosophical convictions, sexual life or trade union membership. This also includes genetic data, biometric data and health data. See also Article 9(1) GDPR. The Citizen service number is often considered to be included in this category of data because of the very restrictive conditions under which it may be processed. See also Article 87 GDPR in conjunction with Section 46 of the General Data Protection Regulation Implementation Act (UAVG).

[315] These are data that have not been designated special personal data in the GDPR but which are considered sensitive in society, such as: data on a person’s professional achievements, financial or economic situation, personal preferences or interests, personal problems, reliability or behaviour, location or movements, data from personal documents and login data.

[316] See also Recital 89 and 91 GDPR.

[317] Article 28(3)(f) GDPR.

[318] URL: https://www.norea.nl/nieuws/8151/nieuwe-norea-handreiking-data-protection-impact-assessment, most recently accessed on 16/06/2021.

- CNIL (from the French supervisory authority and made available together with tooling to enable the DPIA-process to be conducted digitally, and including various explanations);[319]
- Criteria put together by the Article 29 Working Group (particularly suitable for inspiration for creating one's own DPIA model);[320]
- ICO (from the English supervisory authority, a concise model that can be used for 'light' DPIAs).[321]

Many organisations opt to perform a DPIA not only for mandatory processing operations, but also for operations for which it has not yet been established if they involve a (high) privacy risk or in which the organisation has a major interest. This is why organisations often have two models in use: one model for the processing operations for which a DPIA is compulsory (like migrating the entire digital environment to the Cloud) and a light model for the less risky processing operations or for operations where the risks cannot yet be properly assessed (when a new events tool is put into use, for instance).

Digital information security

As already stated, information security is an important part of a DPIA. Because one of the components that must be tested within a DPIA is whether 'appropriate technical and organisational measures' have been taken. This could include measures such as: authorisations, encryption, encrypted connections, logging, pseudonymisation, physical access control, et cetera. Can no appropriate security measures be taken? Then that is a risk that must be highlighted in the DPIA.[322] To assess whether the security measures are 'appropriate', the following must be looked at:

[319] URL: https://www.cnil.fr/en/privacy-impact-assessment-pia, most recently accessed on 16/06/2021.

[320] URL (Dutch-language version): https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf, p. 28 et seq. Most recently accessed on 16/06/2021.

[321] URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/, most recently accessed on 16/06/2021.

[322] It is of course also possible to carry out the test for (digital) information security in a specific security assessment (such as Business Impact Analysis (BIA) and/or Threat and Vulnerability Assessment (TandVA)) to which reference is made in the DPIA.

- The current state of the art (what is possible at the moment?);
- The implementation costs (what do the (various) security measures cost?);
- The nature, scope and context of the processing purposes (what does the processing entail, what and how many personal data are processed for this and what is the aim?);
- The risks in terms of seriousness and likelihood (what could go wrong, how serious are the consequences and how likely is it that this would happen?).[323]

The reason why these four facets must be looked at, is to ensure that the risk is proportionate to the measures (and their costs) which are taken. This risk-based approach prevents the security framework from the privacy legislation becoming outdated too quickly.

Required persons and positions

The writing of a DPIA in any event requires persons with knowledge about:

1. The project/process/system to which the DPIA pertains;
2. The organisation of the controller;
3. The privacy legislation and regulations;
4. The state of the art and the possible technical and organisational security measures; and
5. The working method/product of the processor, if the processing is carried out by a processor.

A project team is usually put together to perform a DPIA, whereby every area of expertise is asked for input.

Start moment and time periods

In terms of lead time, a full DPIA takes three months on average. This is because expertise is needed from different areas and there are often multiple coordination, review and advisory rounds needed before a DPIA is definitive. Light DPIAs take two weeks on average because all the risks and requirements are zoomed into in less depth.

If a DPIA pertains to a product/activity to be procured, it is advisable to request information on information security and privacy in the tender procedure already. As soon as this is received, a light DPIA could be performed. This ensures

[323] Article 32 GDPR.

that information security and privacy is already taken into account when choosing a product/activity. Once the choice for a product/activity has been made, a full DPIA can be performed. In this way, the privacy and information security test delays the process as little as possible but the statutory requirements can still be satisfied.

A similar strategy is advisable for new ideas or plans in an organisation. Once the main points of these are known, a light assessment can already be performed to verify whether all the relevant elements have been considered. The height of the risk can already be charted out in this way. Once the plans are then made concrete, the full DPIA can be performed.

Mandatory advice

If a Data Protection Officer (DPO) has been appointed at the controller's organisation, it is required that this DPO be asked for advice on the DPIA.[324] The DPO is then free to decide whether he/she wants to give advice or not, and if so, in what form. Advice provided by the DPO must be added to the DPIA. If the DPO's advice is not followed, a reasoned explanation as to why not must be documented.

If the DPIA highlights high privacy risks that cannot be mitigated, the relevant supervisory authority must be consulted in advance. The supervisory authority then also provides advice and can already exercise its powers (for instance, to start an investigation and take corrective measures).[325]

In cases that arise, the opinion of data subjects or their representatives must also be requested (for instance, by means of a survey). The opinion of employees could be asked, for instance, if the DPIA pertains to an employee survey, or the opinion of a consumer organisation if the DPIA pertains to developing customer profiles. The opinions obtained must be documented in the DPIA. If the controller decides not to ask the data subjects' opinions and/or not to follow the outcome of that, this must also be documented with reasons.

DPIA policy

In order to safeguard the DPIA process, it is important that it be documented in the controller's organisation:

- Where high risk processing operations must be reported in the organisation;
- When it is compulsory to perform a DPIA;

[324] Article 35(2) GDPR.

[325] Article 36 in conjunction with 58 GDPR.

- Which employees are involved in the performance of a DPIA, who is responsible and how the route to the DPO works;
- Which DPIA-model should be used, and where this can be found;
- Where the DPIAs must be stored and registered;
- How it is guaranteed that the DPIA is updated periodically.

Conclusion

The performance of a DPIA is compulsory for processing operations with a high privacy risk and, depending on the project/process/system to which it pertains, can be a complex matter in which people with various specialisms need to be involved. Since in many organisations, the focus is increasingly on digitalisation, the aspect of (digital) information security plays an ever-more important role in DPIAs. DPIAs are also ideally suited instruments for considering information security in a structured and thorough manner.

Points for attention

- Make sure that a DPIA is performed for all processing operations for which a DPIA is compulsory.
- Choose or create a DPIA model that is geared to the organisation, and preferably use two DPIA models (an extensive version for mandatory cases and a light version for other cases for which a prior privacy and information security investigation is desirable).
- Make sure that the DPIA tests whether appropriate technical and organisational measures have been taken and see whether it is possible to mitigate the privacy risks using (supplementary) security measures.
- For every DPIA, put together a team of people with the requisite expertise, include the processor (if relevant) and ask the DPO and/or the supervisory authority for advice (if relevant) and/or ask data subjects for their opinion.
- Prepare a DPIA policy which specifies how, by whom and in what manner the organisation deals with the DPIA requirement and make clear agreements on DPIAs with processors.

21. IT report and assurance statement offer structural benefits

Jan Matto, Wilfried Olthof and Marc Welters

A plea from the digital infrastructure sector in the Netherlands for a mandatory annual IT audit at companies and government organisations that belong to the so-called ‘vital infrastructure’ of the Netherlands prompted NOREA, the professional association of registered IT auditors in the Netherlands, to undertake further investigation. How could an IT audit opinion be provided for? The outcome of such an audit ultimately determines that the audited organisation is adequately ‘in control’ of its IT and the related digital security. NOREA is currently working on guidance of an IT report with reference to which the company or government organisation accounts for itself and this account is then audited by the IT auditor. To this end, based on international reporting standards, best practices in the area of IT governance are being developed.

Towards objective IT report

In an interview on Business News Radio (BNR) on 22 January 2020, Michiel Steltman, spokesperson for Digital Infrastructure Netherlands, argued for a mandatory annual IT audit at companies and organisations that are part of the Netherlands’ vital infrastructure.[326] A comparison was drawn with a financial audit. In principle, the accountant who audits a company’s financial statements is expected to also give an opinion on the continuity and reliability of the electronic data processing underlying the financial reporting processes.[327] However, this opinion, which mainly focuses on the audit of the financial statements in its current form, is too limited to give an adequate opinion on the setup of the IT management and the governance of IT which goes beyond the financial accounting processes. Let alone that there would be room in this to determine, for instance, whether an organisation is

[326] https://www.bnr.nl/podcast/digitaal/10400732/to-update-or-not-to-update (BNR, 22 January 2020)

[327] Article 2:393(4) of the Dutch Civil Code.

adequately resilient against cyber attacks and is prepared for the near future in terms of IT.

Moreover, the importance of the control of digital systems and processes now reaches beyond the individual organisation's own interest. The entire ecosystem of an organisation can be dependent on the control of IT systems and processes. The ecosystem comprises a range of stakeholders, from supervisory bodies, supervisory directors and credit lenders, to clients, clients of clients and, ultimately, individuals.

The societal and economic damage from a cyber incident can be many times greater than the damage to the organisation directly affected by the cyber incident. So there is a broader interest to serve than the immediate IT risks linked to an individual organisation. It is also about providing insight into the control of the digital effects on an organisation's environment.

The Netherlands is one of the most highly digitalised countries in the world. IT is in every layer of the business processes of organisations. The Netherlands is also a hub in worldwide internet traffic. Many of the trans-Atlantic internet cables come on land in the Netherlands and then branch out across Europe. IT is now increasingly a topic among directors, administrators and supervisory bodies of (government) organisations. From conversations with these directors, administrators and supervisory bodies we have learned that they want to know whether their organisation's control of IT is adequate. Since the answer to this question does not lie primarily in the scope of an accountant or auditor, there is a growing need for an objective way in which this IT report can take place.

Assurance report from IT auditor as extra safeguard with the IT report

That is why a NOREA working group is currently developing a format for an IT report that, depending on the type of company or organisation and the presumed risks in the industry or sector in which activities are operated, will form the basis for this IT report. The management will then draw up a statement on the IT report, which will be checked by the IT auditor and on which he will subsequently issue an assurance report including an IT audit opinion. An analysis of strategic business objectives, stakeholder perspectives and digital risks for an organisation's ecosystem will help provide direction for the contents of the IT report. The assurance report prepared by the IT auditor in response to this report can be regarded by stakeholders and third parties as an extra safeguard, with a view to the continuity and resilience of the IT governance that can be assumed.

In developing a format for the IT report, the NOREA working group looked at, among other things, the GRI (Global Reporting Initiative) standards for sustainability reporting, because an international report is already operational based on this standard.[328] For the content of the IT report, relevant 'IT Topics' were identified which define the scope of the the report, such as, for instance, (Cyber)security and Privacy, IT Continuity, Incident Management, Change, Data Governance & Ethics, Compliance & Eco-system.

The reporting method assumes a baseline for IT risk management supplemented with objectives formulated by the organisation itself and risks it has identified in relation to digitalisation, and the measures taken in response.

Topics which are reported on

Without attempting to provide a comprehensive list in this article, an illustration is provided below of the topics addressed in the IT audit reporting method. The overview stems from the interim results of an ongoing survey by the NOREA Professional Regulation Committee, the committee currently charged with further elaborating the IT audit reporting method.

- **(Cyber)security.** The reporting topic of cybersecurity addresses the risk management linked to the specific setup of an organisation's IT environment, the role that IT plays in the chain of which an organisation may be part, the protection of data, the continuity of data processing and the capacities available for anticipating expected developments in relation to cybersecurity.
- **IT Continuity.** IT continuity refers to an organisation's own performance and its dependencies on IT. Also very important, however, is the potential impact of an organisation's use of IT on its environment. Topics discussed in this context also concern identifying the potential societal damage caused to the organisation's ecosystem by system failures, the impact on information chains, continuity risks linked to licence management and contract management.
- **Incident Management.** Incident management from the perspective of the IT audit report means the reporting on digital incidents that have manifested, the subsequent incident response and the degree to which lessons are learned by taking future-looking measures based on the root cause analyses.

[328] See the text added below about the Environmental, Social and Governance reporting standards based on the Global Reporting Initiative.

- **Change.** Various stakeholders indicate that they want insight into an organisation’s innovative capacity. Are the steps being taken towards digital transformation geared to the company objectives formulated? The degree to which IT projects are being realised as compared to the project objective also falls under this reporting topic.
- **Data governance & ethics.** Data governance is relevant, on the one hand for achieving the company objectives and the vital role it can play in an organisation’s revenue model. On the other hand, data governance is an important topic in compliance with legislation and regulations. It is also a topic that has a place in corporate social responsibility. Consider the ethics surrounding the use and handling of personal data, privacy requirements, issues relating to data retention, the use of algorithms, artificial intelligence and machine learning. The importance of recognising the potential negative or positive impact of an organisation’s digital footprint on stakeholders in that organisation’s ecosystem is a topic that is being increasingly acknowledged.

For the audit of specific control objectives and measures, the IT auditor can of course draw on the most relevant and acceptable standards frameworks that are available for this.

According to NOREA, the introduction of this IT report need not be too complicated in practice. After all, in the current situation, the IT auditor is already part of the external auditor’s audit team. The IT auditor can broaden the scope of the opinion from purely financial aspects to the entire IT organisation. A concurrence of other, already existing audit operations can also be strived for if the organisation already uses IT auditors who, for instance, assess the cybersecurity or processing of personal data in accordance with the GDPR, whether or not as part of a third-party assurance report. This also keeps it affordable.

Conclusions

The professional association of IT auditors NOREA advocates the introduction of an annual IT report, including security aspects, because on the basis of objective criteria and starting points, the transparency in relation to the resilience of businesses and organisations in vital infrastructure, along with their suppliers, will increase. This contributes to our digital security and continuity. NOREA is therefore developing proposals for the format of an IT report with reference to which companies can account for themselves, and this account is then verified by the IT auditor. The management will then draw up a statement on the IT accountability, which will be checked by the IT auditor and on which he will subsequently issue an assurance report. As a basis for the reporting standard, NOREA is looking to the ESG standards of the Global Reporting Initiative, to which the IT report could be added as a topic-specific standard. Topics that would be addressed in the report include Cybersecurity, IT Continuity, Incident Management, Change, Data governance & ethics.

Environmental, Social and Governance (ESG) reporting standards based on the Global Reporting Initiative (GRI)

Looking at the broader societal perspective of the IT report, the objectives and nature of the topics to be addressed, there are major similarities to the existing ESG reporting standards from the GRI. The growing importance of ESG reports is endorsed by the fact that investors and other stakeholders are calling on companies to account for their sustainability, environmental, social and governance strategies.

ESG reporting encompasses not only qualitative information on topics, but also quantitative measures that are used to measure a company's performance with respect to ESG risks, opportunities and related strategies. ESG reporting is an ideal and effective means for enabling companies to, in a single document, answer a broad range of questions that stakeholders might ask. Putting together an ESG report can be a challenge, however, because it must satisfy the requirements of the reporting methodology and attain the right balance of information from the individual agendas. The companies must also determine how relevant information must be communicated and what ESG information and indicators must be reported.

Assurance on ESG report

The professional standards contain requirements and guidelines for the involvement of the auditor if other information is included in the document with audited financial statements. Sustainability reports and ESG information is often included in company reports that do not contain audited financial statements. In these cases, the auditor has no responsibility for the ESG information in the audit of financial statements.

The information that is reported by a company must be credible, however, and properly substantiated, so that interested parties can take informed decisions. As far as the audits of the financial statements are concerned, the external assurance of an audit firm increases the reliability of ESG information that companies present to investors and other interested parties.

An assurance report is intended to increase the reliability of such information for the envisioned users of the ESG report by giving an objective and impartial assessment of the claims, data and other disclosures made by the management. Obtaining some degree of assurance via the audit encompasses evaluating processes, systems and data, to the extent applicable, and then assessing the findings to substantiate an opinion.

The most important advantage is verifying the non-financial data and information in order to help companies win the trust of interested parties.

Assurance is given by the auditor in accordance with the International Standard on Assurance Engagements (ISAE) 3000: Assurance Engagements other than Audits or Reviews of Historical Financial Information.

GRI Standards

The guidelines for sustainability reporting from the Global Reporting Initiative (GRI) provide an internationally recognised standard for preparing a sustainability report. In the context of transparency with regard to the sustainable development of an organisation's activities, companies can use a sustainability report to communicate publicly about their (positive and negative) economic, environmental and social performance.

GRI's mission is to make sustainability reporting for all organisations - regardless of size, sector or location - as routine and comparable as financial reporting. At the end of 2016, the Global Reporting Initiative published the current generation of guidelines for sustainability reporting. The GRI G4 Sustainability Reporting Guidelines (the fourth generation of the reporting guidelines, launched in 2013) have transitioned into the GRI Sustainability Reporting Standards, also called GRI Standards or SRS.

The GRI Standards are divided into six different related standards. There are three universal standards: GRI 101 Foundation, GRI 102 General Disclosures and GRI 103 Management Approach. And three topic-specific standards: GRI 200 Economic, GRI 300 Environmental and GRI 400 Social.

22. Cybercrime, from mischief to menace

Maarten Souw

What consequences does the latest hack have for my organisation? =This is the question you should be asking yourself, when following the news. You may also be wondering how humanity got here.
This chapter answers this question and looks back, in a nutshell, on a half century of cybercrime: how software lost its innocence and became an instrument of organised crime. The mechanism behind the actual hack is also briefly addressed. This look back concludes with the logical consequence of the rise of cybercrime: the renewed interest in information security.

Introduction and method

Although Von Neumann - one of the founders of the modern information society - already spoke about viruses[329] in the 1960s, cybercrime first entered the news a half century ago. The first worms[330] and viruses spread in the wild and humanity was faced with the phenomenon of malware for the first time. Criminals quickly discovered the opportunities presented by IT. IT opened new pathways for spreading digital contraband, but it also proved a means of gaining control of knowledge - the quintessential valuable of the 21st century. This marked the start of an arms race between cybercriminals and security expert.

This analysis - of all possible definitions[331] - focusses on cybercrime in a narrower sense: every form of crime for which knowledge of ICT systems is required. After all, it is the use of IT resources that makes cybercrime so accessible and gives it global impact. Add to this the fact that a large percentage of the cyber threat plays out invisibly and cybercrime gives a whole new meaning to the word 'stealthy'.

[329] Theory of Self-Reproducing Automata, Von Neumann (Burks Ed.), 1966, University of Illinois http://fab.cba.mit.edu/classes/865.18/replication/Burks.pdf

[330] https://corewar.co.uk/creeper.htm

[331] See possibly Schjolberg 2008, The History of Global Harmonization on Cybercrime Legislation

This approach also means that other aspects of cybercrime are left out of consideration. We will not be addressing the use of IT to spread illegal content, for instance; nor are things like using IT to support traditional crime discussed.

The historical role of malware in cybercrime

Although the history of cybercrime[332],[333] allows various angles of attack, the perspective in figure 1 provides the most insights; specifically, how malware developed from a helpful tool into an instrument for sabotage and espionage.

Sabotage

Rendering IT resources unusable started in 1989 with attacks on individual personal computers.[334],[335] Criminals blocked files (the key component of our information processing) or entire systems. These small-scale attacks grew into cases like StuxNet[336] and NotPetya[337.] Here malware was used to sabotage a factory or disrupt infrastructure. This sabotage software developed into ransomware: software that rendered a system unusable until ransom was paid. What is striking in this development is the growth in ambition and the capacities of the attacker. An attacker no longer has to have direct access to the victim; he or she can strike from another part of the world.

Espionage

Wiretapping is a somewhat loaded term for breaching confidentiality; this interpretation goes a bit beyond the original definition[338] of spyware. Key point is extracting confidential information. How the attacker extracts this information is

[332] Mohanta, Evolution and Shift in Trend of Cybercrime, Cyber Times International Journal of Technology and Management, Volume 10, Issue 2, April 2017

[333] Wielsputz, Evolution! From Creeper to Storm, Presentation for the Seminar on 'Malware', University of Bonn, 2006

[334] Richardson, North, Ransomware: Evolution, Mitigation and Prevention, Kansas State University 2017

[335] Hampton, Baig, Ransomware: Emergence of the cyber-extortion menace, Edith Cowan University 2015

[336] Langer, Stuxnet: Dissecting a Cyberwarfare Weapon, IEEE Security & Privacy (Volume: 9, Issue: 3, May-June 2011)

[337] A Greenberg, The untold story of NotPetya, the most devastating cyberattack in history- Wired, August, 2018

[338] Stafford, Urbaczewski, SPYWARE: THE GHOST IN THE MACHINE, Communications of the Association for Information Systems (Volume14, 2004)291-306

less relevant for this analysis. It could be the case that an attacker deliberately creates malware to this end; it could also be the case that an attacker exploits a vulnerability in existing software. So-called Trojan Horses (Trojans, a message that contains malware) are examples of a targeted attack. Heartbleed is an example of a vulnerability - in OpenSSL- that was exploited. In April 2014, the software exhibited a security leak: attackers were able to retrieve confidential information[339] by offering too long a text message (this is a form of buffer overrun attack). The SolarWinds hack[340] is an example of a targeted attack. Here, attackers (assumed to be state actors) modified management software so that they could break into SolarWinds users.

The SolarWinds hack brings this look back right up to the 21st century. It is an example of an attack via the ecosystem. Our current IT landscape displays all the characteristics of an biotope. The time in which one organisation managed everything itself, on site, is behind us. Today's IT solutions consist of an edifice of underlying solutions and services. A number of services are commonplace, like networks or data storage, others are more specialised, like identity service provision. Resourceful attackers take advantage of our dependency on service provision to attack organisations.[341] This has made cybercrime - attacks via the chain - a factor that also plays a role in service provider selection.

Figure 1: Historical background of this chapter

Year	Event	Explanation
1971	Creeper	This is an example of a worm; software that spreads throughout a network. In this case, ARPA net, the predecessor to the internet.
1986	(Pakistani) Brain Virus	First outbreak of a computer virus that attracted public attention. The Brain virus hit the emerging MS-DOS operating system, bringing the larger public in contact with malware.

[339] NIST advisory over Hearthbleed, April 2014 https://nvd.nist.gov/vuln/detail/CVE-2014-0160, retrieval date August 26 2021

[340] SolarWinds: What Hit Us Could Hit Others, retrieval date August 27 2021, https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/

[341] NIST ITL July 2012 CA Compromise, Retrieval date August 28 2021, https://csrc.nist.gov/CSRC/media/Projects/Forum/documents/2012/october-2012_fcsm_pturner.pdf

2010	StuxNet	Malware that explicitly targeted industrial control systems (SCADA). It is generally assumed that StuxNet was aimed at sabotaging ultracentrifuges[8)].
2014	Heartbleed	A leak in open source security software undermined the assumption that Open Source is unreservedly secure.
2017	NotPetya	This malware attack caused disruption in the physical economy.
2020	SolarWinds	Attackers broke into end customers via a managing party (a software provider).

A chronological overview of the examples from this chapter. This very limited group of examples illustrates how cybercrime is growing in its ambition, sophistication and impact.

This concise history illustrates how attackers learn from each other; criminals reuse components from earlier attacks and combine these into a new procedure. This reuse of information is made easier by the openness of the internet. Traces and examples of successful attacks are relatively easy to find. Where information cannot be found on the open internet, hackers share information in internet forums.[342]. This translates into a growth in the attacker's ambition and an increase in the number of threats.

Our analysis has been confirmed in part by the National Cybersecurity Centre (NCSC). This government organisation mentions in its annual assessments the advent of:

- Chain dependencies, the use of a subcontractor can offer advantages, but also presents additional opportunities for the attacker.
- Cybercrime as a service, cybercriminals don't even need to have IT knowledge themselves.[343]

This does not make the retrospective in this chapter any rosier - what may be an acceptable security solution today could be outdated tomorrow, but there is a light on the horizon. The potential victim of cybercrime is not entirely defenceless. He or

[342] NCSC, Cyber Security Assessment Netherlands 2020, outlook, p 26

[343] Cybercrime as a service (CSBN 2019, p27) (CSBN 2021, p 28)

she can stand up to cybercriminals with a good risk analysis and/or information security. Just as a good lock can prevent many (physical) break-ins, good information security helps defend against cybercrime; this view follows from a reasoning from the absurd (*reductio ad absurdum*):

1. Whether an attacker is trying to sabotage and/or engage in espionage is irrelevant. He has to manage to get in first;
2. Attackers take advantage of a number of standard vulnerabilities;
3. The usual information security is aimed at reducing these vulnerabilities.

Cyber Kill Chain or the anatomy of an attack

The first axiom is well expressed in the Cyber Kill Chain,[344],[345] the steps that an attacker takes; In every attack, there is a moment (step 3, delivery) that he actually attacks your information supply. This brings us right to step 2, how the attacker gets in. A quick analysis of ransomware (a leading source of data breaches) provides the insight that attackers usually exploit:

- Deficient IT-support, Eg. insufficient patching;
- Human weakness as a first step in the breach;
- Poor compartmentation of user rights, especially administrator accounts;

Briefly summarised, attackers exploit (recently discovered) vulnerabilities in software. A good software provider will fix the vulnerabilities and publish new software. The client organisation needs have to have the discipline to install this new software in time. If a party fails to apply these patches, an attacker can exploit this (temporary) vulnerability. Most attacks also involve a human component. The victim opens an attachment or clicks on a link. This is what is understood by the second bullet point. For the third and final step - utilising the breach - administrators are a favourite target. After all, administrators have the access rights to intervene everywhere in the system, and deep in the system. Whether the

[344] Kill Chain, 2017 Carnegie Mellon, retrieval date August 27 2021 https://fedvte.usalearning.gov/courses/RCA/course/videos/pdf/FIM_D03_S04_T01_STEP.pdf

[345] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, retrieval date August 31, 2021

attacker wants to install ransomware or steal information, administrator accounts offer the attacker the most opportunities.[346]

Security management and preventing cybercrime.

It was argued in the previous section that an attacker takes advantage of human weakness or technical vulnerabilities: it would be logical for an organisation to strengthen or in any event secure these weak spots. It is also argued in this chapter that cybercrime is constantly developing and innovating; it is therefore not enough to just take security measures as a one off. If an organisation wants to stand up to cybercrime, it must take a structural approach to information security. Not only must it devote sufficient attention to all the security topics; it must also systematically maintain the security measures. This is actually what an Information Security Management System is focused on. It should come as no surprise, therefore, that the importance of information security is increasingly being felt. Since June 2020, for instance, the Dutch government has been required to observe the Governmental Information Security Baseline, BIO.[347] This is a government-specific version of the familiar (to information security experts) ISO27001 standard. Awareness is fortunately starting to grow among smaller and non-government parties as well. Various companies provide services in the information security domain. These companies range from large accounting firms, security testing specialists to information security services. The consumer has not been forgotten either. Alert Online is a cooperation of several ministries. Every year they promote security awareness in society. Another interesting platform, accessible free of charge, is the centre for information security and privacy.

Setting up an ISMS is a large and wide-ranging topic. For most organisations, it will not be possible to introduce all the measures in one go. The solution is for the organisation to prepare itself for the risks to which it is exposed. The organisation must ask itself what resources it wants to protect. Some

[346] A very readable illustration of this working method can be found in the report on the hack at Maastricht University. Maastricht University has been very open about its experiences. https://www.security.nl/posting/642572/Fox-IT+rapport+Maastricht, retrieval date August 30, 2021

[347] The BIO can be found in several places, such as https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/, Retrieval date August 28, 2021 or https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor-informatieveiligheid/baseline-informatiebeveiliging-overheid/

companies want to protect their client list above all else, while others might have intellectual property that gives them a competitive edge.

A possibly overlooked consideration is the choice of provider. In theory, every service that is provided offers the attacker a new entryway; a professional provider will therefore endeavour to provide a secure and predictable service. The customer will have to look into whether the provider takes adequate security measures.

Following on from this, the organisation will have to ask itself what points it wants to improve first. Does it want to improve employee security consciousness or are technical improvements needed first? It is precisely for these questions that it can be worthwhile bringing in a specialist.

Conclusion

This chapter looks back on a half century of cybercrime. A period during which attackers learned from each other and became increasingly bold. What once started as intellectual pranks has thus become a serious threat to everyone who uses or manages information. Fortunately, knowledge about attacks and how to defend against them is being shared more often and more easily. A number of reliable parties share information on cybercrime and information security.

The author believes this look back can also be a tool when going about setting up good information security. To paraphrase a famous military philosopher, a good defence starts with knowing your enemy.[348] The full quote is of course: ‘If you know the enemy and know yourself, you need not fear the result of a hundred battles.’ Translated to cybercrime, every organisation must ask itself these questions:

- What are my essential resources? What information sources or business assets do I want to protect and must I protect?
- How can I protect myself and against what attackers?
- Who can help me set up security or solve a cyber incident?

[348] Sun Tzu, ‘If you know the enemy and know yourself, you need not fear the result of a hundred battles’, https://www.gutenberg.org/files/132/132-h/132-h.htm, retrieval date October 22, 2021

23. Secure Software Development LifeCycle: find vulnerabilities earlier by empowering developers

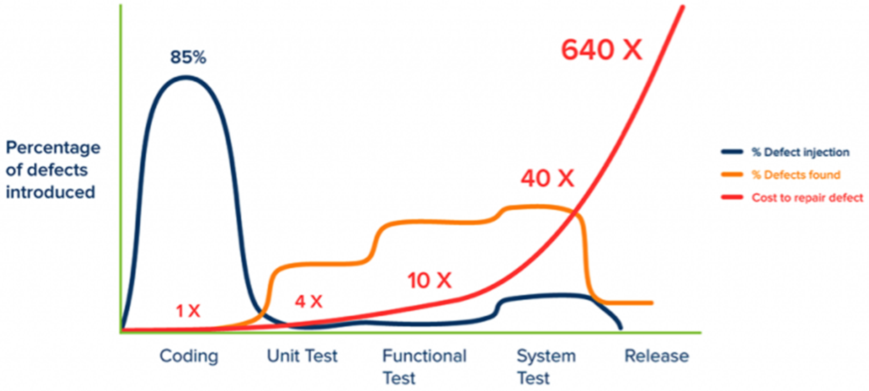
Davide Cioccia and Stefan Petrushevski

As a result of the digital revolution, almost every business runs on one and zeros. Developing software and hardware has become the central point for many organizations, whether they want to reach new customers, automate their processes, or create new businesses or simply put to stay relevant and grow as a business. This digitalization also brought cybersecurity as a factor in our world. Every software and hardware are prone to errors and mistakes which lead to weaknesses and vulnerabilities. As a consequence, everyday new vulnerabilities and exploits are disclosed online on publicly accessible websites. These vulnerabilities directly expose the components on which the business runs to cyber-attacks, may that be new and old applications, websites, Software as a Service (SaaS) platforms, Internet of Things (IoT) devices and any connected device.

Security by design

Software security has been a hot topic for many years now, so, why are we still experiencing data breaches? Security is not something we can plug and play, easily buy or install as an add-on, but rather a mix of three very important pieces: people, process, and technology. How security is perceived, can vary based on the risk appetite of the company and the criticality of their applications. In practice this is manifested in different forms, for example, companies can go from yearly compliance penetration tests to a well-established secure development process, secure pipelines, skilled security teams and well-implemented security by design in their product lifecycle.

Security by design is a software and hardware development approach where security is embedded in different phases and steps throughout the Software Development Lifecycle (SDLC). This approach does not only help companies avoid the introduction of vulnerable code in production, but also save money, shifting the vulnerability detection phase as early as possible in the SDLC.



Jones, Capers. *Applied Software Measurement: Global Analysis of Productivity and Quality.*

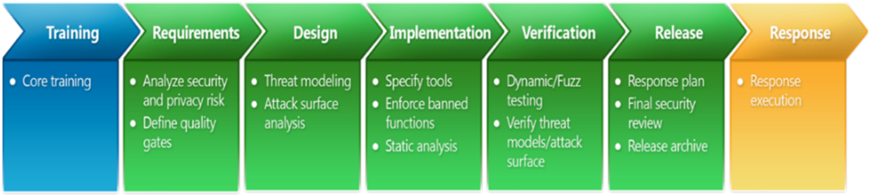
The graph from Capers Jones[349] shows the increasing cost of bugs and defects as they are introduced into the software at each phase of software development. Most defects are introduced during coding, due to misunderstood requirements, missing security requirements, but also when pieces are put together later on. Defects are mostly found during testing, but the price to fix them, exponentially increase the later the defects are found. “Shifting left” helps development teams to detect and avoid defects and vulnerabilities much earlier in the SDLC. That is the main reason why “shift left” has grown to become a mantra in the recent years of application security and software development.

SSDLC: A developer centric approach for security

Many companies think about security as another way of testing their products, using a traditional approach of security, performing penetration tests and vulnerability assessments just before the release date. Given the current state of software development that follows DevOps philosophy, this type of security is not able to keep up with constantly changing environments, fast-moving DevOps processes, practices, and tools or multi cloud instances or continuous delivery. This results in long waiting times (in the order of weeks) and limited coverage.

[349] https://www.stickyminds.com/article/shift-left-approach-software-testing

Implementing a developer-centric security program, allows engineers to introduce security even before writing the first line of code and get feedback about possible vulnerabilities as early as possible, to reduce overhead and create fixes with minimum effort (read, cost) and maximum benefits. More generally speaking, a secure SDLC (SSDLC) is set up by adding security-related steps to an existing development process. For example, applying security requirements alongside functional requirements, or performing architecture risk analyses and design reviews during the design phase of the SDLC.



There are many existing documents on secure software development practices, but a good starting point could be the NIST Secure Software Development Framework (SSDF)[350], that describes a subset of high-level practices based on established standards, guidance, and secure software development practice documents.

Security requirements, Design reviews and Threat models

When new features are defined and worked out in use case diagram by developers, reviewing security requirements, and identifying potential risks within the design, prior to coding is a critical step for preventing vulnerability to end up in the codebase. Activities such as Architecture Reviews and Threat Modelling can help developers avoid design mistakes that will later result too complex to fix.

Security requirements are as important as functional requirements and can be used to drive the implementation to better quality software. Developers could leverage the power of tools such as OWASP Security Knowledge Framework (SKF)[351] that provides security requirements from the OWASP Application Security Verification Standard (ASVS)[352] and Mobile Application Verification Standard (MASVS)[353] standards, based on the functional requirements selected by the

[350] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf

[351] https://www.securityknowledgeframework.org/

[352] https://owasp.org/www-project-application-security-verification-standard/

[353] https://github.com/OWASP/owasp-masvs

developers. Vulnerable and safe code examples are also provided by the platform to educate software developers how to create secure applications and enhance developers' coding skills.

Threat modelling is the process of identifying possible threats actors, threats, and vulnerable components in the design, analyzing the business logic and data-flow diagrams and overall documentation that explains how the data flow through the code. Two most famous examples of few Threat Model Frameworks are:

- STRIDE[354] provided by Microsoft[355], that focuses mostly on the type of threats, or
- DREAD[356], more focused on the impact of a possible threat.

Once the threats have been identified it is possible to identify mitigations, if present or not yet in place, that will be translated in security controls.

Tooling and early feedback: the art of scanning

To make sure that no vulnerabilities are overlooked during and after coding and stop them for being introduced into production releases, developers need to use the support of different type of tools, categorized as the following:

- **SAST:** Static Analysis Security Testing
- **DAST:** Dynamic Analysis Security Testing
- **IAST:** Interactive Analysis Security Testing
- **SCA:** Software Component Analysis
- **Secret scanning**: scan for secrets in repositories

SAST tools scan the application code base using different methodologies and security rules, to identify possible coding issues and vulnerabilities, and providing technical details on the applicable remediations. While SAST tools do a great job for well know issues (mostly injections and information disclosure), they also

[354] STRIDE stands for six threat categories: Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service and Elevation of privileges

[355] https://www.microsoft.com/security/blog/2007/09/11/stride-chart/

[356] DREAD stands for the five main categories into which the framework is broken: Damage, Reproducibility, Exploitability, Affected Users, and Discoverability

produce a lot of false positives and are not able to detect business logic issues, due to the lack of context. This type of activity is also known as Whitebox testing.

DAST is a different type of testing, also known as Blackbox testing, where a scanner is launched against a running instance of an application to detect possible vulnerabilities. The idea is to test the application against malicious payloads and monitor its behavior. When vulnerable patterns are identified, an alert is raised. Due to the lack of context and source code, this type of testing can generate false positives and low code coverage.

IAST is what bridges the gap between SAST and DAST and gives high confidence results. IAST makes use of the power of instrumentation, by deploying agents and sensors that run alongside with the applications, granting very little false positives and high-quality results. Because IAST is not scanning the codebase, to achieve high coverage, it must be supported by a wide set of tests. This usually is combination of manual and automated interactions with the application. That's why frequently IAST is also run in combination with DAST.

SCA is an automated scanning process that analyses the open source (OSS) components and frameworks in the solution.

The SCA tooling detects the open-source components and identifies the security vulnerabilities that are associated with them. This process can only identify known and (publicly) disclosed vulnerabilities. SCA also helps to avoid and/or resolve possible license violations.

SCA is mostly used in early phases of development. Companies can leverage the SCA results to enforce their Free and open-source software (FOSS) policies.

The manual touch: Penetration Testing

Penetration testing involves automated and manual tests that aim to test the security controls of running applications, usually in production environment for compliance purposes. Tests can be performed in pre-production environment as well for high risks application. We recommend white box pentesting methodology to achieve best results and the optimal coverage in the given limited timebox. While a pentest gives a very good idea of what an external actors could do, it's also the most time-consuming process. Making sure that the right time is allocated to have the right coverage is key. Skilled pentesters, can uncover critical vulnerabilities that less skilled ones cannot identify, that's why is very important to recruit the right partners and allocate the right resources, in terms of time and skills. Results must be recorded, and follow-up actions defined, to make sure that the same mistakes do not happen again.

Conclusion

- Getting security input at the commit or pull request level allows developers to have the information they need to fix security issues while they're still working on the code of the next release. Having early feedback centralized in one place, means that developers can interact with security teams as soon as the detection is performed, and implement security related changes in the code based on the security guidelines defined in the process.
- Aligning development and security teams is crucial to make sure that uncertainty does not lead to critical issues in critical systems, like Industrial Internet of Thigs (IoT) or Automotive, with the risk of putting in danger human lives.
- People, process, and technology must work together for a brighter and safer future.

24. Digital Security in Zimbabwe

Givemore Dube

Secure digital transformation is a boon for any developing economy, Zimbabwe included. The country has made digital advancements over the years. This has come, to a lesser extent, as a result of a policy driven digital program and to a greater extent as a means of survival and adaptations by the population in response to their day to challenges and the corona virus pandemic limitations. The transformations have not been complimented by a purposeful security and privacy program to safeguard sensitive and critical information assets and infrastructure. Digital security risks have not been adequately addressed and the country and its citizens, both natural persons and corporates, remain exposed. Securing identities, assets and technology in the online and mobile world remain unresolved.

Basic demography and key statistics

Zimbabwe is a land locked country with a population of 13,5 million living on land area of three hundred and ninety thousand eight hundred (390 800) square kilometers. It is bordered on the South by the Republic of South Africa, on the east by Mozambique; on the north by Zambia and on the west by Botswana. Below are key extracts from Zimbabwe National Statistical Agency (ZIMSTAT) Inter-censal Demographic Survey 2017 Report.[357]

- The female gender constitutes 52% of the population
- 40 percent of the population is below 15 years and 6 percent being 65 years and above.
- It has a literacy rate of 94 percent and life expectancy of 60 years (digital and digital security literacy rates still to be determined).
- 68 percent of the population live in rural areas (mainly communal lands and resettlement).

[357] https://www.zimstat.co.zw/wp-content/uploads/publications/Population/population/ICDS_2017.pdf

- 22.9 percent of the economical active population is formally employed, 6.6 percent is unemployed, and 70.5 percent informally employed.

The high literacy rate is a potential key enabler for a possible digital security awareness and training program. The high informal sector participation by the population points to the need for secure digital inclusion programs. The statistics also show the potential reach of digital attacks and the affected demography, that is, rural communities and informal sectors. These make up the majority of small to medium scale enterprises and constitute a large part of the attack surface. The economic and social impact can also be visualized from the above numbers.

Key features of the country's key digital infrastructure presented by the Postal and Telecommunications Regulatory Authority (POTRAZ) in its Abridged Postal & Telecommunications Sector Performance Report for 2021 first quarter[358] are as follows:

- 249489 active fixed telephone lines, representing a tele density of 1.7%.
- Three (3) mobile service providers (Econet with an 8.7m user base, NetOne 3.7m, Telecel 0,6m)
- Four cable service providers providing international internet bandwidth (Liquid 260000Mbps, TelOne 87500mbps, Powertel 5000Mbps and Dandemutande 3416Mbps)
- 13 million active mobile subscribers – mobile penetration rate of 87,8%
- Internet penetration of rate of 61,1% – 9029644 Internet and data subscriptions
- Declining fixed telephone voice traffic and increasing mobile voice traffic
- Increasing mobile Internet and data traffic – 21865TB
- Used international incoming bandwidth – 159665Mbps

The above, POTRAZ's, statistics point to pervasive use of digital technology and hence the need for digital security. Marrying these to the ZIMSTAT data we can see that the lack of digital security can have a destabilizing effect on both rural and urban populations, as well as digital inclusion social and economic programs.

[358] https://www.techzim.co.zw/wp-content/uploads/2021/07/Abridged-Sector-Performance-report-1st-Q-2021.pdf

The state of digital transformation and digital security

Zimbabwe enacted the Zimbabwe National Policy for Information and Communication Technology (ICT) in 2005 to guide the digital revolution.[359] This was reviewed and revised in 2012 and 2016 leading to the second and third policies respectively. The third was due for revision in 2020.

The coverage of digital security by the Policy has been quite limited. Focus has only been on the enactment of the necessary cyber laws and legislative provisions relating to intellectual property rights, data protection and security, freedom of access to information, computer related and cybercrime laws. That is, adopt data protection and privacy, intellectual property protection and copyright, consumer protection and child online protection. The laws and legal provisions, however, have remained in the pipeline.

The Smart Zimbabwe 2030 strategy that is also meant to help guide the digital transformation of the country does not sufficiently cover the digital security risks that the country and its citizens are facing and will face in magnified proportion if the country were to turn "smart".

The government purposefully introduced the schools computerization program (SCP) and introduced an education curriculum which presented ICT as a subject right from infant school level.[360] At tertiary level there has been an increase in ICT courses, from national certificate to PHD level. However, the curriculum does not include complimentary digital security content. Digital and/or cybersecurity are not examinable subjects at grade seven, ordinary level or advanced administer by Zimbabwe School Examination Council (ZIMSEC), but ICT and computer science/studies are courses at Higher Education Examinations Council (HEXCO) national foundation certificate, national certificate, national diploma or higher national diploma, but they have computer studies

Cyber security degree programs

Out of the sixteen (16) government university only two (2) have digital and cyber security degree programs. This is despite all of them having either computer science, information technology, informatics, software engineering or information

[359] https://en.unesco.org/creativity/sites/creativity/files/qpr/zimbabwe_national_policy_for_ict_2016_-_final_1.pdf

[360] https://docs.edtechhub.org/lib/G4UUX5P3/download/DQVKPKSZ/EdTech%20in%20Zimbabwe_%20A%20rapid%20scan%20%28DOI_%2010.5281_zenodo.3903838%29%20.pdf

systems degree programs. Private universities have a similar challenge. Individual persons are either enrolling for online or distance programs offered by university outside Zimbabwe. Some privately study cybersecurity certification courses offered by international bodies such as ISACA, ISC^2, Offensive Security, EC-Council, CSA, SANS, CompTIA and vendors such as CISCO, Huawei, Checkpoint Sophos, Microsoft, Google and Amazon. Private colleges are offering tuition for a limited number of these courses. The Computer Society of Zimbabwe supported ICDL is also pushing its IT Security offering in addition to its tradition ICT courses.[361]

E-Government

Zimbabwe has been working on a national electronic government (e-government) programme which aims to introduce several e-services to the population and stakeholders.[362] This involves sharing information and data between government actors, that is, government to government (G2G), between government and business (G2B) and government to citizens (G2C). In the e-government space all actors will have digital personas (identities) and data is transferred between the identities, ideally security. Without a digital and cybersecurity framework, e-government cannot be sustainably realized. Confidentiality, availability and integrity of the data, communication, the services and the actors cannot be guaranteed. The safety of the identities (identity protection and management) is paramount for e-government to work, a proposition that is untenable without a robust digital security program in place.

Payment transactions

In the payment space mobile money, various bank and store cards are used in addition to online, Internet, social banking applications to drive digital transactions. The regulator, the Reserve Bank of Zimbabwe, has put in place measures to regulate this space including the implementation of a national payment gateway, anti-money laundering (AML) regulations and making the Society for Worldwide Interbank Financial Telecommunications (SWIFT) Customer Security Programme (CSP) assessment a mandatory requirement for financial institutions.[363] However, these measures have not sufficiently counteracted the various digital security hazards.

[361] https://icdlafrica.org/workforce/cyber-security/

[362] https://publicadministration.un.org/egovkb/Portals/egovkb/MSQ/Zimbabwe_28012021_125758.pdf

[363] https://www.rbz.co.zw/documents/mps/mpsfeb2019.pdf

COVID-19

In addition to the above, the Covid 19 pandemic accelerated the digital transformation, mostly in in an uncontrolled manner. The lockdowns and closure of non-essential services led to the proliferation of digital services:

- Online digital newspapers
- Electronic commerce
- Online shops
- Online education
- Online and social banking
- Work from home facilities
- Remote access-based service support
- Financial payment systems

Digital security and privacy challenges

The local digital space has remained largely insecure, there has been no deliberate investment at national level to complement the levels of digital transformation. The country has seen an upsurge in:

- Online bullying
- Intellectual property theft and counterfeiting
- Illicit online content and fake news
- Misuse of mobile money payment platforms
- Financial crimes (card cloning, fraud)
- Identity theft
- Ransomware and other malware attacks

Legal and regulatory framework

The Legal and regulatory framework has remained largely inadequate to ensure and assure digital security. The Data Protection and Privacy and Electronic Transactions and Electronic Commerce bills are still to be gazetted into law. The National Policy for Information and Communication Technology remains out of date and the country does not have a Digital Security Strategy and/or Policy. It lacks a coherent digital and cyber security framework. Governance, operational and other supportive structures to drive and ensure digital security risk management are none existent. It is not clear who is accountable and responsible for digital and cyber security. A clear definition and protection requirements for critical sectors and assets (aspects that have a bearing on digital security) have not been defined as is the case in other jurisdictions. For example, the United States defined its 16 critical infrastructure sectors that include commercial facilities, communications, healthcare and public health, information technology, food and agriculture.

Education and awareness

Digital and cyber security education and awareness has not been purposefully driven and thus knowledge in the space has remained depressed. The human factor remains the weakest security link due to knowledge incapacitation. The country has seen an increase in digital and cyber crime where the victims include the disadvantaged members of the community (rural poor, elderly, women and children). Digital insecurity has thus affected the economic wellbeing of marginalized members of society.

Personal identifiable information (PII), personal payment information (PPI) and protected health information (PHI) has not been and is not being safeguarded to the levels that are demanded globally due to lack of legal, regulatory and compliance standards and requisite knowledge and skill. There is no reciprocal local law to extraterritorial laws from other jurisdiction, such as the European Union's General Data Protection Regulation (GDPR), California Consumer Protection Act (CCPA) and the Health Information Portability and Accountability Act (HIPAA). The digital space being hyper-connected and transcending many borders including political and jurisdiction, it is imperative that digital security for any nation must be a reasonable fit to the global security puzzle.

Conclusions

To foster trust in the digital space and optimize the opportunities arising from digital transformation, it is imperative that the country manages the digital security risk. Though the digital horse has already bolted out of the stable, Zimbabwe is still early on its digital transformation journey and can take measures to bake in digital security. It can avoid some of the pitfalls of bolting on security as it can learn from other countries in structuring its digital security program.

Improvement recommendations

The following may form the basis of the journey:

- Establishment of digital security governance, management, operational and policing structures
- Establishment of a responsive legal and regulatory framework
- Defining critical sectors, processes and assets
- Digital security risk management capacity building
- Building trust-based partnerships with other digital ecosystem players
- Integrating into regional and international digital security programs and enhance international cooperation.
- Drive digital security research and innovation

25. Experiences from a ransomware attack

Michiel Borgers

Being held digitally 'hostage' or 'for ransom' is a nightmare. Not only for the CIO, but for the entire organisation. After all, no organisation can function without the availability of IT because virtually all business operations today are fully or partially digitally supported: email, finance, planning, logistics, the coffee machine, doors and entry barriers, laboratories, communications, and much more.

Getting an organisation back up and running after it has fallen victim to hostageware takes a great deal of time, effort and money; even aside from the question of whether ransom is paid to unlock the systems. A ransomware attack is no exception, given the many reports in the news. Since cyber attacks are constantly increasing - worldwide - the likelihood of an attack is high. According to the NCTV's cybersecurity assessment,[364] the digital threat continues to grow. Only the implementation of more security measures and more cooperation will ultimately mitigate the effects of these digital threats. A number of personal experiences from the ransomware attack at Maastricht University on 23 December 2019.

The attack

23 December 2019 - 6.55 pm, 267 servers are encrypted. As CIO, you are informed that not a single employee of Maastricht University can access his or her own systems. Around 11.45 pm, the first ransomware note is found (see Illustration 1) and the cause is definitively known: a ransomware attack. How the attackers

[364] Cyber Security Assessment Netherlands 2021 – NCTV, https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021 June 2021.

prepared and carried out the ransomware attack is described in detail in the Fox-IT report and Maastricht University's response to that.[365]

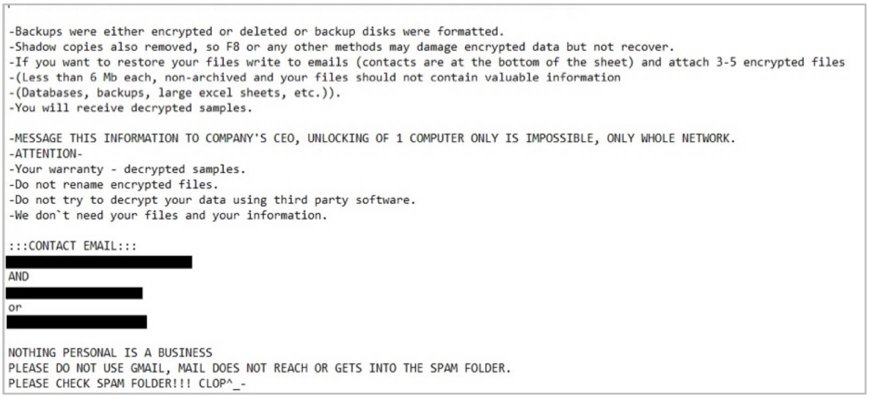
In this case, there are a number of facts that are interesting for improving cybersecurity. Firstly, the initial compromise occurred via a phishing email (see Illustration 2). This should come as no surprise because we know that even at an organisation that is aware of phishing emails, at least 20% of employees still click on a link in the phishing email.[366] In this case, it was interesting that multiple identical phishing emails were sent, the only difference being the link, which differed by only a single character from each other link. So it is always important to check that you have cut off all the bad links.

The time between the initial compromise and the actual activation of the ransomware was also more than two months. This means that there is time to act after a criminal has gained access to the technical infrastructure. For the rest, this time frame could be shorter, as emerged in the case involving University of Amsterdam and the Amsterdam University of Applied Sciences.[367] In that period, too, there were a number of signals indicating that something peculiar might have been going on. There was an antivirus report, for instance, and somewhat later an antivirus program was also deactivated (see Illustration 3). These signs must be responded to vigilantly because criminals also cover their tracks as quickly as possible.

[365] Urgent support project Fontana – Fox-IT, version 3.0 - 5 February 2020 and Response from Maastricht University to the FOX-IT report - 5 February 2020. Https://www.maastrichtuniversity.nl/nl/updates-cyberaanval

[366] https://itdaily.be/nieuws/security/20-procent-werknemers-klikt-op-phishing-mails/

[367] 'Attack repelled' - Learning evaluation of the cyber attack on University of Amsterdam and the Amsterdam University of Applied Sciences, 6 July 2021. https://www.uva.nl/content/nieuws/nieuwsberichten/2021/07/evaluatie-cyberaanval.html?cb



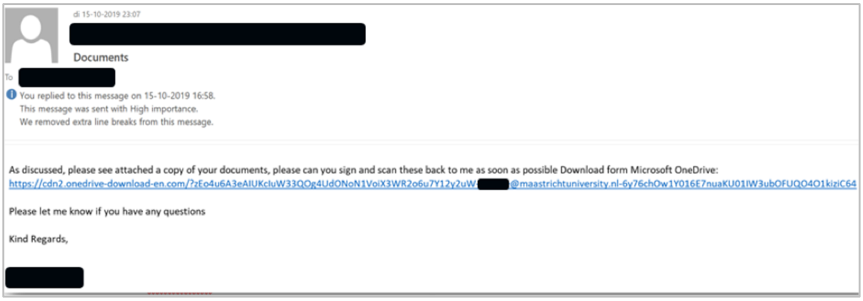
```
-Backups were either encrypted or deleted or backup disks were formatted.
-Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
-If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 3-5 encrypted files
-(Less than 6 Mb each, non-archived and your files should not contain valuable information
-(Databases, backups, large excel sheets, etc.)).
-You will receive decrypted samples.

-MESSAGE THIS INFORMATION TO COMPANY'S CEO, UNLOCKING OF 1 COMPUTER ONLY IS IMPOSSIBLE, ONLY WHOLE NETWORK.
-ATTENTION-
-Your warranty - decrypted samples.
-Do not rename encrypted files.
-Do not try to decrypt your data using third party software.
-We don`t need your files and your information.

:::CONTACT EMAIL:::
[redacted]
AND
[redacted]
or
[redacted]

NOTHING PERSONAL IS A BUSINESS
PLEASE DO NOT USE GMAIL, MAIL DOES NOT REACH OR GETS INTO THE SPAM FOLDER.
PLEASE CHECK SPAM FOLDER!!! CLOP^_-
```

Illustration 1: Ransomware note found on the servers



di 15-10-2019 23:07

[redacted]

Documents

To [redacted]

You replied to this message on 15-10-2019 16:58.
This message was sent with High importance.
We removed extra line breaks from this message.

As discussed, please see attached a copy of your documents, please can you sign and scan these back to me as soon as possible Download form Microsoft OneDrive:
https://cdn2.onedrive-download-en.com/?zEo4u6A3eAIUKcIuW33QOg4UdONoN1VoiX3WR2o6u7Y12y2uW[redacted]@maastrichtuniversity.nl-6y76chOw1Y016E7nuaKU01IW3ubOFUQO4O1kiziC64

Please let me know if you have any questions

Kind Regards,

[redacted]

Illustration 2: the phishing email with the link to the ransomware software

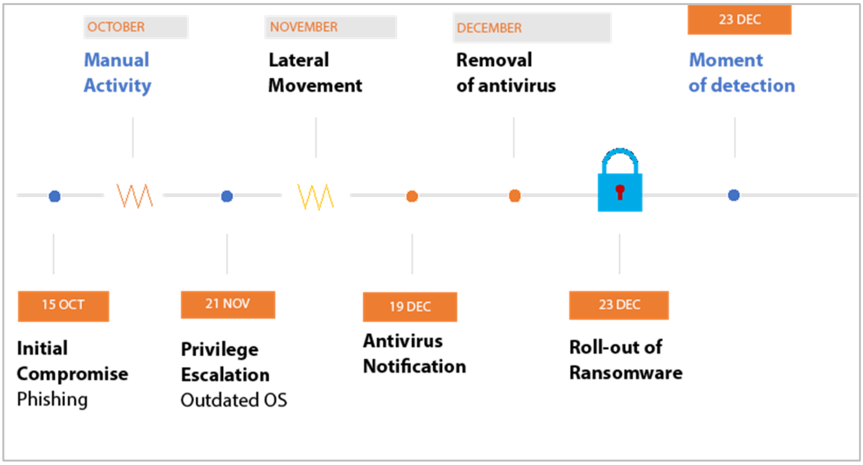


Illustration 3: Timeline of the ransomware attack

The recovery

After it became known that Maastricht University had been ransomed, a start could be made on fixing the problem and restoring service. All of this is also described in the various reports, such as the report entitled 'Cyber attack on Maastricht University' from the Education Inspectorate.[368] It is interesting to look at several topics in more detail, without being able to discuss all the necessary steps exhaustively (see Illustration 4).

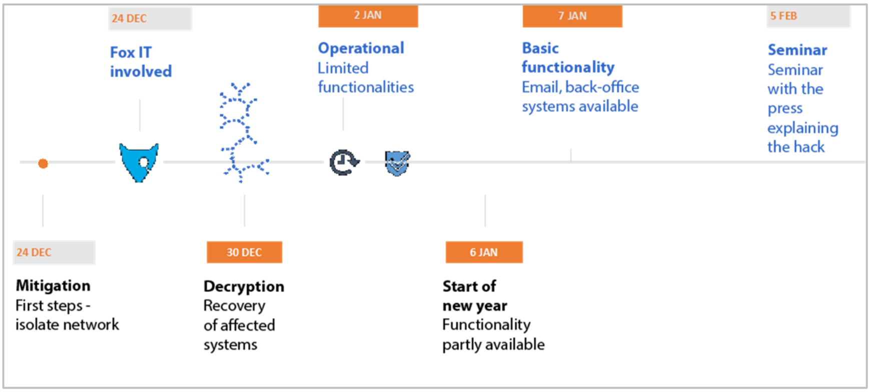

24 DEC
Fox IT involved
2 JAN
Operational
Limited functionalities
7 JAN
Basic functionality
Email, back-office systems available
5 FEB
Seminar
Seminar with the press explaining the hack
24 DEC
Mitigation
First steps - isolate network
30 DEC
Decryption
Recovery of affected systems
6 JAN
Start of new year
Functionality partly available

Illustration 4: Timeline of the recovery

The first step is isolating the network by making both inbound and outbound traffic impossible. This is to prevent criminals from still being able to get into the systems from outside and possibly taking data from the network. The tendency is to switch off servers that are infected with ransomware or other malware. Switching off a server could possibly destroy forensic data still contained in the server's (dynamic) memory, however. These forensic data can be useful for the recovery of the technical infrastructure and later in a possible criminal investigation. It is important not to cut off power to the servers, therefore, but to disconnect the server from the network. In other words, disconnect the system from both the internet and from the internal network.

Quickly sharing the 'indicators of compromise' meant that two other universities were able to prevent the same ransomware attack. The experiences

[368] CYBER ATTACK AT MAASTRICHT UNIVERSITY (BRIN: 21PJ), Education Inspectorate, Ministry of Education, Culture & Science, Utrecht, May 2020. https://www.onderwijsinspectie.nl/documenten/rapporten/2020/06/12/rapport-cyberaanval-universiteit-maastricht

from the ransomware attack also proved useful later on in preventing the attack on the shared infrastructure of University of Amsterdam and the Amsterdam University of Applied Sciences. This demonstrated that sharing knowledge about cyber attacks is important to prevent damage at other parties and it is urgently advised that a cyber attack be reported to a limited group of (trusted) authorities, which can often be done anonymously at first.

For the recovery of your technical infrastructure, it is important to identify your most precious assets. What processes, systems and data are crucial for the functioning of the organisation and in what order must the systems be made available again. At a university, but certainly also at other types of organisation, that may differ depending on the time of year. During the academic year, the systems for delivering education will be crucial, while during examination periods, the examination material and testing software will have the highest priority.

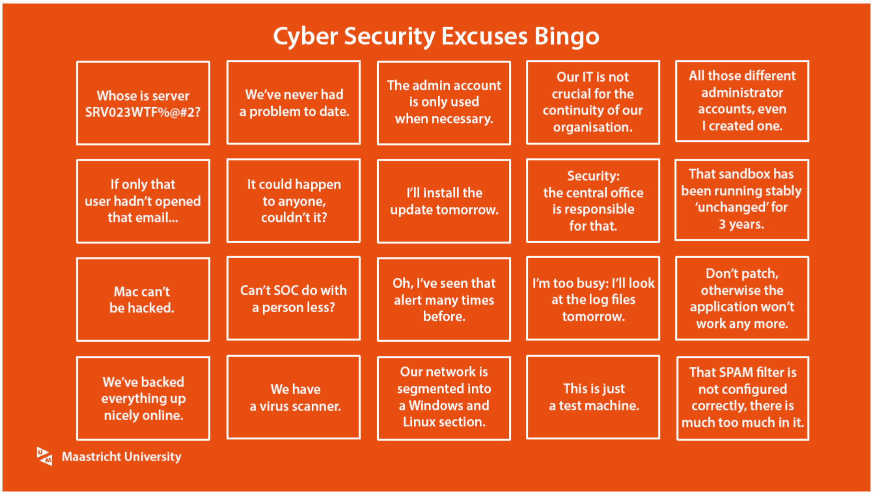
When determining the recovery scenarios, the question will also arise of whether the organisation should pay the criminals the ransom in order to get the decryption key. In principle, one should never pay criminals because this rewards the criminals for their methods and perpetuates this form of crime. Ultimately, the ethical, financial, technical and operational aspects must all be weighed to determine an answer. It is a balancing act between a societal issue and an issue of commercial continuity.

As in every crisis, communication is essential. Added to this is the fact that in many cases, internal communication also means external communication. This sometimes makes it difficult to make announcements that are only relevant for internal employees, for instance. In any event, take the lead as organisation in the crisis communication and stick to the facts. In the Maastricht case, a conscious choice was made to only answer many of the substantive questions at the end, once all the facts were clear. This approach was also communicated clearly.

Analysis of the dangers - Bingo card

Like with so many dangers, people have a tendency to think 'it won't happen to me'. Following on the ransomware attack at Maastricht University, an overview was made of statements made at various organisations which could potentially imply a security risk. These have been put together in a so-called 'Cybersecurity Excuses Bingo' (see illustration 5). It is contended that at every organisation, at least one, but probably more, of these statements are made at some point or other.

Looking at the bingo card, it is striking that while a number of statements are technically oriented, there are certainly organisational security issues that need fixing as well. In any event, it makes it visible that there is a potential security risk present. The bingo card also highlights that awareness among managers and among IT employees has still not reached the desired level.



Cyber Security Excuses Bingo

Whose is server SRV023WTF%@#2?	We've never had a problem to date.	The admin account is only used when necessary.	Our IT is not crucial for the continuity of our organisation.	All those different administrator accounts, even I created one.
If only that user hadn't opened that email...	It could happen to anyone, couldn't it?	I'll install the update tomorrow.	Security: the central office is responsible for that.	That sandbox has been running stably 'unchanged' for 3 years.
Mac can't be hacked.	Can't SOC do with a person less?	Oh, I've seen that alert many times before.	I'm too busy: I'll look at the log files tomorrow.	Don't patch, otherwise the application won't work any more.
We've backed everything up nicely online.	We have a virus scanner.	Our network is segmented into a Windows and Linux section.	This is just a test machine.	That SPAM filter is not configured correctly, there is much too much in it.

Maastricht University

Illustration 5: Cybersecurity Excuses Bingo card

The experiences

The experiences of a ransomware attack victim can be used by others to prevent attacks or limit the damage they cause. We identify five important lessons here that can be drawn from this case.

1. IT is core business, and that means that without IT, the entire organisation no longer functions. That is true, in principle, for every type of organisation in the Netherlands. Because of this, the impact of a ransomware attack is, by definition, great and this impact must be kept as small as possible. As such, this makes it a topic that belongs at the boardroom table.
2. In every organisation, there are employees who will click on phishing emails and not all these phishing emails will be reported to or detected by the IT organisation. This means that every organisation will be hacked, sooner or later. It is therefore important to detect that hacker by constantly monitoring the technical infrastructure for suspicious signals (*Indicators of Compromise*). All sorts of measures are also possible, such as segmenting the network, keeping offline back-ups, and updating the software and curtailing

administrator rights, which ensure that a malicious actor can only cause limited damage, if any, to the core of the technical infrastructure.

3. An important lesson can also be drawn in relation to back-up facilities. *Online* back-up systems are effective and inexpensive: online back-up systems allow you to restore a back-up quickly and they are less labour-intensive and therefore cheaper than *offline* back-up systems. Cybercriminals are precisely on the lookout for back-up systems, however, because holding those systems hostage ensures that recovery after a ransomware attack becomes even more difficult. That is why an offline back-up system is nonetheless strongly recommended, possibly alongside an online back-up system.
4. Awareness of cyber threats and security will have to be at an adequate level among everyone in the organisation, not only in terms of knowledge, but particularly in terms of conscious behaviour. The Bingo card shows that there are many excuses for putting security on a back burner. And the fact that in organisations where people are indeed conscious of cybersecurity, they still respond to phishing emails in at least 20% of cases means that awareness on the part of the end user is important, but that awareness on the part of the IT employee and manager is even more important.
5. We will have to share 'Indicators of Compromise' with each other. This will enable us to prevent greater damage, as occurred in this case as well. We must share technical and process-related signals of a cyber attack with each other as widely as possible. No distinction should be made in this respect between private and public organisations. As organisations, we are so connected with each other that an attack on one organisation can easily have an impact on many others. This also became painfully obvious in the Maersk case.[369] And that also means that you as organisation must be open, at least to certain reliable parties, if you are hit by a ransomware attack. The fact that you have fallen victim to an attack is nothing to be ashamed of.

Points in conclusion

- Ransomware attacks are now of an international and geopolitical order. At President Biden's first meeting with President Putin, cybersecurity was

[369] Maersk, the shipping giant, has suffered millions of dollars in damage due to the NotPetya ransomware attack http://zd.net/2DV9fgP by @SecurityCharlie

therefore rightly included as one of the topics on the agenda.[370] In order to be able to conduct the political discussion properly, however, facts will have to be on the table. Commercial hackers are protected in a number of countries from which they operate, for instance.

- Both private and public organisations will have to be open about the fact that they have been hacked and must give full disclosure of the indicators of compromise.
- This means that both technical and process-related signals of a cyber attack must be shared as widely as possible.
- Sharing information can help prevent attacks at other organisations or limit the damage from such attacks.
- Only together are we safe.

[370] Putin meets Biden at 'low point in relationship', what can we expect? - https://nos.nl/artikel/2385223-poetin-ontmoet-biden-op-dieptepunt-in-relatie-wat-valt-er-te-verwachten

26. Real-time responsibility: from content to context

Vincent Hoek

Professor of political economics and founder of the World Economic Forum (WEF) Klaus Schwab is one of those who describe our social reality as the 'fourth industrial revolution'. It is a time in which the flood of cloud computing, real-time data systems and the Internet of Things is giving rise to autonomous cyber-physical production environments (IT-OT convergence), with new risks and responsibilities. Industrial revolutions have drastic effects on how societies are organised, how they prosper and how they wage war. Data relationships that reach beyond the organisation and beyond the jurisdiction have such an impact that the interpretation after the fact of implicit intentions by an accountant, lawyer or auditor no longer works in a world of real-time logic systems. Which is why a cyber-physical environment results in more than one reality, with all sorts of consequences for administrators, politicians and professionals.

Datafication as a trend

In a time of 'social engineering', 'whaling'[371] and 'deep fakes', how do we know who our organisation represents and with what authorities (entitlement)? What provider issues the means of identification and/or claims and how reliable are these? Is information accurate, not misused and current? How do you handle technology with unprecedented capabilities and how are mistakes fixed if your data have been in contact with them? How do you embed consequences if something goes wrong in an organisation that is intertwined with third and fourth-degree data producers? Difficult, for anyone still working with an application-centric, content-centric, organically grown IT landscape, intended for Humans, with their own jargon, perceptions, knowledge level, decision making and behaviour, who still input their data themselves and recall them again using the same software. *The so-called*

[371] Whaling: A whaling attack is a specific type of phishing attack that targets important officers, such as the CEO or CFO, with the goal of manipulation and data extraction.

'datafication' overturns all certainties. Networked data is shared more *between* organisations than *within* them. Formal communication under imposed standards loses out, as a result, to open, uninterrupted data exchange, which no longer focuses on what 'the Director' preordains, but on what the end-user needs at that moment.

Domain knowledge

The viability of datafied organisations depends on the use of adaptive, proactive data management, to be able to cooperate in a manageably flexible manner in varying contexts, thanks to seamless data delivery chains. Data delivery chains for which the Director is responsible, incidentally. 'My Mess for Less' outsourcing to a cloud service provider does not release someone from Accountability. Digital Security therefore requires up-to-date multidisciplinary knowledge of (software-defined) infrastructure and data platforms, of digital services and digital work spaces, of corporate culture, organisation and process models; *from (IT) governance[372] to resilience issues*.[373]

One must have knowledge of combinatory effects between portfolio elements, of legal aspects, such as compliance, privacy and liability, of sociological aspects (including work forms and collaborative patterns), of psychological aspects and the human dimension[374] (including ethical issues), of HRM (including digital literacy) and of economic and financial aspects, such as business cases.

Each one a topic that has unexpected data relationships with the others. *A cyber-physical environment also results in more than one reality* because more possibilities for inter-trans-action arise in Time and Space. So we have both the real time and real space, but also the virtual time and virtual space. In all sorts of combinations. A physical object can only be in one place at a time. A networked sensor can perform and recall a whole world of time and location-independent logical tasks.

[372] The overarching set of policy rules, procedures and relationships by which an organisation determines its objectives, sets its limits and monitors its deliverables so that they remain attuned to the needs and interests of its primary stakeholders.

[373] Resilience: being able to deal smoothly with (rapidly) changing (negative) circumstances.

[374] Direction and focus of the work context, in which activities have a reciprocal meaning, in the realisation of output valued by those involved.

From zoning to 'trust anchors'

A building is traditionally secured 'from the outside in' (in Dutch: the OBE concept)[375], whereby the 'interests to be secured' serve as the basis. In a datafied world, we have to determine whether and how we can even trust a virtual object at all.

Trust is a function of verifiability, so we must look for 'trust anchors'.

1. Legal trust anchors which determine the policy basis for the trust framework and support the operational rules. These operating rules and rule sets are standardised for use in organisations to support the common policy.
2. Data anchoring anchors, which relate to the entities and characteristics to be processed, whereby an extremely high data quality is of vital importance.
3. Cryptographic trust anchors, which form the roots of cryptographic trust and enable cryptographic connection, revocation, authentication, signing, coding and other trust functions.
4. Cybersecurity trust anchors, which monitor, detect and respond to policy breaches and compel compliance with the policy. This encompasses, inter alia, assurance, test and certification regimes.

The international standards ISO 29003 and ISO 29115 already provide much background for how Trust with Assurance can be derived in a virtual world. Data quality in conjunction with identity determination is described in ISO 8000:2019. Thus a new way of thinking is developing. From the traditional outside-in approach, which assumes threat mitigation with zoning and the integration of physical and logical control and delaying concepts, to concepts in which no human, machine, application, process or data set is trusted any longer without context. The difference between putting on armour and building up an immune system.

Information security

Along with digitalisation came digital information security: the security of information and information systems, including connection security, in all its facets. To this end, traditional risk management encompasses the systematic stocktaking, assessment and - by taking measures - management of risks with the help of guidelines, influencing behaviour and control measures, which are periodically audited. Datafication brings additional challenges in other reality domains.

[375] OBE: Organisational, Structural and Electronic Measures for Zoning.

Besides in the real time and in the physical space, we now also run risks in combinations of (virtual) time and (virtual) space, in which (legal) acts also take place. All the combinatory effects must be identified and disentangled. Every action must ultimately be able to have just one expected and desired output. Quite the task, but realisable with modern AI/ML techniques.

Software-driven infrastructure

By no longer seeing code as the basis for applications, but as a raw material for specific functions, the conditions under which code responds to convert triggers into actions and to merge actions into processes can be finetuned. By henceforth assigning identity to people, as well as machines, applications, processes and individual data sets, it becomes easier to stipulate stringent conditions for which data, under what conditions, can be transported and used, and along which routes. This could make it possible for a virtual system to only be started up if two biometrically identified people with the right 'credentials' have entered a physical space at the right time and in the right order. That already makes hacking a bit more difficult.

Advanced access control

Infrastructure as Code and Identity as Service continue to grow rapidly and have already resulted in concepts such as Zero Trust Architecture[376] and Secure Access Service Edge (SASE);[377] Sorely needed, because the business sector is starting to cooperate more and more (internationally) by exchanging data. Increasing compliance requirements complicate the organisation of liability and information protection across data delivery chains, however. An Airbus aircraft is finally possible thanks to thousands of cooperating, networked businesses, who work with self-employed individuals working from home and 3D printers. *Information security requires significantly better access control than many are accustomed to these days.*

[376] The zero trust model suggests that no single user, even if admitted to the network, must be trusted as standard because he or she can be compromised.

Identity and device verification are required throughout the network, not just at the perimeter.

[377] SASE is a network architecture that combines WAN possibilities with 'cloud-specific' security functions, such as secured web gateways, cloud-access security (for example, Federated Identity Access Management), firewalls and zero-trust network access.

Reliable

Access control requires identity, authentication and authorisation refinement as the basis for trust. Organising trust between multiple organisations requires federation (mutual cross confidence). Organisations must, in some way or other, be able to be deemed reliable in order to trust each other. To that end, they need a common business language to understand each other. Federation requires joint management and agreed shared policy. Federation standards usually build on national ID activities, such as the European eIDAS Regulation for the residents of the European Union.[378] Standardisation institutions also adopt ontological standards.[379] Business process modelling industries set up architectural standards, which make it precisely clear which trigger leads to which action; which actions together form which process, and what data must be transported to that and in what manner.

Conclusion

It is important to realise that Digital Security is no longer limited to data networks and infrastructure. It is a transparent game of 'assets' and 'resources' with a digital component within a notion of predictably reliable, trustworthy and resilient service provision. In order to arrive at *formalised insights*, a multidisciplinary approach is needed to realise sustainable security for dynamically connected ecosystems of (sub) organisations, with their own (sub) mandate, ICT (legacy) systems and corporate cultures, which play roles in the dynamic game from sensor interpretation to case management.

Considerations

- Digital security today goes beyond technology and networks. Psychology and behaviour also play a role. After all, society is made up of individuals, networks and communities, which are connected by ideology or association, spread across and informed - but no longer limited - by geography.

[378] The European Economic Area Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 is the most important legal instrument of the European Union that regulates trust in electronic transactions. eIDAS stands for 'Electronic Identification and Trust Services'.

[379] A structured data model with concepts and possible relationships between concepts that are current and important in a particular discipline or field (epistemology).

- This is where new vulnerabilities lie, where digital resources are used to circumvent conventional digital security defences. Digital security is still primarily seen as a vertical field; part of a functional hierarchy, with a calcified organisational, technical and market perspective, but that time has definitely passed.
- The coronavirus lockdowns forced the transition from *People-Based Processing* to *Straight-Through Processing*. From physical encounters to input data into systems, to working online, spanning time and place, to be able to enrich data in dynamic collaborations. Until recently, an organisation was our reference point for Trust, compliance and security. However, datafication makes false organisations (WHOIS - Domain Name Spoofing[380]) and bad data an enormous problem that pulls the rug out from under our societal trust.
- There is therefore a strong connection between trust anchors and distributed trust frameworks for identity management, at different levels of reliability. Reliability depends on legal conditions for the quality and reliability of the identity information and on the liability conditions of the issuing institution. The authoritative source / issuer will ultimately only be liable for trusting parties if all the policy requirements are satisfied. Including the way in which the trusting party complies verifiably with policy and system implementation requirements. The transparency requested and the requirements for data quality are in any event increasing, which makes digital security a function of data governance.
- The answer to the challenges lies in verification of every facet of our data landscape. We will have to get visual and audio of the value of data interactions between similarly and dissimilarly secured organisations. Whatever the picture is within Cybertech, InsurTech, RegTech and FinTech, where technological and legal developments reinforce each other in the new field of Legal Engineering.[381]

[380] A form of phishing in which an attacker appears to use a company’s domain to impersonate that company or one of its employees in order to commit fraud.

[381] The correlation of technology, law and data to be able to convert legal text into logical and traceable instructions for humans and machines, whereby interpretable decisions can be taken across organisational boundaries.

27. Underappreciated issues in advanced security policy

Victor de Pous

No organisation can avoid setting up, implementing and monitoring an up-to-date digital security policy, including disaster response. In larger organisations, a Chief Information Security Officer (CISO) will be responsible for this, who must also work with lawyers. They consolidate statutory regulations, translate these to practice *and* stay up to date on the legal developments. It is a strikingly dynamic and broad legal domain. The EU is working on a significant expansion of the Network and Information Security Directive, while the Netherlands currently wants to amend the cybersecurity act based thereon (Wbni) to establish a basis to provide *all* companies with threat and incident information. The endless series of incidents can also give rise to important points of reference for policy. While some are well enough known - such as measures for offline back-up and archiving, or a 'digital security law due diligence' in the event of an acquisition - it emerges that organisations are still falling short. Not to mention somewhat neglected breaches. Not all companies and government organisations have a security policy for email and domain names that have fallen into disuse.

Mergers & Acquisitions

On 30 October 2020, the British privacy regulator Information Commissioner's Office (ICO) fined hotel chain Marriott International 18.4 million pounds.[382] Investigation by the ICO had indicated that errors had been made in taking appropriate technical and organisational measures to protect personal data against breaches, as prescribed by the European General Data Protection Regulation (GDPR). Marriott estimated that 339 million guest files worldwide were leaked after

[382] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/ The original fine was 99 million pounds, in fact, but was reduced because of the financial effects of the COVID-19 pandemic for the hospitality and travel sector.

a 2014 cyber attack on Starwood Hotels and Resorts Worldwide. Marriott International acquired this competitor in 2016. The attack remained unnoticed until September 2018, however. Malicious actors may have had unauthorised access to the information systems for four years.

N.B: the fine only pertains to the breach from *25 May 2018* onwards, the date that the GDPR was declared applicable. Because the security breach occurred prior to Brexit, the ICO investigated the breach as leading supervisory authority on behalf of all the EU authorities. The case shows in passing that a digital security incident is not necessarily a closed case once the administrative fine is imposed. After all, data subjects whose privacy has been violated are free to go to court to demand damages. The hotel chain is now facing a number of class actions, in both the United Kingdom[383] and the US.[384]

In the event of an acquisition, joint venture or other significant financial transaction, pointing out the need for thorough digital law due diligence - explicitly including security law aspects - is akin to stating the obvious. After all, in cases that arise, it has long since ceased to be exclusively about traditional financial audits, now that ICT has become conditional for every company. The buying or investing party cannot avoid conducting technical *and* legal assessments, therefore. On a related note: if you look back, you will see that since the 1980s there have been regular calls in the Netherlands for a - statutory - independent statement on ICT, to be drawn up first of all by the registered accountant (RA). In 1982, for instance, NIVRA director at the time H. Volten argued that its specialised members should have a role as guardian.[385] After that, the registered IT professional(RI – 'Register Informtacus') entered the picture and recently, possibly again, the (registered) IT Auditor (RE – Register EDP Auditor).[386]

Back-up and archiving

How wrong things can go when it comes to the security of offline media is clear from the case of the organ donor register in the Netherlands. 'In the digitalisation

[383] https://techcrunch.com/2020/08/19/uk-class-action-style-claim-filed-over-marriott-data-breach/?guccounter=1

[384] https://topclassactions.com/lawsuit-settlements/data-breach/marriott-data-breach-class-action-allowed-to-proceed/

[385] Dagblad Trouw, 19 June 1982.

[386] https://www.accountant.nl/nieuws/2021/8/norea-pleit-voor-invoer-it-auditverklaring/. Also see chapter 21: IT report and assurance statement offer structural benefits.

project of the paper registration forms of the organ donor register (from 2011), a back-up was made at the time onto two external hard disks. These two external hard disks, which were most likely not secured, contained a copy of the digitalised files of 6.9 million organ donation decision forms as registered or amended in the period from February 1998 to June 2010. A check revealed that these two external hard disks were no longer in the safe where they were being kept.'[387] The personal data of millions of Dutch residents suddenly seemed to have disappeared in 2020. Besides general personal data, such as name and address details, the data also included their previous decision on organ donation, a signature and the citizen service number or A number (unique personal number under which a person is registered in the municipal persons database).

In response to this data breach, the National Audit Office started an investigation. 'The applicable information security plan included an inventory of business resources. The business resources such as external data carriers, like DVDs, USB sticks and hard drives, were not included in this, however. As a consequence, no (references to) measures, procedures or working methods for external data carriers were found in the plan', according to the report. Procedures for handling and storing information in order to protect it against unauthorised disclosure or abuse were also not fully worked out in detail. As far as the use of safes was concerned, there was no key protocol and no work instruction, which meant there was no up-to-date overview of who had been in the safe and what was supposed to be in the safe.

Electronic mail

Caution is still advised with email traffic, and not just in the use of the popular and transparent CC functionality; probably a very common incident. This recently befell the Party for Freedom (PVV). Due to an error by a party assistant of the Overijssel chapter, the email addresses (and therefore in many cases the names) of the addressees were visible to all the recipients of the invitation. As a result, the political views - a special category of personal data - of the recipients were shared. The Dutch Data Protection Authority imposed a fine of 7,500 euros on the organisation on 11 May 2021 for failing to report a data breach.[388]

[387] Letter from the director of the CIBG Agency to the Minister of Public Health, Welfare and Sport of 9 March 2020.

[388] https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-pvv-overijssel-vanwege-niet-melden-datalek

The use of email addresses of personnel who have since left an organisation is also subject to privacy rules that can be included in the digital security policy. On 7 January 2021, for instance, a Norwegian company was fined by privacy regulator Datatilsynet because of the unlawful access to the email account of a former employee.[389] In addition to paying an administrative fine, the organisation must henceforth document in writing the procedures for accessing the email accounts of employees and former employees.

A manager of the company had changed the password and logged into the former employee's email account daily for a period of six weeks after the employment contract had ended. He also obtained access to the correspondence from over five months previous. The account had reportedly been kept open to be able to follow up on contact with customers. That may seem a legitimate purpose; according to Datatilsynet the modus operandi was in violation of both the company rules and the European privacy legislation. There was no legal ground for the processing.[390] The continuation of a former employee's email account, including that of the CEO, had incidentally already been deemed unlawful by the Belgian privacy regulator, the Gegevensbeschermingsautoriteit (GBA).[391]

Domain names

Another topic for the digital security policy: system leaks that arise because domain names that have fallen into disuse are not properly 'cleaned up'. This type of disaster can, in turn, result in a breach of the security of personal data (a data breach in the sense of the privacy legislation), the loss of trade secrets and/or other negative implications for the organisation. A security investigator in 2015 alerted Dutch police about an incident involving expired, old domain names, and the police then apparently did little with the security information.[392]

[389] https://www.datatilsynet.no/en/news/2021/fined-for-accessing-former-employees-e-mail-inbox-and-failing-to-close-e-mail-inbox/ Although Norway is not an EU member state, it is a member of the European Economic Area (EEA) and the country has incorporated the GDPR in its national legislation.

[390] For the record: the company failed in its duty to provide information (Article 13 GDPR), to delete the content of the complainant's email account (Article 17 GDPR) and to handle the complainant's objections (Article 21 GDPR).

[391] https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-64-2020.pdf

[392] https://www.security.nl/posting/500610/Politie+lekt+gevoelige+e-mails+via+verlopen+domeinnamen

Five years later, RTL Nieuws reported about a similar matter at the Youth Care Office in Utrecht.[393] On 1 October 2020, a youth care institution was again in the news because the personal data of thousands - many of them underage - clients turned out to be accessible via a domain name that was no longer being used.[394] All these Dutch cases concerned errors in the management of crucial domain names, according to the Netherlands Internet Domain Names Foundation (SIDN).[395] It would probably be more correct to say 'serious' errors, because domain names are used not only in email addresses and websites, but also in all sorts of applications. In theory, it should - finally - be clear that digitalisation imposes higher demands on an organisation, both in terms of substantive expertise and due care in its actions, but that does not mean in advance that this is adequately fleshed out in practical terms. SIDN therefore warns that suddenly closing down and disposing of the domain name enables cybercriminals to take control of the particular domain names and use them to obtain access to the applications. Setting up and carefully implementing an adequate management policy prevents the risk of security breaches. SIDN draws five lessons from practice:

1. do not immediately stop using a domain name after a switch;
2. make a list of the domain names and what they are used for;
3. inform employees that certain domain names and email addresses are no longer being used;
4. monitor rogue registrations and login attempts; and
5. use multifactor authentication.

The problem is not confined to the Netherlands, of course. Research in the US, for instance, shows that the legal profession in particular acts carelessly in this respect.[396] In particular, the frequent mergers and acquisitions of law firms are a reason for no longer using domain names and simply letting the registration expire. With all the ensuing consequences. On that side of the Atlantic, where there is no

[393] https://www.rtlnieuws.nl/tech/artikel/4672826/jeugdzorg-datalek-dossiers-kinderen-utrecht-email

[394] https://www.rtlnieuws.nl/nieuws/nederland/artikel/5187220/jeugdriagg-kenter-jeugdhulp-datalek-dossiers

[395] https://www.sidn.nl/nieuws-en-blogs/verkeerd-gebruik-domeinnaam-leidt-opnieuw-tot-datalek-in-jeugdhulpverlening

[396] https://medium.com/@gszathmari/hacking-law-firms-abandoned-domain-name-attack-560979e0b774

strict privacy legislation on par with the European Union's GDPR, the advice is strikingly different. Set up a so-called 'catch-all email service', so that all email correspondence continues to arrive, *even that addressed to former employees*. It is also advisable to receive 'password reset emails' from online services.

In conclusion

The rapid and divergent developments in the digital security domain demand a great deal from directors, policymakers, implementers and auditors; in particular in the boardroom of any organisation, because this is where all the lines come together. The monolithic digitally-related threat of the past - mainly fraud and sabotage by an organisation's own employees - has changed from a niche problem to a generic one; multifaceted and permanent in nature. A multidisciplinary approach has become unavoidable in this context, one that devotes attention to technology, people and the organisation.

We can find important points of reference for more legally-initiated components in the digital security policy not only by looking to the legislation and regulation and caselaw, but also by closely monitoring the day-to-day practice of incidents and disasters. This can then result in sharpening existing rules and even in an entirely new sub-policy, such as one for domain names.

A few analyses

- An organisational form that is dispersed , work that is independent of location and time, and hybrid work, the digital processing of business information, doing business electronically and the corresponding legal frameworks require up-to-date and advanced digital security policy more than ever because of the permanent threats. Small businesses and institutions can seek support from industry and umbrella organisations. Intensive cooperation and knowledge sharing is unavoidable, in view of even just the complexity alone.
- In addition to satisfying the mandatory regulations, there is also room for choices. Digital rules of conduct for personnel can, if desired, also reflect the nature and culture of the organisation. Strict or less strict (with more autonomy for employees to perform their work), but always with a holistic approach and a sharp eye for the legitimate interests of the employer and its customers.

- Realise that digital security policy is dynamic in nature. The policy rules will each time be updated in response to new factual and legal developments and will have to be declared applicable anew, in any event in the staff relationship.

28. How financial institutions handle the risks of the quantum computer

Marco Doeland and Oscar Covers

The Dutch vital financial infrastructure was informed by the Dutch General Intelligence and Security Service, AIVD at the end of 2015 about the advent of the quantum computer and the threats associated with it. From that moment onwards, the financial institutions in the Netherlands have been closely following the developments in relation to the quantum computer and trying to gain insight into what implications it has for the security of (inter) banking business processes. This chapter summarises the insights gained on how banks and payment institutions can best anticipate the advent of the quantum computer and what actions can already be put in motion now, even though this field is still fully in flux. This insight was obtained by bringing together quantum computing experts and experts from financial institutions so they could jointly analyse the impact of the quantum computing developments on the sector. This is updated annually and, if necessary, the Dutch Banking Association adjusts the recommendations accordingly. The key objective is to arrive at an approach for dealing with the threats posed by the quantum computer so that payment traffic can continue securely and without disruption.

Impact of the quantum computer

Quantum computing is a fundamental research area that is rapidly developing.[397], [398] The advent of the quantum computer is a disruptive innovation that will have a

[397] Birch consultants. "Bouwen aan een Q-Campus: Realiseren van een Quantum Ecosysteem in Delft." Rijksoverheid, Birch consultants, 4 Oct. 2018, www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/10/04/building-a-qcampus-realising-a-quantum-ecosystem-in-delft/Building een Q-Campus - Realiseren van een Quantum ecosysteem in Delft.pdf.

[398] Boston Consulting Group, et al. "The Coming Quantum Leap in Computing." Https://Www.Bcg.Com, 16 May 2018, www.bcg.com/publications/2018/coming-quantum-leap-computing.aspx.

revolutionary impact on the global economy. The threat stems from the major impact that the quantum computer has on cryptography as we know it. Using a large quantum computer, the cryptographic keys used can be figured out much more easily than using today's supercomputers. At the moment, no one knows how long it will take before the quantum computer has enough computing power to crack today's encryption algorithms. For the financial sector, it is very important to understand how quantum computing impacts the security of the financial key infrastructure and the payment system.[399]

The quantum computer is fundamentally different from the computers we know today. The difference starts at the level of the data medium used by the quantum computer. The traditional computer uses a 'bit', which has two states: a zero or one (0 or 1). The quantum computer uses a 'qubit' (quantum bit), which is in both states at the same time. This property is known in quantum mechanics as superposition. A qubit in superposition cannot be read without influencing it. When observed, the qubit will 'collapse' into, either 0 or 1. Which value it will be cannot be predicted in advance. These and other unique quantum mechanics properties that the qubit has also mean that the calculations follow a fundamentally different method and the results are also reached very differently. If a qubit in superposition simultaneously represents two states then it is also conceivable that the computing power of a quantum computer scales up very rapidly for each additional qubit that participates. Adding one qubit doubles the computing capacity.

There are currently quantum algorithms known that can solve some mathematical problems exponentially faster than today's computers can. This opens up entirely new possibilities for finding new methods of performing chemical processes much more efficiently, such as the process of producing artificial fertiliser, for instance.[400] This also applies for developing new medicines[401] and for much more. But there are also quantum algorithms that are known to weaken today's encryption algorithms. This has consequences for encryption as we currently use it to secure our data.

[399] For more background info, see: Quantum-computing-keep-payments-safe-and-secure.pdf (betaalvereniging.nl)

[400] Reiher, M., Wiebe, N., Svore, K. M., Wecker, D., & Troyer, M. (2017). Elucidating reaction mechanisms on quantum computers. Proceedings of the National Academy of Sciences, 114(29), 7555-7560.

[401] https://research.aimultiple.com/quantum-computing-applications/

Symmetric key algorithms

The symmetric key algorithms are the best known and most commonly used encryption algorithms. A characteristic of these key algorithms is that they use one key for both encryption of the plaintext to ciphertext and decryption of the ciphertext to the plaintext. The major advantage of symmetric encryption is that it is very rapid; the disadvantage is that the key must be kept secret *and* shared with the recipient. If someone is able to eavesdrop on the secret key then all the encrypted messages can be read, but also manipulated. Because in that case the message can be deciphered, read, manipulated and re-encrypted. Another major disadvantage is that a unique key is needed for every communication partner. This quickly becomes an untenable situation.

Asymmetric public key algorithm

Asymmetric or public key algorithms are distinguished by the fact that they have two keys which together form one pair. What is encrypted using the one key can only be decrypted using the corresponding key. This makes it so that one key can be publicly known; anyone can then use this public key to encrypt a message for the owner of the key, who has the other part, his private key. This means anyone can encrypt a message with the public key of the recipient and that encrypted message can only be decrypted using the private key of the recipient. This is a great advantage. Public key algorithms do not need a secure channel for the exchange of one or more secret keys between the communication parties. The disadvantage is that asymmetric key algorithms use much more computing power, especially compared to symmetric key algorithms.

Secure processing of payment transactions

Payment traffic makes much use of encryption algorithms to secure the transaction data, to exchange encryption keys, to guaranteeing the integrity of the transaction, to safeguard the authenticity and the non-repudiation of the transaction.

In order to process financial transactions efficiently, both symmetric and asymmetric encryption are used and the different properties offered by the algorithms are optimal used. Large quantities of data can be very efficiently coded using symmetric encryption algorithms. The secret key used for this can be encrypted using asymmetric encryption. Thus the different properties are utilised optimally in combination.

The property that gives the encryption algorithm its strength

Encryption algorithms code the information by means of a key. In the process, the original data are converted into an alternative form, what is referred to as ciphertext. This process erects a barrier that makes it difficult to decode the ciphertext back to the original message without knowing the key used. In cryptography, this barrier is called 'the hard problem', based on a mathematical problem. The mathematical problems of cryptography are tailored to the computer architectures and their computing power. Some mathematical problems from which today's encryption algorithms derive their strength are easily solvable by a quantum computer. There are two quantum algorithms known, for instance, that have a major impact on our current cryptography: the Shor algorithm[402] and the Grover algorithm.[403]

The means needed to implement the Grover or Shor algorithm on a quantum computer to break cryptography systems are not yet available. The quantum computer does not at present pose a direct threat, but it could already be a threat for data that need to be kept secret for a long period of time. The so-called '*store now, decrypt later*' problem. After all, the cryptograms could be stored now and decrypted at the moment the quantum computer becomes available. We refer to that moment as 'day z'.

Mosca's theorem

So in the research area of the quantum computer there are still many unknowns, including day z, that the quantum computer can break current cryptography systems. This means it is also unknown for how long today's cryptography systems can still be used securely. How to deal with this? Mosca's theorem[404] is useful in this regard. This theorem says, in short:

If $x + y > z$, then we have a problem.

[402] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). Ieee.

[403] Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

[404] Mosca, M. (2013, September). Setting the scene for the ETSI quantum-safe cryptography workshop. In e-proceedings of 1st Quantum-Safe-Crypto Workshop, Sophia Antipolis (pp. 26-27).

Where:

x = shelf-life of the encryption algorithm in question. How long can you securely use that encryption algorithm in combination with that key?

y = migration time. How much time does the organisation need to migrate from today's encryption algorithm to another secure encryption solution?

z = the day that the quantum computer, or another method, can break the particular encryption algorithm x.

In other words, if the shelf-life of today's encryption algorithm plus the time needed to migrate to a secure solution is further away than day z, on which a quantum computer breaks the encryption algorithm mentioned, we have a problem.

So if you must guarantee the confidentiality of data for the long term, you already face a major challenge, not to mention a problem, if these confidential data are exchanged via a public channel. The so-called '*store now, decrypt later*' problem, this is precisely the challenge governments and embassies already see themselves facing now.

Quantum-safe encryption

The question is: what encryption will still be safe in the era of the quantum computer? The Grover algorithm weakens symmetric key algorithms. Without going into detail, we can report that academics agree with the rule of thumb that symmetric key algorithms can be safely used by doubling the key length. But a popular symmetric key algorithm like DES will be retired even before the era of the quantum computer because the inherent encryption key is too short.

The Shore algorithm breaks the asymmetric key algorithms, so we need alternatives for the public key algorithms.

In December 2016, NIST put a standardisation process in motion for this. Academics had anticipated on this since even before 2005, many researchers had already started searching for alternative encryption algorithms for the public key algorithms. These algorithms are known as post-quantum cryptography (PQC).

At the end of 2017, the standardisation process started with 23 signature schemes and 59 key encapsulation mechanisms. At present there are still 3 and 4 algorithms, respectively, in the process. The work is expected to end between 2022 and 2024.[405]

[405] Cryptography-Workshops, NIST Post-Quantum. 'Timeline.' Technical report, NIST, 2017. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

Steps the banks are taking

As outlined above, there are still many uncertainties in relation to the advent of the quantum computer, but there are also a few certainties. Based on these certainties, the Dutch banks have drawn up so-called low-regret moves, advices for pragmatically and realistically dealing with the threats posed by the quantum computer.

1. Closely monitor the developments in relation to quantum computing and PQC.
2. Make an inventory of all the (inter) banking processes that use encryption, which encryption algorithms are involved, the key lengths used and keep this list up to date.
3. Alert international financial organisations to the risks introduced by the quantum computer so that they can also prepare for the advent of quantum computing.
4. For symmetric key algorithms, immediately start the migration to the Advanced Encryption Standard, secure hash and key derivation algorithms.
5. Develop a fall-back scenario that uses traditional quantum-safe cryptography for the card payment infrastructure.
6. Develop a smart card profile for the payment card that does not depend - for security - on asymmetric encryption.
7. Enforce a policy to implement the latest official Transport Layer Security releases and gain experience with PQC algorithms.

Conclusion

The Dutch financial institutions will have to take the necessary steps together to maintain a secure, stable and robust payment system in the era of the quantum computer as well.

It is crucially important to include all relevant parties, not only in the Netherlands but worldwide, and inform them in order to guarantee the continuity of international payment traffic. This requires active involvement of all participants. Besides the banks, this includes transaction processors and payment service providers of national and international payment products, for instance, but also universities and governments.

Recommendations

What are the generic takeaways? It starts with ‘understanding your business risks’. Does the ‘*store now, decrypt later*’ risk apply? How to deal with encrypted documents that already appear in the public domain? The damage can be limited by henceforth only using quantum-safe encryption and/or not using public networks.

Companies that conclude important agreements which are only endorsed on the basis of digitally signed documents would be wise to provide this agreement annually with an extra digital signature based on the most recent standards. The standards are evolving in line with the technical developments, and stacked digital signatures are also (more) difficult for a quantum computer to compromise.

The steps the banks are taking can be generalised as follows:

1. Closely monitor the developments in relation to quantum computing and PQC.
2. Make an inventory of all the business processes that use encryption, which encryption algorithms are involved and keep this list up to date.
    a. explore which quantum-safe encryption algorithm can replace a vulnerable encryption algorithm.
    b. explore what migration time frames are involved in introducing the quantum-safe encryption algorithm.
    c. start the migration on time so that any setbacks can be dealt with. Remember that infrastructures that use embedded systems generally have longer migration time frames than internet-based infrastructures.
3. Alert your supply chain to the risks introduced by the quantum computer so that they can also prepare for the advent of quantum computing.
4. For symmetric key algorithms, immediately start the migration to the Advanced Encryption Standard, secure hash and key derivation algorithms.
5. For asymmetric/public key algorithms, adapt the design if necessary so that the security does not depend on asymmetric encryption.
6. Implement the latest official Transport Layer Security releases.

29. How do we train the new generation of security specialists?

Peter van Eijk

How do we educate the new generation of specialists in digital security? On closer look, who are these experts? What do they do? The field continues to evolve at a rapid pace, which has implications for the content and form of degree programmes. From the perspective of an ICT institute in higher education, on the one hand, and the giving of security instructions in the cloud-computing domain to experienced professionals, on the other, a new, innovative direction is taking shape that embraces above-all project-driven and so-called 'gamified' learning. In this chapter, we explore the breadth of what makes someone a digital security professional. It should also be pointed out in this regard that properly speaking, the developments are moving too fast to build and roll out a standard curriculum; especially for an individual educational institution. Finally, we conclude with some recommendations.

Introduction

Digital security is a field that continues to develop. In the 1960s and '70s, the first 'EDP auditors' concentrated mainly on the integrity of data processing. The key threats at that time were software errors and the internal abuse of administrative processes. After that, the IT security field developed, to deal with a wider scope of sources of risk. With the rise of data communication and the internet, IT now lives in 'cyberspace',[406] with the corresponding series of new threats. That is why we also often talk about 'cybersecurity'. The rise of complex IT supply chains, like those facilitated by cloud computing, gives rise in turn to new security challenges.

The demand for security specialists exceeds supply and is growing. In 2019, the UWV wrote: 'The increased digitalisation and strong demand for data security caused employment growth among (the still relatively modest group of) security specialists (5,000) to outpace growth in all the other ICT professions

[406] Wikipedia has an interesting entry on the origin of the term 'Cyberspace'. These days it mainly denotes the overall world of information systems, which is primarily connected via the internet.

(+54%).'[407] Security is also increasingly becoming an important part of the work of people in other jobs (software developers, for instance). We seriously underestimate the training need, therefore. This raises the question of how to meet the training need for these professionals. Historically, many people with an IT security profile have completed higher education, but not in security. They have 'landed' in this field through additional training and retraining, on the job and otherwise.

In an occupation that is becoming more professionalised, we usually see a recognisable 'body of knowledge' arising, standard ways of working, and common standards and values. Together, this ensures that the occupational group can face bigger challenges, with more effectiveness and efficiency. The challenges are also growing. While in the past we mainly saw 'script kiddies', we now see organised crime (currently focused on ransomware) and nation-state actors that carry out attacks on an industrial scale. Where in the past we mainly had to keep track of the risks and quality in the internal IT, that has expanded to include an entire ecosystem of hundreds to thousands of cloud suppliers on which the average organisation is dependent. This demands further professionalisation of the field.

Objective and resources

The objective of security is ultimately to keep the risks associated with the use of information technology manageable and reduce these to a level that is acceptable in relation to the utility of the use of that technology. For a core banking system, the risk tolerance will be substantially lower than for an AI-based helpdesk chatbot.

The main lines of security as a body of knowledge are as follows. Risks can concern the availability, reliability, and confidentiality of information. These risks can manifest in the storage, use and transmission of data. Security measures can relate to the technology, the people involved, or the processes (People Process Technology). The security specialist needs knowledge and skills in each of these dimensions.

Sample card

It would go beyond the scope of this article to give a detailed summary of the field, the job classification system or even just the level of the competent starting professional. We will suffice with a sampler.

[407] UWV Factsheet ICT Professions 2019, https://www.uwv.nl/overuwv/Images/factsheet-ict-beroepen-2019.pdf.

- Many risks arise from the technology, and to have a thorough understanding of these, the security specialist will therefore have to have in-depth understanding of that technology and the way in which it is developed and managed. Morover, some of the work of security specialists also involves applying that technology by automating security tasks.
- Examples of relevant technology: Windows and Linux, Cloud infrastructure, networks, basic programming skills in Bash, Python, and the like, automation tooling like Ansible and Terraform, security tooling like Kali Linux, and continuous delivery pipelines.
- Organisation of the technology: the architecture as cornerstone of the 'defence'.
- Knowledge of and experience with security processes (security operations, ethical hacking, incident handling and workflow, forensics, threat intelligence, offensive/defensive).
- Information risk and security management models and classification models such as the ATT&CK framework, and the Cloud Controls Matrix.
- Analytical skills.
- Communication skills. Security is pre-eminently a team sport, not least because of the breadth of the knowledge required.
- Legal aspects (including privacy, intellectual property, ethics and contract law).

Developments in IT security never stand still. To think that at some point we will have tracked down and fixed the last vulnerabilities is as naive as thinking that we will at some point have written the last line of software code. That means that in addition to basic concepts and practical skills, we must also foster in our students a learning attitude.

How to educate?

As an educational institution, one of our challenges is to keep our material and curriculum up to date. Information technology is developing rapidly, digital security is developing even faster, and new threats can emerge from one day to the next. But we simply cannot afford to independently revise every field virtually every year. At the moment, we see two solutions for this: more project-based learning and more inter-institutional cooperation.

Identifying IT vulnerabilities is not something you can learn (solely) from a book, no more than you could learn to drive a car from a manual. Project-based learning in security has therefore been commonplace in the field for years, albeit under the label of 'gamification'. In security professions outside of IT, such as defence and disaster response, we also see 'train as you fight' as a starting point. The 'shooting range' is a familiar concept in this world. Analogous to that, we talk about 'cyber ranges'. The best-known appearance of this in cybersecurity is the CTF (Capture the Flag) competition. In this, individuals or teams compete to win one or more flags as quickly as possible. That can be done by cracking codes, taking advantage of vulnerabilities, or whatever else sprouts forth from the CTF designer's creativity. With IT security, evaluating the result is particularly simple. The flag is either captured, or it is not.

The main variants of cyber ranges are Jeopardy and Attack/Defence. In Jeopardy style (like the American quiz show), the participants can choose from categories and win points in those categories with individual tasks. In Attack/Defence, teams fight for control over a server or network, for instance. Aside from the formats, it is customary to reflect on what has been learned via so-called write-ups.[408] In education, these write-ups are also a useful assessment component.

Learning while playing

The Jeopardy format in particular can be easily used for IT security education. The content and weight of the assignments can be varied widely, the result achieved can be tested automatically and unequivocally, and the 'gamification' makes it appealing for students. There are points for concern as well, of course. Not all security topics lend themselves to this form in the same way. This form seems less suitable for teaching legal knowledge and skills and social engineering, for instance.[409] Measures also need to be taken to prevent fraud and plagiarism. The experience is that one way of doing this is by having students produce write-ups.

In an educational context, the explanation of the tasks (also called puzzles or challenges) can range from detailed (for beginners) to practically absent (for advanced). This latter method also contributes to 'learning how to learn'. The student learns the autonomy that we also expect in professional practice.

Project-based learning, and therefore also CTF as a form of education and assessment, gives us the latitude to focus more on learning yields than on elaborating the content. Nevertheless, developing the tasks and learning scenarios

[408] Švábenský, Valdemar; Čeleda, Pavel; Vykopal, Jan; Brišáková, Silvia (March 2021). "Cybersecurity knowledge and skills taught in capture the flag challenges". Computers & Security. 102 (102154): 102154. arXiv:2101.01421. doi:10.1016/j.cose.2020.102154. S2CID 230523819

[409] This is defined as manipulating individuals in order to gain access to secret information or systems.

remains an effort. An actual software platform to be able to carry out those CTFs is also a significant investment. Reason to seek out collaboration in this respect. A number of universities of applied sciences in the Netherlands have therefore taken the initiative for a 'Joint Cyber Range', following suit from similar initiatives abroad.[410] This is a platform for offering IT security education that can be broadly deployed, provided with a series of exercises supplemented with educational content, to which every institution can contribute and in which each can make its own selection. The first pilots on this have already been run.[411]

Conclusion

Digital security is a rapidly developing field which is also growing in societal importance. It is therefore important to continue professionalising the education of specialists in this field. It is precisely because of the special characteristics of IT security, such as the speed of its evolution and ease of assessment, that it lends itself for more project-based learning. The use of the aforementioned cyber ranges is a good option in this respect. At the same time, this form can make it more feasible for the educational institutions to continue to provide the up and coming professional with up-to-date training while keeping development costs at an acceptable level.

Points for attention

- Digital security is a rapidly changing field in which knowledge quickly becomes outdated.
- The demand for degree programmes is growing strongly.
- Learning environments incorporating so-called 'cyber ranges' are effective and efficient.
- Explore the possibility of expanding existing security education with games and a practical environment. Many platforms are available, but their applicability for specific learning questions varies.
- For tertiary (and secondary) education, investigate the desirability of inter-institutional collaborations in developing and managing the curriculum and

[410] For example, the US Cyber range https://www.uscyberrange.org/.

[411] See, for instance, the introductory series of podcasts (TS101) by Daniel Meinsma https://anchor.fm/ts101, with topics like Ethical Hacking, Security by design, Internet of Things, Security Operations Center, Cloud Security, Digital Forensics, Botnets.

course material. Without this collaboration, it is difficult to continue offering an up-to-date degree programme.

- There is also a need for constant training outside of the regular education system. It could be useful to seek out collaborations with educational institutions for this.
- For active cybersecurity companies, developing challenges could be a way of translating knowledge about new threats into learning material for the training and degree programmes.

30. Liability for digital security vulnerabilities

Jeroen van Helden

Defective software security can result in data loss, entire production environments coming to a standstill or the remote takeover of critical infrastructure. The consequences can be enormous. In 2017, shipping giant Maersk fell victim to a ransomware attack. As a result, transport and transhipment of containers was on hold for weeks. Damage: 300 million dollars in lost turnover. Closer to home, Maastricht University was hit by a cyber attack in 2019. Students and employees were unable to access their files for weeks and only regained access to the systems after the university paid 200,000 in ransom. After the dust is settled and the incident is handled, the same question irrevocably arises: who is liable for the damage? This chapter sheds light on this question with reference to a fictional case involving the Boerhaave Hospital.

Case: smart thermostat

Boerhaave Hospital wants to save on energy costs and decides to purchase a smart thermostat. The thermostat is manufactured by the company ThermosX and is delivered and installed by IT provider ComputerAssistent, which also takes care of Boerhaave's company automation. When the thermostat is installed, ComputerAssistent fails to segregate the network used by the thermostat from the company network. The firmware of the smart thermostat contains a vulnerability which enables hacker collective DarkForce to gain access to the thermostat. From the thermostat, the hackers penetrate the company network and then carry out a ransomware attack.

Boerhaave does not have any back-ups on which to fall back, but initially refuses to pay the ransom. The hackers then put part of the patient database online, including the health data of patient Herman. The hack also causes Herman's scheduled surgery to be postponed, which causes damage to his health. Boerhaave is forced to pay the ransom after all, in the form of 5 Bitcoin, equivalent to over

€200,000.[412] A substantial loss. Boerhaave wants to recover the damage from ThermosX and/or ComputerAssistent. Herman wants compensation for the injury he has suffered and the breach of his privacy.

Breach by ComputerAssistent?

Boerhaave only concluded a contract with ComputerAssistent and can sue only ComputerAssistent on grounds of breach of contract (Article 6:74 DCC). Boerhaave will then have to prove that ComputerAssistent failed attributably in performing the contract by insufficiently segmenting the network and/or failing to provide for an adequate back-up structure.

The parties may well have made explicit agreements on these kinds of aspects, in which case these agreements will be decisive for the question of whether there has been breach of contract. There is a good chance, however, (if experience is anything to go by) that the parties have not made (clear) agreements on this. Does this mean that a lawsuit based on breach of contract is doomed to fail? No, not necessarily.

The content of a contract consists of what the parties *intended* to agree (the so-called Haviltex formula). What either side was reasonably able to expect plays an important role in that. As such, obligations could become part of a contract without this having to have been agreed in so many words. The District Court of Amsterdam held in 2018, for instance, that a customer who ordered delivery of a 'total package' - consisting of the installation and management and maintenance of a corporate network - could expect that adequate security in the form of a firewall and an adequate back-up structure would be included.[413]

The contract on the basis of which ComputerAssistent provides services moreover qualifies as a contract for services, so that ComputerAssistent must exercise the care of a good contractor. ComputerAssistent must, in other words, conduct itself as a reasonably competent and reasonably acting professional.[414] This duty of care can have far-reaching consequences for an IT service provider's

[412] Exchange rate on 15 September 2021.

[413] http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2018:10124. A year later, that same district court held that a customer of a professional IT service provider could expect that the latter would work with due observance of the ISO/IEC 25010 standard for software quality, even if this had not been explicitly agreed, see http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2019:9635.

[414] P.G. van der Putt & C.A.M. van de Bunt, 'Bijzondere zorgplichten van IT-leveranciers', Computerrecht 2018/160.

liability in the event of security vulnerabilities. The judgment from the District Court of Amsterdam is once again illustrative. In this case, the IT provider had actually proposed that extra security measures be taken in the form of a firewall and different back-up structure, but the customer rejected these measures saying they were too expensive. In that case, the district court ruled that the provider should have refused the assignment on grounds that it could not be performed, put forward alternatives, or warned urgently and repeatedly about the risks.

Kelderluik criteria

In 1961, a Coca-Cola delivery person fell through an open cellar door in an Amsterdam café and broke his leg. The Supreme Court then formulated the so-called Kelderluik criteria. With reference to these criteria, it can be assessed whether creating a hazardous situation or allowing it to continue constitutes such a degree of negligence that it gives rise to liability (Article 6:162 DCC). Account must be taken of the likelihood of careless behaviour, the chance that accidents will occur, the seriousness of the consequences and how onerous it is to take security measures.

As far as is known, the caselaw does not contain any examples of IT providers who have been held liable, on the basis of this doctrine, for defective information security, but it is not inconceivable: the Kelderluik caselaw has been successfully brought to bear in cases of earthquake damage[415] and climate damage cases.[416]

Is ThermosX liable as manufacturer?

Alongside the general doctrine of tort, the law has several other special regimes for extracontractual liability, including that pertaining to a manufacturer of a defective good (Article 6:185 et seq. DCC). This regime gives rise to strict liability on the part of manufacturers in favour of consumers. The current Dutch regulation on product liability is based on the European Product Liability Directive (Directive 85/374/EEC). This regime is in need of updating in a number of respects.

For instance, the directive assumes a clear distinction between products on the one hand and services on the other. It is precisely a characteristic of the digital revolution that the dividing line between products and services has increasingly blurred. Products and services have become more and more intertwined. Software is being supplied 'as a service' to a growing extent, and, at

[415] http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:HR:2019:1278.

[416] http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2021:5337.

the same time, is being integrated in or connected with products in all sorts of ways. This means that software can make a material product defective and result in physical damage. Take the case of defective car software which prevents a brake pedal from functioning properly, causing an accident.

The manufacturer is currently moreover not liable if the defect did not exist at the moment when the product was put on the market. This starting point is logical and comprehensible for the traditional manufacturer. A furniture maker who sells an armchair loses control over the product at the moment of sale, so defects that arise subsequent to that moment should not be at his risk. The manufacturer of an IoT device, on the other hand, still retains control over the product after its sale, because he has the possibility of issuing (security) updates. In that case, there is no reason (or at least less reason) to limit the strict liability for defects to those defects that existed at the moment the product was put in circulation.[417]

The European Commission also reached these conclusions in a report on the question of whether the current frameworks for liability are adequately equipped for developments such as artificial intelligence (AI), the Internet of Things (IoT) and robotics.[418] The European Parliament has since called on the Commission to reconsider the directive on the above-mentioned and other points.[419]

No compensation of financial loss

Back to our case. The financial loss suffered by Boerhaave as a result of the hack is not eligible for compensation on grounds of product liability, but Herman's health damage might be. In that case, Herman will have to demonstrate that the thermostat '*does not provide the security that one can expect of it*' (Article 6:186(1) DCC). It seems that it can be expected of a manufacturer of IoT devices that the firmware protects against very common vulnerabilities. Nevertheless it could be difficult and expensive for Herman to demonstrate how the damage arose and that ThermosX is, as manufacturer, (partly) responsible for that. Which is why the EU

[417] Cf. EU Expert Group on Liability and New Technologies, 'Liability for Artificial Intelligence and other emerging digital technologies, 2019.

[418] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM/2020/64 final.

[419] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)).

legislator is also considering easing the burden of proof for victims of AI/IoT-related damage.

Privacy violation?

Herman is, finally, outraged at the fact that his medical data were put online, with his name attached. On grounds of the General Data Protection Regulation (GDPR), any person who has suffered material or non-material damage as a result of an infringement of the GDPR '*shall have the right to receive compensation from the controller or processor for the damage suffered*'' (Article 82 GDPR). In this case, Boerhaave is the controller for the processing of Herman's personal data and ComputerAssistent is involved in that processing as processor. Herman could consider suing one of them, or both of them, on grounds of Article 82 GDPR. For that, Herman must demonstrate, briefly put, that these parties failed to take appropriate security measures in accordance with Article 32 GDPR. The caselaw indicates that compensation of non-material damage can be awarded for a violation of the GDPR, but the size of that is usually limited: usually not more than a few hundred euros.[420]

Conclusion

It emerges from the fictional case of the Boerhaave Hospital that Dutch law recognises various grounds on the basis of which an IT provider can be held liable for a digital security vulnerability. In this article, we have looked in turn at breach of contract, tort, product liability and liability on grounds of the GDPR. And yet the number of lawsuits concerning defective information security in the Netherlands (and, for that matter, elsewhere in the European Union and the United States) is still relatively small. Why is that?

This could be explained in part by the lack of *standardisation*. For liability to arise, a standard must always have been breached in some way (a contractual agreement, an unwritten duty of care, an obligation under the GDPR, et cetera). Without the breach of a standard, there can be no liability. For a long time, such standards did not exist, or the standards were unclear or unknown. But now an increasingly more refined and streamlined framework of standards has arisen. Take the ISO/IEC 27002 standard for information security, for instance, the OWASP Top 10 for the security of web applications or the guidelines for securing personal data published by the Dutch DPA. These kinds of standards represent a broad consensus

[420] For example, see http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RVS:2020:898.

on security risks and security measures to be taken. These standards could be declared explicitly applicable to a contract or be brought to bear in substantiating an action grounded on tort. Also consider the Grip on Secure Software Development method which has been developed within the government's Centre for Information Security and Privacy Protection (CIP) and which consists of specific, testable product requirements that can be enforced in tendering procedures and contract management.[421] Or the investigation that is currently being conducted by the Dutch Safety Board (OVV) into the course of events surrounding a security leak in the Citrix software.[422]

These and other initiatives are commendable and should be replicated more widely. With the help of standards and best practices for information security, purchasers can contract more sharply on digital security and lawyers can better advise on the viability of claims. All of this ultimately facilitates the route to the ultimate setter of standards: the judiciary.

Points for attention

- **There is no such thing as 100% security.** A hack as such does not automatically mean that the provider of the software or administrator of the network is liable.[423] That would require that the IT supplier had violated a standard in relation to information security.
- **Duty of care.** The contract on the basis of which IT services are provided often qualifies as a contract for services, so that the IT service provider must exercise the care that can be expected of a good contractor. This could mean that the IT service provider has a far-reaching duty to warn, also in relation to security risks. Failing to comply with this duty to warn could result in liability.
- **Product liability.** The regime for product liability was developed for traditional products and business models that are not geared to the way in which modern suppliers of digital technology deliver their products to consumers. An update of the regime is desirable at this point.

[421] https://www.cip-overheid.nl/media/1500/20200720-ssd-normen-v30.pdf.

[422] https://www.onderzoeksraad.nl/nl/page/17171/beveiligingslek-citrix.

[423] The Court of Appeal of Arnhem-Leeuwarden acknowledged in 2019 that every computer system could ultimately be hacked, so that a customer cannot in principle expect an entirely 'hack-proof' system, see http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2018:7967.

31. Is there any point in cyber insurance against digital crime?

Sieuwert van Otterloo

Many organisations are rightly worried about all sorts of digital threats and attacks. At the moment, the possible infection with so-called ransomware is of particular concern. In the meantime, insurance companies have moved with the times and the computer insurance of times past has evolved to include cover against computer crime as an uncertain event. But is there any point in taking out so-called cyber insurance against the risk of such incidents? For some organisations there might be, because it provides peace of mind. For others there is not. Firstly, there are better preventative measures required before a cyber policy is even useful at all and can be taken out. Secondly, organisations must take into account that some damage, such as reputational damage, is difficult to substantiate and is therefore not covered. Thirdly, it is also a consideration that paying ransom is socially undesirable, even if this is covered by insurance.

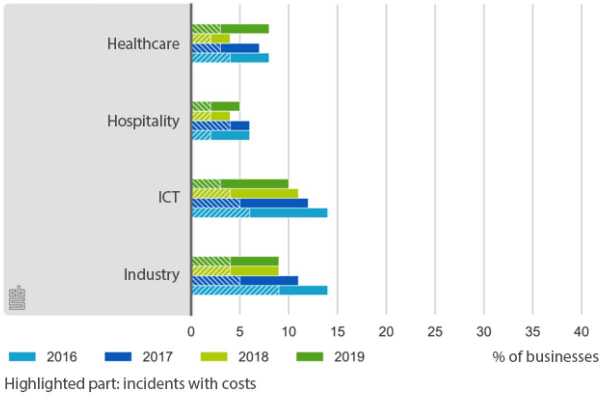
Why attention?

Cyber insurance is a non-life insurance that compensates the damage caused by hacks, system breaches, data loss and other forms of cybercrime. Cyber insurance covers both the damage caused by accidents and the damage caused by criminal attacks. Figures from insurer Marsh show that the number of claims due to accidents account for just 20% of the total, while 80% of the claims concern cybercrime[424].

Properly considered, cyber*crime* insurance would therefore be a more appropriate name, since this is what the insurance is more addressed to. Many companies are looking for ways to defend themselves against digital crime, on account of, among other things, a number of attacks that have made the news. Ransomware attacks in particular make the news because of the number of attacks and the substantial damage they cause. Take, for instance, the attack on Maastricht University in

[424] Marsh Cyber Claims Report 2021, via https://www.marsh.com

2019,[425] the attack on the NWO in February 2021,[426] and the attack on shipping company Maersk in 2017.[427] The attacks are not only targeted at large organisations. Statistics Netherlands reports in its Cybersecurity Monitor 2020 (see illustration) that between 5 and 10% of businesses have dealt with incidents caused by external attacks.[428] Half of the cases caused damage.



Source: Statistics Netherlands (2017e, 2018e, 2019a, 2020c)

ICT security incidents due to external attack by industry sector

Many of the attacks involve ransomware infection. This is actually extortion. Criminals encrypt files and demand ransom to decrypt the files. In some cases, they also threaten to publish the files if no ransom is paid. Criminal organisations make money directly on these kinds of attacks. The criminals are also running a relatively low risk because they can carry out these attacks remotely, from another country. Many organisations are therefore rightly concerned about the risk of ransomware. So it makes sense to investigate the insurance options. Many insurance companies offer cyber insurance.

[425] https://www.nu.nl/tech/6020068/computers-van-universiteit-maastricht-gegijzeld-door-malafide-software.html

[426] https://nos.nl/artikel/2370178-wetenschapsorganisatie-nwo-afgeperst-door-bekende-cybercriminelen-gaat-niet-in-op-eisen

[427] https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million

[428] https://www.cbs.nl/nl-nl/publicatie/2021/18/cybersecuritymonitor-2020

Advantages

Cyber insurance is insurance against the risk of damage, like building insurance or house contents insurance. Most will be familiar with the general features of insurance that covers damage risk: there is a premium which is based on the cover chosen, the size of the company and possibly an excess. Having insurance against damage gives many people peace of mind. In theory, having an insurance policy does not reduce the risk of a certain event occurring, it simply eliminates financial stress. In practice, the cyber insurance offers a handful of advantages:

- Prior to concluding the insurance, a risk scan is performed. This can yield new insights and practical advice. Topics included in a scan are, for instance, the security of websites, the back-up policy and employee awareness. An organisation that has not sorted this out yet will benefit a great deal from this advice.
- An insurer can stipulate certain requirements for security as a condition for providing cover. In that case, the insurance also acts as an incentive to continue satisfying the requirements.
- When responding to a digital incident, speed is of the essence. Most small and medium-sized enterprises do not have security specialists on staff, nor do they know who the best specialists are in the case of a cyber attack. It takes time to find the best help. Insurers already have contacts with security specialists who can investigate quickly or negotiate with the hostage-takers.
- Having insurance for major damage is sometimes a requirement stipulated by certain clients. It can also help guarantee the business continuity in the event of an incident, or eliminate worries among customers and employees.

An organisation that does not take out cyber insurance will have to satisfy information security requirements in some other way and, for example, itself carry out a cybersecurity scan, draft a plan for responding to cyber attacks and keep funds on hand for such eventualities.

Disadvantages

An obvious disadvantage of the cyber insurance is the cost. A cybercrime insurance costs money and the premiums have increased because the number of attacks and amount of damage per attack have risen.[429] International insurers like AIG indicated in August 2021 that the costs had increased 40% because of the high number of claims,[430] and that they were consequently tightening up terms and conditions as well. Anyone taking out insurance now will most likely pay a higher premium with a higher excess per incident. Alongside this obvious disadvantage, there are also other disadvantages, however, which apply specifically for cybercrime insurance:

- The small print of insurance terms and conditions contain certain exclusions. Many insurance policies exclude cover for damage caused by 'war' and 'terrorism', for instance. A major cyber attack like the NotPetya attack in 2017 is qualified as 'war' by, among others, Zurich International, which means claims are denied.[431] Zurich and other insurance companies are officially correct in this respect: much cybercrime is committed on a large scale by hackers backed by non-democratic regimes. It is problematic for companies, however, that precisely the biggest incidents, like the attack at Merck which caused 1 billion euro in damage, are not covered.[432]
- Much of the damage from cybercrime incidents is reputational damage which is difficult to prove. In the event of a large data leak, an organisation will have to notify all customers that a hack has occurred, and the organisation will also be the subject of negative publicity. This has an influence on reputation and thus on future revenue. This damage is indirect, cannot be demonstrated and is not compensated, therefore. So prevention is much better than a cure or a claim. An organisation that genuinely wants to avoid damage or loss must therefore take preventative measures and not rely on insurance.
- Insurance is often taken out to be able to pay the 'ransom' demanded by cybercriminals. Paying ransom is ethically and morally problematic, however. It is better in the long term if companies refuse to pay ransom, but then insurance cover is of little use.

[429] https://www.darkreading.com/risk/ransomware-losses-drive-up-cyber-insurance-costs/d/d-id/1341436

[430] https://www.reuters.com/article/aig-results-cyber-idCNL1N2PD1AJ

[431] https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html

[432] https://www.insurancejournal.com/news/national/2019/12/03/550039.htm

Bitcoin effect

The last point requires explanation. Cybercrime is not new, but has certainly taken off since 2015. Prior to 2015, computer crime often involved property crime, such as embezzlement and theft (by a company's own personnel as well), and sabotage, such as a DDOS attack that causes system outages. Sabotage and vandalism cause a lot of damage but do not produce any financial gain for the perpetrators. Digital extortion was rare because hackers would have to provide their bank details in order to get paid. Consequently they would lose their anonymity.

Since 2015, however, cybercriminals have been able to be paid anonymously via Bitcoin and other virtual currencies, and a ransomware industry has arisen.[433] Attacks are no longer ideologically driven but carried out for purely financial reasons. Hackers keep going as long as they are making money and target every country and branch of industry in which money can be made. The hackers are often not techies themselves, but organisations that purchase hack-scripts. The techies themselves run less risk as a result, because they are no longer directly involved in the attacks. The profits from the hacking activities are reinvested in new attacks.

The current wave of ransomware attacks is therefore a consequence of the decision by organisations to pay ransom: as long as it pays, the criminals will keep going. Paying ransom perpetuates the problem. If criminals know that organisations are insured, they can demand higher amounts. Maastricht University was hacked in 2019 and paid 197,000 euro in ransom.[434] Dutch politicians disagreed with this and the government is now investigating the possibilities of prohibiting the payment of ransoms.[435] If this is introduced, there will be less point in insurance: there will be less insured financial damage and more indirect, uninsured damage.

Alternatives to insurance

Instead of taking out insurance, organisations can take better technical measures. In the cybersecurity monitor mentioned earlier, Statistics Netherlands cited ten recommended measures. Important measures include antivirus software, encryption, training courses, log files, network access control, strong password policy, storage at another location, two-factor authentication and regular updates.

[433] In relation to this, see chapter /../.

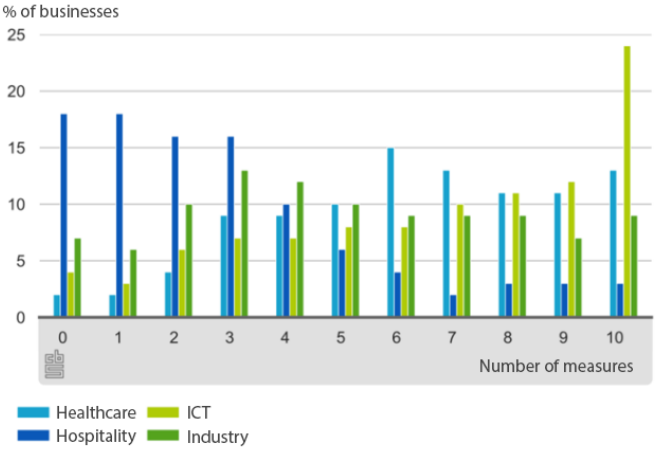
[434] https://www.agconnect.nl/artikel/minister-wilde-niet-dat-universiteit-maastricht-losgeld-betaalde

[435] https://nos.nl/artikel/2398399-overheid-in-actie-tegen-betalen-van-losgeld-aan-ransomware-criminelen

Just one quarter of businesses take more than five measures (see figure). Taking these measures reduces the likelihood of an attack, as well as the potential damage. If all the companies in the Netherlands were to take these measures and stop paying ransom, Dutch organisations would ultimately become unattractive targets.

Conclusion

A cyber insurance policy - for the damage that can arise as a result of digital accidents and crime - is certainly not the most effective measure against ransomware and other attacks. In fact, the insurance does not prevent attacks or damage. Organisations must make a plan to prevent cyber attacks which is based on technical and organisational measures. This plan could be based on ISO 27001, for instance, and implement the concrete measures from this standard. These concrete technical prevention measures are actually effective and therefore more important.



It is only after all the basic measures, such as a strong password policy, two-factor authentication, back-ups, firewalls, security scans and event logging, have been taken, that there is any point in investigating the cover and costs of cyber insurance. For this, one will have to request several quotations and then compare the cover, excess and premium to determine whether there is any point in taking out the insurance. One benefit from this exercise is that the questions posed by insurers or the policy terms and conditions can highlight new points for attention for digital security policy. Applying for insurance can therefore be a good final step in the plan and as such a useful addition to other measures.

Points for attention

- Make sure that the basics are in order: awareness, training, strong password policy, logging, two-factor authentication.
- Have a recovery plan ready for after a cyber incident, and practise this plan to be sure it works.
- Pay close attention to the terms and conditions and exclusions of cyber insurance. Large international attacks are not always covered.

32. Security awareness for employees

Carlos Rieder

Due to the comprehensive technical security measures taken nowadays, attacks are increasingly directed at people. Practically all attacks involve organization-specific information being obtained via Social Engineering beforehand. If people are barely aware or even totally unaware of the intent and purpose of security measures, they quite frequently consider them annoying and disruptive and are likely to circumvent them. Raising security awareness results in a much improved security culture in any organisation and will enhance acceptance of information security, so that this becomes a matter of course and an integral part of company culture. One mandatory requirement for the successful implementation of information security is the regular sensitisation of all employees, taking into account its target audience.

Developing a security culture

People are of paramount importance for information security. They are fully responsible for their own behaviour. There is no way of delegating this responsibility. A company's security therefore significantly depends on every single individual's personal, responsible and vigilant behaviour, and also on the meaning security has for individual people, or on what they understand this to be.

Raising security awareness results in improved acceptance of information security and hence in an improved security culture in any organisation and will enhance acceptance of information security, so this becomes a matter of course and an integral part of company culture. All things considered, the aim is to permanently change behavioural patterns.

To attain this goal, awareness should be refreshed and updated on a regular basis. All employees involved should feel that they are being addressed directly, and should be aware of just how important the role they play is on the road to success. For as long as employees aren't aware of risks and don't know all the relevant security measures or how to apply them, they cannot act appropriately. To support employee awareness of security and the major importance of information security in an organisation, you should run an extensive awareness campaign across the whole of your organisation. There are different approaches to building and shaping a security culture. A communication which is repeated at regular intervals, taking into account its target audience, is the key ingredient for sustained success. Developing a security culture can be roughly split into three phases:

1. Creating a good understanding

The first phase should be used to create a good understanding of the subject involved. Employees are provided with sufficient background information to enable them to understand what security measures and regulations which are relevant to them there are in their organisation. Employees will also need to be motivated to enter phase two as well, i.e. to actually apply what they have learned in practice.

2. Changing behavioural patterns

Changing behavioural patterns is the actual core issue when building a security culture and is therefore also at the heart of any awareness program. You cannot force employees not to open an e-mail which is most likely malware-infested either. But if they are aware of all the potential consequences of doing so, we can at least hope that they will refrain from doing so.

3. Cultivating a habit

The aim of the third phase is for people to automatically or unconsciously apply security measures. A successful awareness campaign will eventually result in sustained changes in employee behavioural patterns. Employees will have to be continually reminded of the subject of information security, so that it becomes a natural part of their daily working lives.

Social Engineering[436] – the vulnerability called "human"

Social Engineering is a wide-spread method of snooping on confidential information. This always targets humans. To obtain such confidential information, it is not only people's credulity and helpfulness which are being exploited, but also their insecurities. Anything from faked telephone calls to people pretending to be someone else and phishing attacks is possible. In general, it is only common sense

[436] Social Engineering - Describes interpersonal influence with the aim of inciting certain behaviour in people, for example, persuading them to divulge confidential information, buy a product or release financial resources.

paired with a healthy dose of suspicion which can successfully thwart a targeted attack. Contrary to that frequently heard opinion, common sense is not something which is innate. It is based on decision-making and responsibility, something which will have to be developed, for instance with the help of awareness campaigns.

The most important contribution to combating social engineering attacks is provided by those attacked themselves, i.e. by checking identity and authorisation of someone requesting something before doing anything about it. Something as simple as asking a caller for the name and telephone number of their superior and their exact business might just expose an attacker.

Achieving a high level information security culture

To support the security and general awareness of all employees and to underline the importance of information security in your organisation, you should run an extensive awareness campaign across your whole organisation, with the aim of rendering information security an integral component of daily working life.

Management support

Employees have to actually feel that management supports and lives information security itself. Management should also sign any covering letters on the subject of information security, so that employees can see that senior management is actively supporting activities in this field.

Information security policy/User policies

Every employee must be familiar with the contents of your information security policy[437]and your user policies[438] and know where these are stored.

Hiring and onboarding

New employees must be familiarised with the subject of information security straight away when hiring and onboarding them. Important requirements like user guidelines should be signed to underline their importance and as proof of acceptance.

[437] Information security policy – strategic statement by the organisation on how to handle information and information processing systems securely.

[438] User policies – mandatory policies for all employees on how to handle information and information processing systems securely.

Communicating information security aspects

The thematisation of information security should never be an isolated event. Instead, this subject should be addressed on a regular basis and on different occasions.

Ideally, employees should be provided with sufficient background information to help them understand what purpose is served by those security measures und regulations they will eventually have to apply and adhere to. If an action or measure makes sense to employees, they are much more likely to actually and reliably apply it.

Target group oriented training

Not all employees have the same information security needs. Some additional groups might like to be trained amongst themselves, e.g. management. For best results, training should be optimized for the needs of its audience. Some typical groups are: management, general employees, external supporters, members of the IT team, sales, and human resources.

Security measure training

Every individual is empowered and motivated to handle information and IT systems with care. A general understanding of the meaning of security overall is conveyed to employees. They are advised as to how information security intersects with all other fields of safety and security. This is meant to instil an understanding into your employees that information security is actually a component of comprehensive security and safety, so-called integral security.

All relevant courses and events pertaining to information technology should mention and present the relevant information security requirements. This is meant to impart to employees that information security is an integral aspect of every activity in the field of IT.

Training can take the following forms:

- Classic training
- Guided workshops, webinars
- Web-based training
- Computer-based training

- Training videos
- Gamification[439]

Ongoing process

It is of utmost importance that not all security contents involved are implemented right at the very beginning of the campaign, since this will often risk overloading employees. The more favourable approach involves distributing individual subjects across a longer period of time so that information security is highlighted time and again.

Employees will have to live information security and must become actively involved in this subject. This will sustainably support acceptance of this issue.

Creating an awareness concept

To align all awareness activities with each other, it is important to describe them in an awareness concept. This should include the following aspects:

- Target audience
- Framework conditions
- Reference documentation
- Type, means, media of communications
- Contents, practical aspects
- Resources required
- Performance measurement
- Reporting

Controls

There have to be controls of the acceptance level of your information security policy. The classic method of employing surveys to do so tends not to be representative, since it is generally only those actually interested in this topic which will reply. A better approach would be a survey of randomly selected employees or drawing conclusions from helpdesk enquiries concerning information security.

Any findings gained from a survey should be communicated to your employees. This results in a deeper awareness and indicates to employees that they can actively help improve information security and are taken seriously.

[439] Gamification –training which includes typical elements of game play (e.g. point scoring, competition with others) which raises audience interest and acceptance

The point here is not to expose any individual employees, but to obtain an overview and indication of the state of your organisation's security awareness. Launching a simulated phishing attack is another option to check your employees' awareness. To do so, a number of employees are sent an e-mail asking them to click an external website link and then enter their log-in name and password there. To achieve this, you will have to employ seemingly plausible-looking explanations and interesting decoys (e. g. an iPhone with a massive price reduction). Your rate of success will very much depend on the quality of the website and decoy used.

Conclusion

Information security should be supported by every employee within their sphere of influence. Major guidelines like Information security policy and user policy should be defined and published. To ensure this will account for a very important part of the overall defence against cyber-attacks. All employees must be motivated to fulfil the regulations and guidelines of the organisation. Frequently repeated trainings, focusing on the requirements of the target group, will build the required security culture. Management should set a good example and enforce the required standards.

Basic awareness tips for employees

- Use common sense. Stay critical, and apply a healthy dose of suspicion.
- Kindly ask people you don't know to provide their name, the name of a contact and their business.
- Make sure you don't leave any confidential documents at your workplace unattended (clear desk).
- Only ever store confidential information on mobile devices in encrypted form.
- Only ever send confidential e-mails in encrypted form.
- Choose strong passwords and keep them private.
- In public, don't let anyone else listen any internal or confidential company matters
- Never connect any USB sticks of unknown origin to your computer.
- Securely dispose of data carriers and confidential documents (shredder).

Final remarks

- Information security concerns everyone.
- Due to the comprehensive technical security measures taken nowadays, attacks are increasingly directed at employees.
- Management must act as a role model for information security, too.
- Information security is a continuous exercise.

List of authors

- Dr. P.E. Baak is Managing Partner at KBenP in Voorburg and duo chairperson of KNVI.
- R. Bierens is a PhD researcher on digital risk at the Amsterdam Business Research Institute of the VU Amsterdam, chairman of the Connect2Trust foundation and strategic advisor to various organizations in the public and private sector.
- Dr.ir. M.A.C. Borgers was at the time of writing this article Corporate Information Officer at Maastricht University. He currently works for the Ministry of Defence.
- P. Borsoi B.ICT is an information security advisor at the Information Services Department of the Dutch Tax and Customs Administration. His contribution appears in a personal capacity.
- B.D. Bosma is an information security consultant and product manager at SURF.
- Dr. W.L. Bronsgeest is duo chairperson of KNVI.
- D. Cioccia LLM is a cybersecurity expert and the Founder of DCODX Cybersecurity.
- O.H.J.B. Covers MSc RE MSc is Cybersecurity Analist at the Dutch Banking Association.
- M.M. Doeland MBA, CISSP, CISM – CISO and Head of the Security Team at the Dutch Banking Association and chairman of the National Forum on the Payment System Working Group on Security.
- S. Dondorp is founder en CEO at Northwave Group and Chairman of the Board of the Cybersecurity Industry Association Cybersafe Netherlands.
- G. Dube MSc, CISSP, CCSP, CISA, CISM, CGEIT, CRISC, CDPSE is a Technology, Cybersecurity and Privacy Consultant and a Computer Society of Zimbabwe Council member.
- N.H.A. van Duuren LLM is attorney-at-law partner for IT, IP & Privacy at De Clercq Lawyers and Notary in Leiden/The Hague and chair of the KNVI Interest Group IT and Law.

- Dr P.H.J. van Eijk is an independent cloud instructor, associate professor at Hogeschool Utrecht and board member of the Dutch department of the Cloud Security Alliance.
- Prof. S. Furnell is Professor of Cyber Security at the University of Nottingham in the UK and the current Chair of Technical Committee 11 in the International Federation of Information Processing.
- Dr. W.H.M. Hafkamp CISSP LL.M. is general director of the Z-CERT foundation, the cybersecurity expertise center for the healthcare sector.
- J. van Helden LLM is attorney-at-law for IT, IP & Privacy at De Clercq Lawyers and Notary in Leiden/The Hague and member of the KNVI Special Interest Group IT and Law.
- Drs. V.G. Hoek is Enterprise Architect at i-Interim Rijk and in this capacity CTO of the Cyber Innovation Hub Defense.
- I.C Huis in ’t Veld is advisor strategy educational innovation and public values at SURF.
- J. Matto RE RI, is partner IT-audit & Advisory at Mazars and also member of the NOREA Committee on Professional Rules and Working Group IT-Audit Report and Statement.
- J.F.K. Nienhuis BSc CISSP is Senior Information Security Officer at Stedin and secretary of the KNVI Interest Group Information Security and IT Security.
- S. Nieuwmeijer is DGA of Secior Cybersecurity, serial entrepreneur and member of advisory board at several companies in the data center industry.
- Drs. W. Olthof is director of NOREA.
- Dr. S. van Otterloo is a consultant on software development, privacy and AI at the ICT Institute.
- Drs F.E. van Paassen RE RA is secretary/treasurer ECP, platform for the information society and chairman of KNVI Information Security & ICT Security (IBIS) Interest Group.
- Mr. S. Petrushevski is a seasoned cybersecurity professional, Senior Security consultant at DCODX Cybersecurity and Senior Security Researcher at Zero Science Lab.
- V.A. de Pous LLM is an independent IT lawyer and analyst in Amsterdam and co-founder and board member of the KNVI Special Interest Group IT and Law.
- Drs. R.L. Pouw is a security officer at SURF, Cooperative for Innovation and IT for Education and Research.

- C. Rieder, Prof. El. Ing FH, isec ag, Lucerne, Switzerland, is a senior information security consultant and assistant lecturer at the Lucerne University of Applied Sciences and Arts - Information Technology.
- Prof. S.H. von Solms is the Director of the Centre for Cyber Security at the University of Johannesburg, South Africa as well as Associate Director of the Global Cybersecurity Capacity Centre of the University of Oxford, UK.
- Prof. R. von Solms is an emeritus distinguished Professor from Nelson Mandela University, South Africa. Prior to retirement, he was the Director of the Centre for Research in Information and Cyber Security (CRICS).
- Prof. S. von Solms is an Associate Professor at the Faculty of Engineering and the Built Environment at the University of Johannesburg, South Africa.
- Prof. E. (von Solms) Kritzinger is Professor in the College of Science, Engineering and Technology at the University of South Africa, South Africa.
- H.L. Souw RE CIPP/E is Information Security Officer at The Dutch Authority for the Financial Markets in Amsterdam and chair of the KNVI Interest Group IT Audit and Risk.
- Dr. D. Velev is professor in computer science at the Department of Information Technology and Communications of the University of National and World Economy in Sofia (Bulgaria). dgvelev@unwe.bg.
- Drs. K. R. Vierbergen-Schuit is programmamanager Agenda Digitale Veiligheid bij de Vereniging Nederlandse Gemeenten.
- H.L. de Vries LLM is director of the National Cyber Security Center, part of the Ministry of Justice & Security.
- S. Wallagh LLM is training manager HBO-ICT Cyber Security & Cloud, Technical Informatics at the University of Applied Sciences in Utrecht and board member of the KNVI Interest Group IT and Law.
- Drs. M. Welters RE RA CRISC is partner IT-Risk EY, also vice-chairman NOREA and member of the IT Audit Report and Statement Working Group.
- B.J.S.A.A.F. de Winter is a publicist, independent expert in information security and privacy protection.
- M. Wijnant, CIPM, CIPT & CIPP/E, is attorney-at-law for IT, IP & Privacy at De Clercq Lawyers and Notary in Leiden/The Hague.
- Dr. P. Zlateva is associate professor in system engineering at the Bulgarian Academy of Sciences in Sofia (Bulgaria), plamzlateva@abv.bg

KNVI Special Interest Group IT and Law

Set up over thirty years ago as the NGI Computer Law Practice Group, the KNVI Special Interest Group IT and Law organises meetings, studies and publications to bring the implications of digital technology and data processing for positive law into focus, preferably in cooperation with the digital professions and where necessary other disciplines, both within and outside the Netherlands Association of Information Professionals.

The developments in digital technology and data processing are constantly changing society and consequently also have implications for the legal relations and application of legal rules between the parties that use ICT or who are confronted with this use. Traditional legal issues often take on different dimensions in the digital era and require new interpretation.

What rules apply in cyber space, what law is applicable to electronic transactions, what consequences does the General Data Protection Regulation have for organisations and why do digital projects still fail? These are just a few of the issues with which the KNVI IG IT and Law is concerned. The angle of approach here is not that of the IT and information professional seeking to implement new technology, but rather that of the legal requirements that society and the law impose on the application and use of information and communication technology.

Further information and application:
Natascha van Duuren, chair of the KNVI Special Interest Group IT and Law
n.vanduuren@declercq.com or +31 (0) 654 983 766

KNVI Special Interest Group Information Security and ICT Security (IG IBIS)

Our society and therefore our entire lives are increasingly dependent on information. That is why the Special Interest Group Information Security and ICT Security (IG IBIS) engages with all aspects of securing information which, after all, we expect to be confidential, incorruptible and available. We also attach a great deal of importance to this from the perspective of privacy (the GDPR).

IG IBIS provides professionals and other interested parties a platform for sharing and exchanging the latest knowledge and developments in relation to digital security. To this end, IBIS organises gatherings at which experts shed light on one or more aspects of information security from different angles of approach. Besides a substantive component, these gatherings are also social events, offering the opportunity to network and catch up in a relaxed atmosphere.

The members and committee of IBIS also contribute to professional publications, recently on blockchain, cloud and cybersecurity, for instance. Company visits provide participants with a surprising look behind the scenes at how people, technology and processes collaborate on information security.

Further information and application:
Frans van Paassen, chair of the KNVI Special Interest Group Information Security and ICT Security (IG IBIS) frans.van.paassen@knvi.nl or +31 (0) 655 853 239

What started with a few basic measures to protect computer systems and the data they process automatically against inadvertent uncertain incidents, such as power outages and fire and water damage, has grown into an advanced, constant battle to make - and keep - information, systems and infrastructure strong enough to withstand both inadvertent and deliberate digital threats, especially computer crime. It goes without saying that digital security is vital today. Without ICT, everything would more or less come to a standstill. A society that is becoming increasingly dependent on digital processes and chains, while analogue fall-back options are in many cases no longer available, must take protective measures. This then means that literally everyone must take into account digital threats and ways of mitigating these risks.

According to the National Cyber Security Centre (NCSC), which, together with the National Coordinator for Security and Counterterrorism (NCTV), set up the Cyber Security Assessment Netherlands 2021, cooperation and knowledge sharing are indispensable in this context. Vulnerabilities and threats in the digital domain must be tackled from a broad perspective.

This message was well received by the Royal Association of Information Professionals (KNVI). For decades, the organisation and its predecessors have been working on knowledge development and sharing, including on information security. In this, a multidisciplinary approach has been expressly chosen each time, which is also evident from the unique series of books to which this collection belongs.

While the NCSC opts for ‘cybersecurity’, without wishing to engage in a discussion of scientific principles, we sometimes use - in the title as well as to some extent in the separate chapters - the term ‘digital security’; a fundamentally broader notion that also encompasses offline media and information and which, for example, includes measures relating to the quality of digitalisation.

This collection therefore envisages providing insight into the broader aspects of the security of digitalisation and the status quo in that domain and fostering more advanced awareness and additional knowledge among the target group: professionals (irrespective of expertise, work area or industry), administrators at government organisations and politicians. Digital security is also a perfect example of a topic that requires a broad-based multidisciplinary approach. After all, it is important to avoid taking a strictly technical or legal view of the countless issues and challenges related to security measures and risk management in and for the digital domain. Only a broad, multidisciplinary approach can increase our digital resilience, limit the effects of digital disasters and prevent social, sectoral, organisational and/or personal disruption resulting from these incidents.

ISBN 978-90-9034977-0
NUR 820