CSR Cyber Security Council

EVERY BUSINESS HAS DUTIES OF CARE IN THE FIELD OF CYBER SECURITY

CYBER SECURITY GUIDE FOR BUSINESSES

1. INTRODUCTION
PAGE 4

1. INTRODUCTION

Information and communications technology (ICT) plays an ever greater role in our society. It brings commercial opportunities for your business, but it also creates new risks. Poor cyber security has major consequences.

Inadequate cyber security may lead to commercial secrets and personal data being divulged through hacking or human error. Major disruptions may even jeopardise the business continuity of your organisation. Cyber security is the responsibility of your organisation's board of directors. It must be clear who on the board will take the lead in this regard. It is crucial therefore that cyber security be placed on the agenda of both the board of directors and the supervisory board.
More information on this can be found in the Cyber Security Council's 'Cyber security guide for boardroom members'. In smaller businesses, the responsibility lies with the director.

In 2014, a data leak at Target (a major department store with operations in Canada and the US) resulted in the theft of 40 million debit and credit card numbers. The data was stolen through the installation of malware on the checkout systems. The incident contributed to the dismissal of the company's CEO.

In 2013, it was found that the RFID (radio-frequency identification) chip in the keys of certain makes of car, which allows cars to be unlocked remotely, could be hacked. This meant that hackers could unlock such vehicles without a key. A large number of cars were subsequently broken into.

What is cyber security?

Cyber security encompasses three areas

1. **Availability: your ICT is available and users have access to the system.**

   - Your ICT cannot be put out of operation by a Distributed Denial of Service (DDoS) attack.
   - Regular backups ensure that business continuity is not jeopardised if an organisation falls victim to ransomware or cryptoware, where hackers encrypt commercial information and only decrypt it on payment of a ransom.
   - The availability of your ICT can be jeopardised by malicious software, viruses or malware. Your business must take measures to prevent 'contamination' by such software.

2. **Integrity: the data that you have processed is complete and correct. The processes used to process data are correct and can be audited.**

   - The stored data is accurate. It can't be deleted or modified by an unauthorised party. If the data is amended however, it can be recovered from a backup.

3. **Confidentiality: only authorised users have access to your ICT and data.**

   - Unauthorised parties can't gain access to your ICT, either via the Internet or on site. Your security systems can't be bypassed through hacking or a remote access tool.
   - Access is protected at minimum by a password and preferably by a two-factor authentication. E.g. to withdraw money from an ATM, a bank card ('something the user owns', factor 1) and a PIN number ('something the user knows', factor 2) are required.
   - Your employees don't open phishing emails. They don't divulge passwords, personal data or other confidential information to unauthorised parties who request them under false pretences.
   - Criminals can't access confidential information by shoulder surfing (visual hacking).

Cyber security can be jeopardised by security incidents. The duties of care in the field of cyber security are designed to minimise the risk of such incidents and if, in spite of this, things do go wrong, to limit their impact.

The following are examples of security incidents:

- An employee loses a laptop or USB stick.
- A hacker gains access to your company's intranet.
- Malware disrupts the operation of your ICT.
- An unauthorised party obtains a password that enables them to gain access to personal data.
- The electronic lock of a car is unlocked without a key.
- A fire or power cut in a data centre means that data is temporarily unavailable.

Responsibility for other people's security

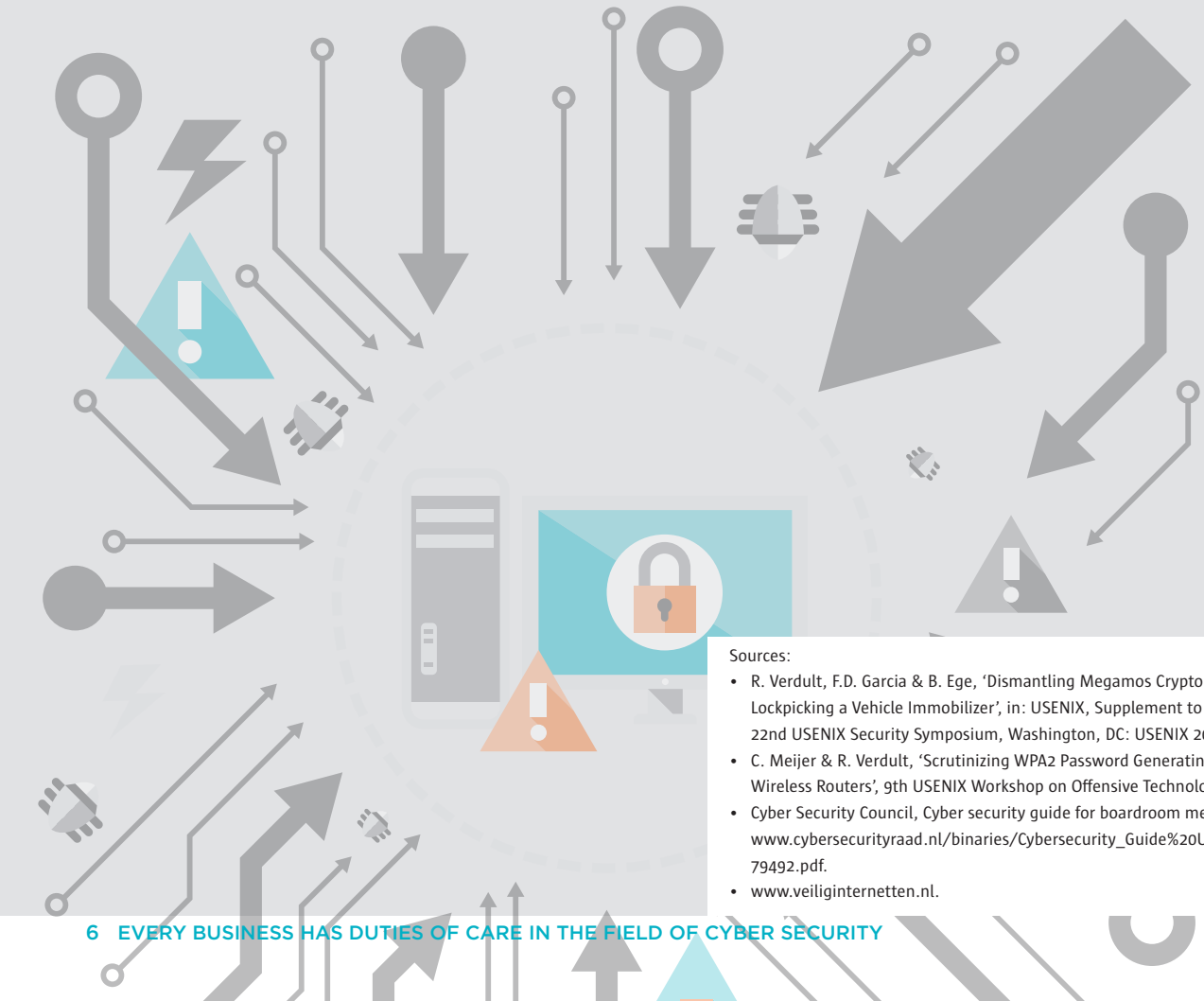
A security incident disrupts your operations and damages your reputation. Often, your organisation forms part of a chain. Your operations may be disrupted by a security incident that has occurred with one of your suppliers, contractors or resellers. Conversely, their operations may also be affected by your cyber security.
Your business must take the interests of third parties into account (to a certain extent). Amongst other things, you must therefore ensure that your ICT is properly protected and that it is coordinated with the other parties in the chain. If you fail to comply with these duties of care, you may be held liable.

Purpose of this guide

This guide provides an overview of the main statutory duties of care in the field of cyber security, and offers guidance on the fulfilment of these obligations. However, it gives only a brief outline of the duties of care and is not sector specific. It does not consider the specific duties of care that apply to businesses that are subject to specific regulations, such as energy companies, telecommunications companies, banks, healthcare institutions, providers of aviation data and other organisations in key sectors.

You can use the guide for information purposes and to check your level of compliance. It is however no substitute for professional advice. Where appropriate, you are advised to engage a specialist lawyer or a security expert and to comply with your duty to report. For practical tips on secure use of the internet, see www.veiliginternetten.nl.

The CSR invites branch organisations to tailor this guide to the needs of their members.



Sources:

- R. Verdult, F.D. Garcia & B. Ege, 'Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer', in: USENIX, Supplement to the Proceedings of the 22nd USENIX Security Symposium, Washington, DC: USENIX 2013.
- C. Meijer & R. Verdult, 'Scrutinizing WPA2 Password Generating Algorithms in Wireless Routers', 9th USENIX Workshop on Offensive Technologies 2015.
- Cyber Security Council, Cyber security guide for boardroom members, 2015. www.cybersecurityraad.nl/binaries/Cybersecurity_Guide%20UK_vdef_tcm56-79492.pdf.
- www.veiliginternetten.nl.

2. DOES MY BUSINESS HAVE DUTIES OF CARE IN THE FIELD OF CYBER SECURITY?

Every business that uses ICT has duties of care in the field of cyber security. This includes businesses where ICT only plays a supporting role.

Even if you 'don't do anything specific' with computers and 'only' use them in your operations, you still have a duty of care to protect your systems. The following example makes this clear.

Duties of care in practice

A distribution centre specialises in the storage, packaging and distribution of magazines. It obtains these magazines from the publisher and delivers them to retailers or delivery companies. The director thinks that he doesn't need to bother with cyber security because the company doesn't work specifically with computers. The director is wrong. The company has several employees and processes the personal data of these employees. In addition, to enable it to package the magazines, it holds a list of the names and addresses of subscribers (Chapter 3). The company also uses computers to keep track of incoming, outgoing and stored magazines. If it was hacked, the company could lose this overview, which would cause a delay in the delivery of the magazines, for which the company would be liable (Chapter 4). Furthermore, a hack could result in personal data being stolen, which may require the company to report the incident to the Data Protection Authority.

Your business may be subject to duties of care for a number of different reasons:

1. Your business processes personal data using ICT (Chapter 3).
2. Your business uses ICT in its operations (Chapter 4).
3. Your business develops, manufactures or supplies products or services that include an ICT component (Chapter 5).

Stringent duties of care in respect of consumers

Your business has duties of care not only in respect of other businesses but also in respect of consumers. These duties of care are essentially the same. Although the obligations in respect of consumers are generally more stringent. Moreover, in the case of consumers, your business has less freedom to form a contract about the obligations in the field of cyber security and to exclude liability. There is more room for this when doing business with another company.

A manufacturer of autonomous cars knows that there is a risk that the sensors on the car won't work in certain instances. The driver must therefore remain on his guard. The manufacturer draws up agreements with taxi firms to ensure that they give their drivers adequate instruction. The inclusion of a contractual provision of this type in agreements with consumers is inadequate. The manufacturer knows that consumers will not read such terms and conditions in detail. They must therefore take additional steps to ensure that consumers are given adequate warning in this regard.

3. DUTIES OF CARE DERIVING FROM THE PROCESSING OF PERSONAL DATA

If your business processes personal data, it has duties of care in the field of cyber security. Personal data is data that relates to an individual, the 'data subject'. It is sufficient that the data subject can be identified from the data in your business.

Data that enables a data subject, e.g. your customer, to be directly identified includes their name and address details. However, data that allows a person to be identified indirectly, when the use of data that could ultimately allow a person's identity to be determined, such as (in many cases) an IP address or a passport number is also personal data. It is also sufficient that a person can be 'recognised' in a group (i.e. can be distinguished from others), even if a link cannot be made to the unique identity of that individual. An example of this is a cookie, whereby the website owner can recognise the visitor but can't relate them to name and address details or other identifying data.

Data protection

Personal data is generally processed using ICT. It is almost always (also) stored in digital form. If your company processes personal data, it has duties of care under the Data Protection Act (WBP). The General Data Protection Regulation (GDPR) includes additional obligations in this regard. It will enter into force on 25 May 2018, at which point the WBP will lapse. In particular, the regulations will require your business to take appropriate technical and organisational security measures, including effective cyber security measures.

Examples of personal data include information on gender, sexual orientation, religion, age, name, marital status, family, state of health or profession, (email) addresses, telephone numbers, fingerprints, IP addresses, cookies, the value of a house and behavioural data derived from the use of ICT products and services.

The introduction of the GDPR will not result in any major changes in terms of the duties of care in the field of cyber security. Under the GDPR, a number of obligations that previously only applied to the controller, including security obligations, will also apply directly to processors. Data processors process personal data exclusively for a data controller, e.g. cloud providers. In addition, the GDPR sets forth a number of duties of care, such as the obligation to incorporate privacy-by-design (and security-by-design). This means, for example, that, wherever possible, data must be pseudonymised, in order to prevent damage in the event of loss or theft.

Mandatory compensation

The terms 'personal data' and 'processing' are interpreted broadly. Consequently, virtually every business processes personal data. Your business doesn't have to be using the data in a particular way in its operations. Even if your business simply keeps a list of data relating to your customers or employees, it processes personal data. All operations or activities relating to personal data constitute processing. The collection or storage of data is processing. Other examples include recording, ordering, updating, amending, consulting, disseminating, deleting or disposing of data.

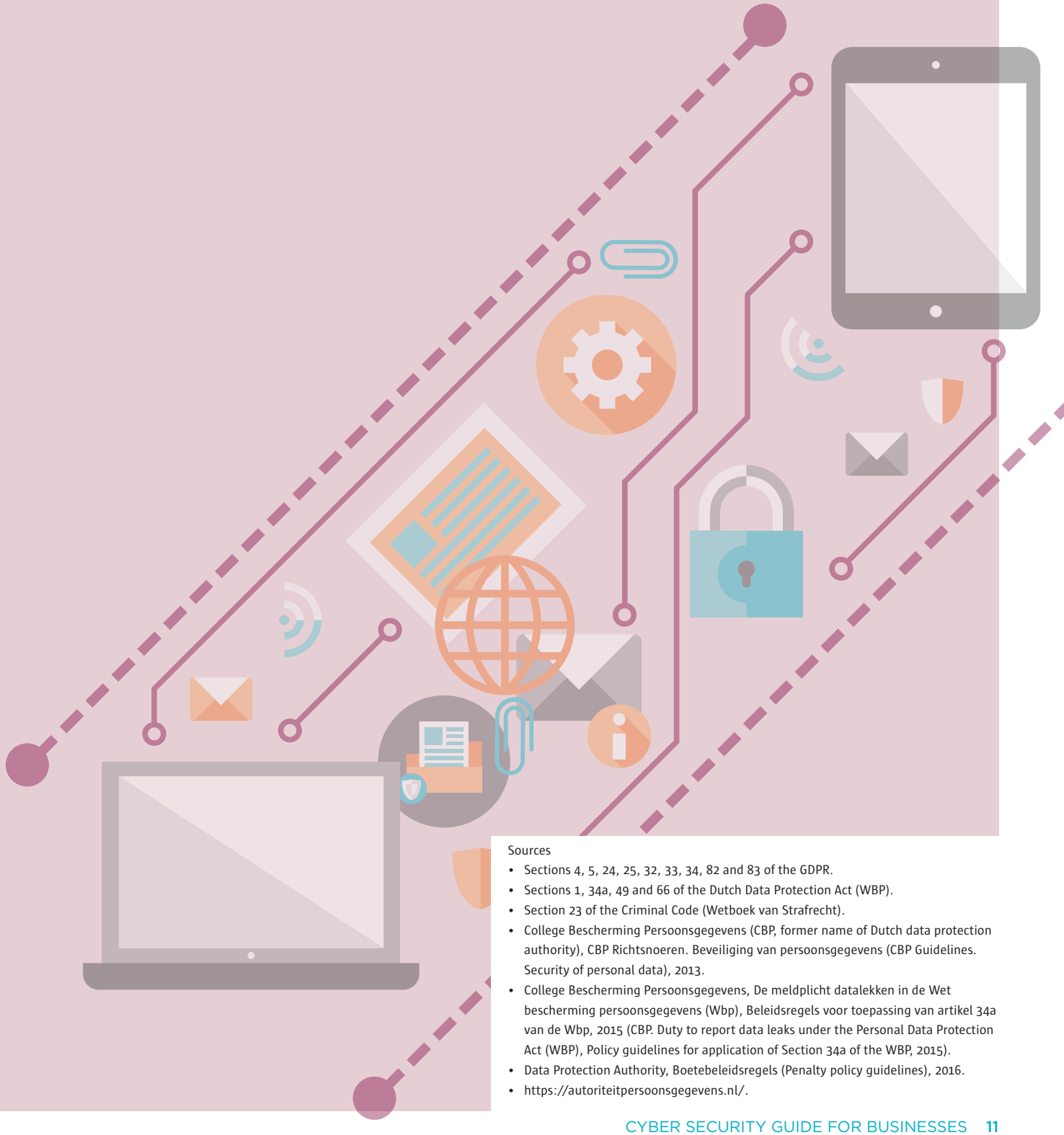
Failure to comply with the security obligations has major consequences. The Data Protection Authority (*Autoriteit Persoonsgegevens*) is the Dutch data protection regulator. It can impose a fine of up to €820,000 per violation or 10% of the annual turnover. Once the GDPR comes into force, the maximum penalty will be €10,000,000 or 2% of the company's global turnover. Your business may also be required to pay compensation for any damage caused by your failure to comply with the obligations.

Fulfilment of duties of care

The Data Protection Authority has published a number of policy guidelines that elaborate on the various duties of care. These policy guidelines offer general guidance on fulfilment of the duties of care, as well as specific obligations in specific situations. This guidance does not consider the specific duties of care in the field of personal data protection in detail. A number of key duties are outlined below:

- Your business must take cyber security into account before it starts to process personal data (privacy-by-design, including security-by-design).
- Your business must carry out a risk analysis before it starts to process personal data. If there are major risks for the data subjects concerned, your business must carry out a privacy impact assessment.
- Your business must only collect and store necessary data (data minimisation).
- Your business must keep the dissemination of and access to personal data to a minimum.
- If a third party processes personal data on your business' behalf, you must conclude an agreement with that party. Amongst others, this agreement must require the third party to take security measures.
- Your business must take appropriate technical and organisational security measures.
- Your business must regularly check that the measures taken are still adequate.
- Your business must have an effective procedure for reporting, resolving and following up security incidents.
- Your business must report breaches involving personal data (data leaks) to the Data Protection Authority (Autoriteit Persoonsgegevens) within 72 hours. If there is a high risk that the data breach will have adverse consequences for the data subjects concerned, your business must also notify the data subjects of the breach.

- Following a data breach, your business must take measures to limit the impact of the breach and to prevent similar breaches from occurring in the future.
- Your business must keep a record of the security measures that it takes.
- Your business must document its processing of personal data.
- If your business collaborates with third parties when processing personal data, you must ensure that these parties also fulfil the duties of care in the field of cyber security. For this purpose, your business must conclude an agreement with such parties.



Sources

- Sections 4, 5, 24, 25, 32, 33, 34, 82 and 83 of the GDPR.
- Sections 1, 34a, 49 and 66 of the Dutch Data Protection Act (WBP).
- Section 23 of the Criminal Code (Wetboek van Strafrecht).
- College Bescherming Persoonsgegevens (CBP, former name of Dutch data protection authority), CBP Richtsnoeren. Beveiliging van persoonsgegevens (CBP Guidelines. Security of personal data), 2013.
- College Bescherming Persoonsgegevens, De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp), Beleidsregels voor toepassing van artikel 34a van de Wbp, 2015 (CBP. Duty to report data leaks under the Personal Data Protection Act (WBP), Policy guidelines for application of Section 34a of the WBP, 2015).
- Data Protection Authority, Boetebeleidsregels (Penalty policy guidelines), 2016.
- https://autoriteitpersoonsgegevens.nl/.

4. DUTIES OF CARE DERIVING FROM THE USE OF ICT

Your business is responsible for the ICT that it uses. The same applies even if your ICT plays only a supporting role within your business or if you haven't actually developed the ICT yourself. This can put you in a difficult position: on the one hand your business doesn't have the expertise to guarantee that the ICT is secure but, on the other hand, a security incident could seriously disrupt your operations.

You can specify in a contract that your business is not liable for any failings in the cyber security of the ICT that you use. For example, your business can stipulate that it will not pay compensation or that it will only pay a limited amount of compensation if it is late in fulfilling its contractual obligations as a result of a problem with its ICT. However, most business partners will only agree to this if you guarantee in turn that you have adequately protected your ICT systems.

Clear agreements

It is advisable to ensure that any agreements relating to cyber security are clearly formulated. Where such agreements are vague, there is a real risk that, in the event of a dispute, the court will interpret the provisions to the detriment of your business. Say, for example, that your business specifies in the agreement that it is not liable if a 'cyber attack' causes a delay in the fulfilment of its obligations. If this term is not specified in more detail, there may be a dispute over whether a particular type of malware constitutes a cyber attack.

The opportunities for making agreements are particularly limited if the other party is a 'consumer'. A provision of the general terms and conditions of a contract has no legal effect ('is voidable') if it is highly detrimental ('unreasonably onerous') for the consumer. A clause that stipulates that your business has no or limited obligations in the field of cyber security is probably unreasonably onerous.

Moreover, any agreements that you have made apply only to the party with whom the agreement has been concluded.

Out-of-date software

Your business cannot exclude every obligation. It will, for example, be liable if, with the knowledge of its management, it deliberately ('intentionally or through deliberate recklessness') uses ICT with highly inadequate cyber security. A business that wittingly uses out-of-date software and takes no measures to protect its computers and networks is unlikely to be able to invoke a clause that excludes liability should such poor security result in damage.

Sources: see page 17

Cyber security of your trading partners

Your business is also dependent on the cyber security of other companies in the supply chain. If you are dependent on other parties in the supply chain, you will not be able to meet your customers' requirements if a security incident prevents your supplier from fulfilling its obligations towards you. This applies in particular if your trading partners have control over your business information or personal data that you need to run your business. It is essential therefore that you conclude agreements around cyber security with your trading partners. After all, a chain is only as strong as its weakest link.

- Your business must conclude agreements about cyber security with other companies in the chain.

Know your risks

It's important to be aware of the risks associated with the ICT that is used by your business. What security incidents could occur if your cyber security is inadequate? How great is the risk of these incidents occurring? To what extent would they affect the reputation and operations of your business? How significant would the impact be if your ICT was temporarily unavailable or if confidential information was leaked? Would the incidents also cause damage to other companies or to consumers? Is your business liable for this? To what extent is it practical and financially viable to minimise risks? Based on the answers to these questions, your business must establish what requirements must be placed on the cyber security of the ICT that it uses.

Investing in cyber security costs money, but it also leads to economic benefits. An increase in the availability, integrity and reliability of your ICT increases the efficiency of your operations and avoids you being held liable and damaging your reputation. From a practical and financial perspective however, it is not possible to make your business 100% secure. So, when defining your cyber security requirements, you will have to weigh the costs against the benefits.

- Your business must be aware of the risks associated with the use of its ICT.
- Your business must establish which risks are acceptable on the basis of a cost-benefit analysis.
- Your business must set aside a budget for cyber security. When defining this budget, you must take the identified risks into account.

Consider duties of care in advance

Before purchasing or using new ICT products or services, you must establish whether the ICT offers the level of cyber security that your business requires. It's also important to conclude clear agreements with the companies from which you are purchasing the product or service. What level of service would your business be offered in the event of a fault? What are your rights if, in spite of this service, the ICT were to be temporarily unavailable? For how long are you entitled to security patches? Most ICT providers will exclude liability for cyber security failings in the contract that you sign with them. Make sure you discuss this during the negotiation process.

Access to a company's ICT network is protected by two-factor authentication. Users can only log in if they have a physical token and a password. After the developer is hacked, all the tokens are replaced. This means that the company can't use the system for a while, which causes over a million euros in damages. The developer supplies new tokens but refuses to pay compensation. The contract contains complex, detailed guarantees. But it also contains a clause that excludes the right to compensation.

- Before your business starts using new ICT, it must establish whether the cyber security of this ICT meets your requirements.
- Your business must conclude clear agreements with the suppliers of the ICT that you use.

Protecting your ICT

When bringing ICT into service, it is essential to take technical and organisational measures to safeguard cyber security. These measures must protect against both remote security incidents ('via the internet') and physical breaches. For example, your business must also take steps to ensure that its ICT is used in a secure manner.

Following a zero-day attack, the software developer immediately releases a security patch. But the business doesn't install this patch for a month, leaving itself vulnerable as a result.

It is important to restrict access to your ICT. A two-factor authentication is recommended. A combination of username and password is not always adequate.

With two-factor authentication, users are only granted access to the ICT if they meet several conditions. For example, access is protected by a physical factor ('something the user owns', e.g. a debit card), combined with a mental factor ('something the user knows', e.g. a password or PIN number).

If passwords are used, they must be sufficiently complex. Dates of birth, '123456789' and the user's name are unacceptable and must not be possible. Moreover, the password that employees use to access important confidential business information or ICT must not be the same as the password that they use at home. In addition, employees must not leave their password lying around, e.g. by writing it on a piece of paper and sticking it on their computer.

For further information on the safe use of passwords, see also the Use two-factor authentication factsheet produced by the Dutch National Cyber Security Centre, 2015.

When taking security measures, your business doesn't need to reinvent the wheel. You can use security standards, codes of conduct or certification mechanisms that apply to your situation.

New security standards, codes of conduct and certification mechanisms are introduced on a regular basis. And existing regulations are often updated.
You should therefore check on an ongoing basis whether new regulations have been published for your field.

An example of a 'general' security standard is the ISO's NEN-ISO/IEC 27002:2013+C2:2015 nl. This standard contains a great deal of relevant information, but since it is general in nature and technology neutral it provides only limited guidance on specific measures. Specific security standards often require more specific measures to be taken.

The Payment Card Industry Data Security Standard sets out a number of different requirements for the processing of credit card payments.

The white paper 'Beveiligingsrichtlijnen voor mobiele apparaten' (Security guidelines for mobile devices) contains several guidelines on the secure use of mobile devices. For example, it recommends the use of tracking software and making regular backups.

- Your business must implement technical and organisational security measures.
- Your business must take measures to protect its ICT against viruses and malware.
- Your business must have a system for ensuring that security patches are implemented quickly and on a regular basis.
- Your business must have regulations in place to ensure that its ICT is used securely.
- Your business must secure its physical ICT and data carriers against theft.
- Your business must protect access to its ICT at minimum by means of a password and preferably through two-factor authentication.
- Your business must comply with relevant security standards, codes of conduct or certification mechanisms.
- Your business must document how its ICT has been protected.

Sources: see page 17

Monitoring your security

ICT is changing all the time and hackers are constantly devising new ways of gaining unauthorised access to your information. Cyber security must therefore be monitored on an ongoing basis. It could be that the ICT used by your business is no longer adequately protected. You must also check that the security measures are being applied consistently. It is advisable to have your security checked regularly by an external party and to take any advice that you are offered in this regard.

More practical examples

You own a construction company and you work with a number of subcontractors. Your main subcontractor has stored the project documentation in the cloud of a cloud storage provider. The cloud storage provider is affected by a security incident. As a result, the subcontractor can't access the documentation, which results in a delay in the implementation of the project.

*A manufacturer of bicycle components is affected by **ransomware**. As a result, it is temporarily unable to access the designs for a component of a new bicycle. Consequently, the bicycle cannot be brought into production. It is unlikely that the manufacturer will be able to use the ransomware attack as an excuse with its customers because, in principle, this is not a force majeure situation.*

*A web shop uses drones developed by another company to deliver its products. Before the customer orders a product in the web shop he must promise not to hold the web shop liable if a drone causes damage during delivery. Due to a **security breach** the drone falls on a car. The owner of the car claims against the web shop. The web shop can't rely on the agreement made with the customer. Nor can it use the argument that it is not the shop but the developer of the drones that is liable for the accident.*

*A major bank regularly manages mergers of listed companies. In this context, it uses the services of an international law firm. Following a security incident at the law firm, **hackers** are able to trade on the stock market with inside information. As a result, the bank has to announce the merger negotiations early.*

*A company plans to purchase remote-controlled factory doors. Before it buys the doors and the associated software, it realises that the **cyber security is inadequate**. The company agrees with the developer that it will improve the level of security. It will not buy and pay for the doors unless the developer does so.*

*A **hacker** is unable to gain control over remotely operated locks via the internet. He can't bypass the **two-factor authentication** that has been implemented without a physical token. So the hacker goes to the building from which the locks are controlled. He goes into the building and steals a token from an experienced employee. Contrary to company regulations, this employee had left the token on a workstation.*

*A company that sends important confidential information by email opts for an email programme that supports strong **end-to-end encryption**. In order to be able to use this strong method of encryption, digital certificates must be exchanged. In practice however, users don't do this. As a result, the encryption is not used.*

*A thief breaks into the house of a public prosecutor. He steals their work telephone and a **USB stick**. The work telephone has been well secured. It is not possible to gain access to it without the public prosecutor's PIN number and fingerprint. The USB stick on the other hand has not been properly secured: information on a narcotics case has been stored without being encrypted.*

*A programming error in OpenSSL known as **Heartbleed** makes a large number of websites vulnerable. As soon as it hears about the error, a clothing company checks whether its web shop is vulnerable by contacting the developer of its website.*

*After a hacker manages to steal the token required for **two-factor authentication** during office hours, the company implements a number of measures. For a while, everyone is on their guard. After a few months however, employees once again start to leave their **tokens** on their desks.*

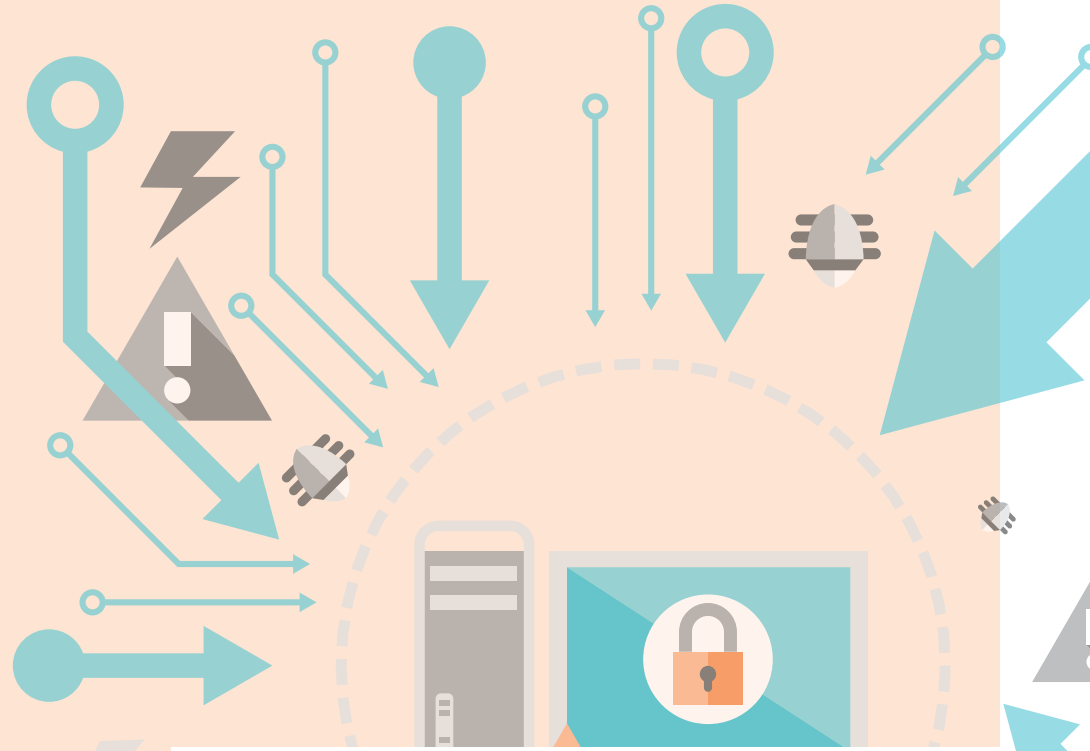
- Your business must check that its cyber security is still adequate, or arrange for a third party to do so.
- Your business must check for the occurrence of security incidents, or arrange for a third party to do so.
- Your business must check that the measures taken have been consistently implemented and are being complied with, or arrange for a third party to do so.

Sources: see below

Measures in the event of a security incident

There is always a risk that, in spite of the measures taken, a security incident will occur. In that case, your business must take steps to limit the impact of the incident and to prevent further incidents from occurring.

- Following an incident, your business must investigate the incident, how it was able to occur and the severity of its consequences.
- Your business must document security incidents.
- Your business must take steps without delay to resolve the incident and to prevent or limit (further) negative consequences.
- Your business must find out whether you need to report the security incident, e.g. because you are required to do so under the terms of an agreement or because personal data (Chapter 3) has been leaked.
- Following an incident, your business must take steps to prevent similar incidents occurring in the future.



Sources ***Verouderde software***:
- Sections 6:75, 173, 233 and 248 of the Dutch Civil Code.

Sources ***Protecting your ICT***:
- Dutch National Cyber Security Centre, Beveiligingsrichtlijnen voor mobiele apparaten (Security guidelines for mobile devices), 2012.
- NEN-ISO/IEC, Information technology— Security techniques — Code of practice for information security controls (ISO/IEC 27002), 2013.
- Dutch National Cyber Security Centre, Factsheet - Use two-factor authentication, 2015.
- PCI Security Standards Council, Payment Card Industry Data Security Standard, 2016.
- www.forumstandaardisatie.nl/open-standaarden/lijsten-met-open-standaarden/.

Sources ***Monitoring your security***:
- Netherlands Bureau for Economic Policy Analysis (CPB) (in conjunction with the Dutch National Cyber Security Centre), Cyber Security Risk Assessment for the Economy, 2016, p. 17.

5. DUTIES OF CARE RELATING TO PRODUCTS OR SERVICES WITH AN ICT APPLICATION

If your business develops, manufactures or supplies a product or service with an ICT application, it must vouch for the cyber security of the ICT. This obligation is based on various principles and applies whatever your position in the supply chain.

Products and services with an ICT application include, amongst others, websites, software, operating systems, firmware, applications, cloud services and physical products with an ICT component. Physical products with an ICT component include, for example, laptops and mobile phones, as well as devices that are connected to the Internet of Things: everyday appliances with an ICT component. An example of such an appliance is a toothbrush that tells you how well you are cleaning your teeth.

Seller's obligations

If your business sells products or services with an ICT application, it must provide the buyer with a product that complies with the terms of the agreement (conformity). Amongst others, this means that the ICT must have the qualities that the buyer would expect and that are necessary for normal use. Cyber security may be regarded as such a quality. A buyer would, for example, expect a mobile phone or a key that can unlock a car remotely to have a basic level of protection against hacking. So, you don't have to guarantee that the product is 100% secure under all circumstances but it must be 'secure enough' to be used in the normal way. If the product doesn't have this level of security, the buyer is entitled to have it repaired or replaced. Consumers are also entitled to a reduction in price, compensation and cancellation of the purchase.

There must be no known security leaks at the time of the sale. It is not necessary to guarantee that vulnerabilities will not come to light subsequently. In this instance, whether or not the buyer can expect that the security of the product will be updated within a reasonable period of time, through a security patch, for example, will depend on the circumstances, including the intended life of the product.

In a European context, a Directive on the delivery of digital content, which makes it clear that security, accessibility and continuity come under the conformity requirement, is currently being drawn up. The proposal also clarifies that conformity includes updates (including security patches).

- The product must be 'secure enough' to be used in the normal way.

Sources: see page 24

Obligations relating to the provision of information

Your business must not give the purchaser of the product or service unrealistic expectations. You must not state or imply that the cyber security of your product or service is greater than it actually is. This applies both when marketing the product, during negotiations and in the purchase agreement itself. In some cases, you must even actively warn the purchaser that the cyber security of a product is less strong than they might expect or that security-related support for a particular product is shortly to be withdrawn. This applies in particular if you are selling the product or service to a consumer. You must not withhold important information relating to cyber security or provide such information in an unclear, obscure or ambiguous way.

Before a consumer purchases a mobile phone he must be notified of the period during which the manufacturer will continue to provide security updates. He must also be told under what circumstances he is entitled to a security patch.

- The purchase agreement, negotiations and marketing must create realistic expectations. They must not state or suggest that the level of cyber security is greater than it actually is or that support for a product will be provided for longer than is actually the case.
- The business must warn the customer if the level of cyber security is lower than the customer might expect or if support for a particular product is shortly to be withdrawn.

Sources: see page 24

Contractual agreements

Your business can conclude agreements concerning the cyber security of the products or services with an ICT application that it delivers. You cannot however exclude every obligation. For the limitations of contractual agreements, see Chapter 4.

- Purchase agreements with other companies must contain provisions that specify in detail the parties' rights and obligations in the field of cyber security.

Cyber security in the supply chain

The fact that your business doesn't develop the products itself does not exempt you from liability in respect of your customers. You are recommended to conclude clear agreements with your suppliers in this regard. How will you cooperate with each other if an end user claims that there is an issue with a product's cyber security? Who is ultimately responsible? You can include a clause in the purchase agreement which states that your business is not responsible or liable for the (inadequate) cyber security of the product sold. However, this clause will only be binding if you sell the product to another company. You cannot limit the conformity requirement if the product is sold to a consumer, either directly or through a reseller.

- Your business must conclude agreements with its suppliers and intermediaries. These agreements must specify the obligations in the field of cyber security and must assign responsibility in the event of an issue with the security of a product or service.

Other agreements
The conformity requirement only applies to purchase agreements. However, other agreements also require your business to take the interests of the other party into account. This may include duties of care in the field of cyber security. These obligations are essentially the same as the obligations that derive from a purchase agreement. In other words, your business will still be subject to the aforementioned duties of care even if it supplies ICT under the terms of an agreement other than a purchase agreement.

Sources: see page 24

A contract to develop a customised Software-as-a-Service solution is generally regarded as a 'service provision' agreement, and, as a result, the developer must act as a 'prudent service provider'. In addition, all agreements require the parties concerned to act with 'reasonableness and fairness'.

Liability in respect of third parties
The cyber security of the products and services that you provide is crucial for your customers. But they are not the only ones that are affected by it. In some cases, third parties with whom your business has not concluded an agreement may also be affected by the cyber security of your products and services. In that case, the duties of care also apply in respect of such third parties.

It is therefore important to establish who is affected by the cyber security of your product or service. Is it just the parties that you do business with? Or is the product or service also resold? Does the availability, integrity or reliability of the product or service only affect the user? Or could poor cyber security also cause damage to other parties?

You must also establish the extent of the risks associated with the products or services that your business provides. The extent of the risks is determined firstly by the likelihood of a security incident occurring and, secondly, by the impact of a security incident. Even if the likelihood of an incident occurring is limited, the risks can be significant. This applies in particular if the consequences of the incident could be substantial, e.g. because there is a risk of 'physical' damage or bodily injury. It is also important to establish whether and to what extent it is practical and financially viable to minimise the risks. Based on this analysis, your business should determine what requirements it must place on the cyber security of its products or services. The greater the risk, the more stringent the cyber security requirements.

You cannot agree with the injured party that your business is not liable because your business has not concluded a contract with that party. You can however conclude agreements with another party, e.g. the purchaser or user of your product or service. However, this does not exempt your business from its obligations in respect of the injured party.

For the limitations of contractual agreements, see Chapter 4.

- Your business must establish who is affected by the cyber security of the products and services with an ICT application that it develops and supplies.
- Your business must be aware of the risks associated with a defect in the cyber security of its products or services.
- Your business must establish on the basis of a cost-benefit analysis which risks associated with its products or services are acceptable.
- Your business must conclude agreements with parties upon whom the cyber security of its products and services is in part dependent. These agreements must specify the obligations in the field of cyber security and must assign responsibility in the event of an issue with the security of a product or service.

Sources: see page 24

Security of products or services with an ICT application

Your business must ensure that the products or services that you have developed have adequate cyber security. This duty of care can only be properly fulfilled if cyber security is taken into consideration at an early stage. Although it is not necessary for a product's cyber security to be in order in every phase of the project, the product must ultimately be adequately protected. You can help ensure that this is the case by creating a climate that encourages the development of a properly protected product, even if this delays development or results in additional costs.

In the case of agile development, the software is regularly adapted to changing requirements. In this context, it is often not possible to determine in advance what the ultimate security requirements will be. But the developer can still bear in mind that it must be possible to modify the cyber security at a later stage.

Your business can enhance the cyber security of the product or service by implementing security mechanisms. The measures required will vary according to the ICT application concerned.

A website recognises DDoS attacks and 'filters' them out. As a result, the website remains online.

When implementing security mechanisms your business can use security standards, codes of conduct or certification mechanisms that apply to your product or service.

The cyber security of a product or service can also be enhanced by making it difficult to modify the ICT or disable the security. If, in spite of this, the ICT is modified, this will be logged automatically. It may also be necessary to protect the product or the production process against 'physical' breaches.

Access to a factory for autonomous cars is protected by an alarm and a security guard. Employees need a pass to enter the premises. The software is also programmed in such a way that minor changes to the sensors mean that the autonomous mode can no longer be used.

More practical examples

Due to a security leak in a computer program, a hacker can easily gain control of a user's computer. This breach is common knowledge. If the seller sells this product despite being aware of this security issue, it cannot rely on a clause that excludes liability. This applies in particular if the customer is not made aware of the security link and could therefore not take steps to limit the damage.

A major web shop sells mobile phones to consumers. It doesn't make the phones itself however, so it doesn't have any influence over their cyber security. Consumers can however claim against the web shop if the phones are found to be insecure. The web shop agrees with the manufacturer that, in this event, the manufacturer will improve the cyber security of the phones and cover the costs involved. If the manufacturer refuses to agree to this, the shop will stop selling the phones.

A company develops 'smart' thermostats. It sells these thermostats to energy companies, which give them to their customers. The company has not concluded agreements with the energy companies' customers but it must still provide these customers with an adequate level of cyber security.

A company develops and sells software that allows the user to collect and manage personal data online. If, as a result of a security breach, a hacker gains access to the collected data, this is detrimental not only to the user of the software but also to the data subjects whose personal data has been leaked. The company can agree with the users of the software that they will cover the costs of a data leak. But this does not exempt the company from its duties of care in respect of the data subjects.

A company agrees with users of the software that they will always report hacks. This information allows the company to rectify any issues with the cyber security. The contract also stipulates that users must always install security updates for the software. This prevents further data leaks.

A company develops a 'smart' electricity meter. This device measures the energy consumption of various household appliances and transmits the results to a central server. This allows the company to predict where and when additional energy capacity is required. In order to protect the privacy of its clients, the company bore in mind at the development stage that the meter must have sufficient capacity to send the data in encrypted form. That way, anyone intercepting the signals from the energy meter can't see how much electricity the customer has used. However, the company has not thought the cyber security of the electricity meter through properly. If a person is not at home, data will be forwarded far less frequently.
This information may be of interest to burglars. When an employee attempted to raise this issue during development of the device, he was overruled by management.

The developer of a mobile phone requires users to set up a PIN number. The device is blocked if a person enters an incorrect code too many times in succession.

The developer and website hosting provider ensure that a client's website is quickly back online following a DDoS attack. Further investigation reveals that the website was not properly protected and, as a result, was vulnerable to such an attack. In principle, the developer is liable. Since the website was quickly brought back online, the damage caused by the attack was less significant than anticipated.

A computer program appears to be vulnerable to a new virus. The risk can easily be avoided however by not using a particular function. The developer notifies users and temporarily blocks the function concerned. In the meantime, it works on a security patch.

A manufacturer of autonomous cars knows that the sensors don't work properly in certain weather conditions. However, since it is concerned about the damage it might cause to its reputation, it doesn't make this defect public. The manufacturer expects to be able to rectify the defect within a week. During the course of that week however, a fatal accident occurs. The manufacturer is liable for the damage.

The operating system of a PC has a built-in firewall. If the firewall is disabled, a clearly visible icon appears on the taskbar. The user is also regularly warned that his PC is not properly protected.

Changes to a website require two-factor authentication. Any changes made to the website must also be logged. It must not be possible for this log to be modified by one individual.

- Your business must take cyber security into account at the development stage (security-by-design).
- Your business must encourage the development of properly protected products and services through organisational measures.
- Your product or service must have built-in technical security.
- Your product or service must comply with relevant security standards, codes of conduct or certification mechanisms.
- Your business must take measures to prevent unauthorised modification of the ICT or the disabling of security.
- Your business must log changes to the product or service.
- Your business must document how the product or service has been protected.

Sources: see page 24

Updating your security

Even if your business has taken adequate measures to protect your product or service, the ICT application may no longer be secure at a later date. This may be due to a better understanding of the situation or to developments in technology. Your business must therefore check on a regular basis that its cyber security is still adequate.

A smartphone manufacturer's phones use the Android operating system. An error known as the Stagefright bug is discovered in this system. As a result, the manufacturer's mobile phones are no longer secure

Encryption that involves hashing can be cracked through a brute force attack. An increase in available computer capacity may mean that encryption that was adequate initially is subsequently too easy to crack.

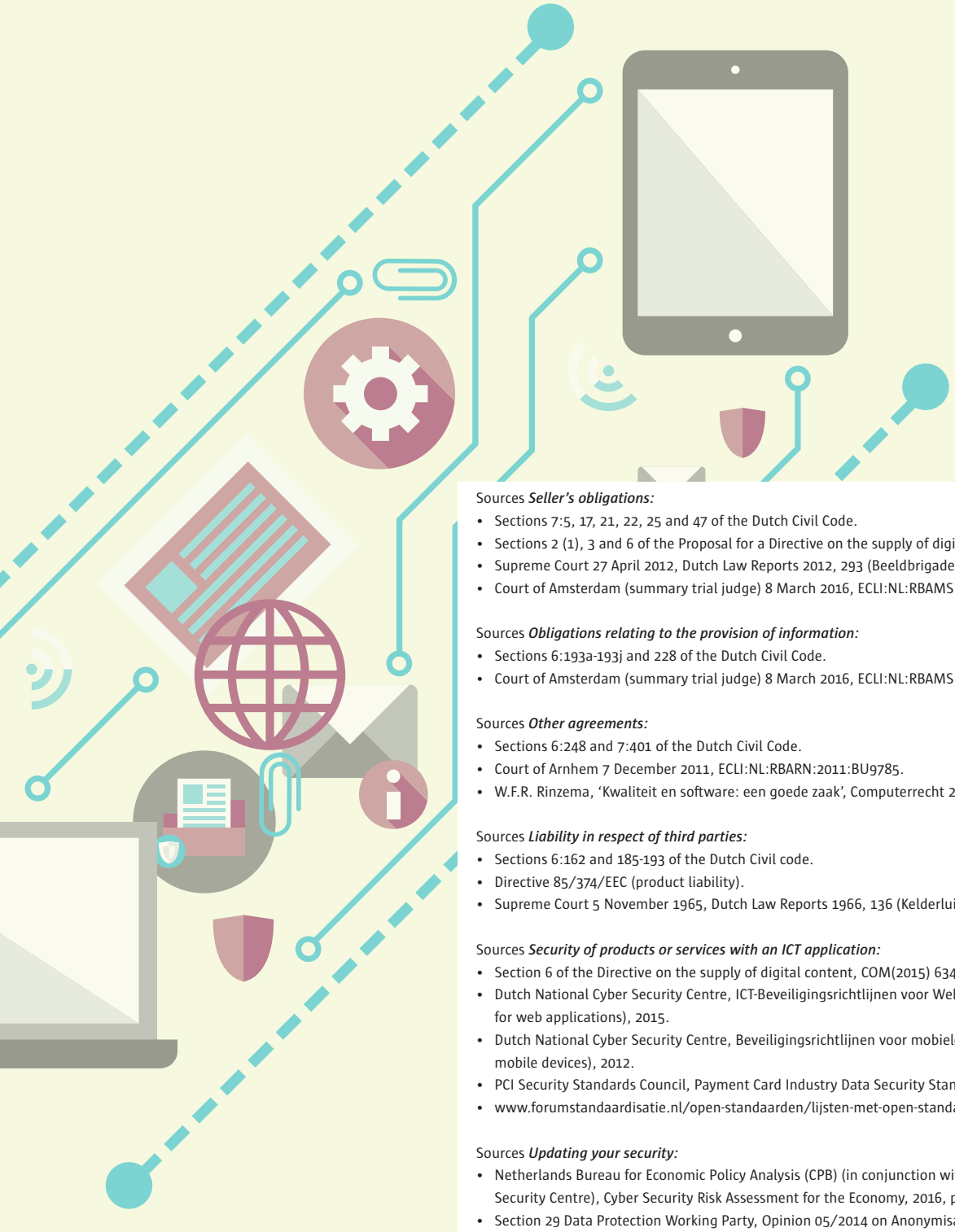
If your business's cyber security is no longer adequate, you must update it so you can deliver secure ICT to new clients. You can also offer existing users support by releasing a security patch. In some cases, you will have to warn users that the level of cyber security is (temporarily) inadequate. This allows users to take steps to minimise the risk of a security incident while you are working on a security patch. In the event of a serious incident, you must also help users limit any damage they incur as a result in a suitable way.

Your security can be updated more quickly if your business encourages users to report security incidents relating to your product or service. You can use these incidents to assess whether, and if so how, your cyber security should be updated.

When software is restarted after a crash, the user sees a pop-up asking him to send a report on the crash to the developer.

- Your business must check the cyber security of the product or service on a regular basis.
- Your business must update the cyber security of a product or service for a specific period of time if it is no longer adequate.
- Your business must use a system to ensure that security patches are installed by users.
- Your business must encourage users to report security incidents. Such incidents must be investigated. You must take measures to prevent similar incidents occurring in the future.
- Your business must offer users support in the event of a security incident.
- Users must be warned (it must be possible to warn users) if the level of cyber security is inadequate.

Sources: see below



Sources ***Seller's obligations:***
- Sections 7:5, 17, 21, 22, 25 and 47 of the Dutch Civil Code.
- Sections 2 (1), 3 and 6 of the Proposal for a Directive on the supply of digital content, COM(2015) 634 final.
- Supreme Court 27 April 2012, Dutch Law Reports 2012, 293 (Beeldbrigade/Hulskamp).
- Court of Amsterdam (summary trial judge) 8 March 2016, ECLI:NL:RBAMS:2016:1175.

Sources ***Obligations relating to the provision of information:***
- Sections 6:193a-193j and 228 of the Dutch Civil Code.
- Court of Amsterdam (summary trial judge) 8 March 2016, ECLI:NL:RBAMS:2016:1175.

Sources ***Other agreements:***
- Sections 6:248 and 7:401 of the Dutch Civil Code.
- Court of Arnhem 7 December 2011, ECLI:NL:RBARN:2011:BU9785.
- W.F.R. Rinzema, 'Kwaliteit en software: een goede zaak', Computerrecht 2012, p. 104.

Sources ***Liability in respect of third parties:***
- Sections 6:162 and 185-193 of the Dutch Civil code.
- Directive 85/374/EEC (product liability).
- Supreme Court 5 November 1965, Dutch Law Reports 1966, 136 (Kelderluik).

Sources ***Security of products or services with an ICT application:***
- Section 6 of the Directive on the supply of digital content, COM(2015) 634.
- Dutch National Cyber Security Centre, ICT-Beveiligingsrichtlijnen voor Webapplicaties (ICT security guidelines for web applications), 2015.
- Dutch National Cyber Security Centre, Beveiligingsrichtlijnen voor mobiele apparaten (Security guidelines for mobile devices), 2012.
- PCI Security Standards Council, Payment Card Industry Data Security Standard, 2016.
- www.forumstandaardisatie.nl/open-standaarden/lijsten-met-open-standaarden/.

Sources ***Updating your security:***
- Netherlands Bureau for Economic Policy Analysis (CPB) (in conjunction with the Dutch National Cyber Security Centre), Cyber Security Risk Assessment for the Economy, 2016, p. 17.
- Section 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, 2014, p. 20.
- Court of The Hague 11 July 2001, Computerrecht 2001, p. 268.
- Court of Amsterdam (summary trial judge) 8 March 2016, ECLI:NL:RBAMS:2016:1175.

6. WHO IS RESPONSIBLE FOR CYBER SECURITY WITHIN MY BUSINESS?

Cyber security is the responsibility of the board of directors. In smaller businesses, responsibility lies with the director.

The board of directors or the director must ensure that the ICT that the business uses contributes to effective operations. It is also responsible for managing any risks associated with the use of ICT and for compliance with the duties of care in the field of cyber security. The director with special responsibility for ICT, the Chief Information Officer (CIO), will take the lead. The board of directors and the CIO will be assisted in the performance of these tasks by an internal ICT auditor.

The supervisory board will oversee the board of directors. If the board of directors fails to pay sufficient attention to cyber security, the supervisory board must draw this oversight to the board of directors' attention. The audit committee will play a key role in audit activities: it is responsible for oversight of risk management and compliance with the relevant regulations. It must also monitor risks and regulations relating to cyber security.

Your business may not have a CIO, an internal ICT auditor or a supervisory board, but the division of responsibility remains the same: the board of directors is ultimately responsible for cyber security. If the board of directors does not have sufficient expertise in the field of cyber security, it is recommended that the help of an ICT consultant be enlisted.

Sources: see page 26

A company works with digital personal data and other confidential information on a regular basis. In order to ensure that this information is kept confidential, employees must lock their computers whenever they leave their desks. These rules are made clear to all new employees. If an employee leaves his computer unlocked, he will be taken to task.

The role of employees

A high level of cyber security can only be achieved if its importance is embedded throughout the organisation. You must take organisational measures to ensure that this is the case.

- Your business must draw up policy guidelines or protocols relating to cyber security. You must distribute these policy guidelines to employees and update them where necessary. You must monitor compliance with these guidelines.
- Your business must inform and train any employees who are involved with ICT. The scope and nature of this training must be tailored to the employee's role and responsibilities.
- It must be clear who is responsible for security within your business and who the contact is for queries relating to security and the reporting of security incidents.
- Employees must know to whom they can and must report security incidents. They must be encouraged to do so as a matter of course, amongst others by creating a culture of alertness, by making cyber security a topic of discussion and by rewarding employees for reporting a security incident (that they have not deliberately caused themselves). There must be a procedure for reporting incidents.
- Details of these security incidents, how they were resolved and over what time frame must be forwarded to management.

Sources: see below

Sources:

- Principles II.1, III.1, III.5 and V.III Monitoring Committee Corporate Governance Code. De Nederlandse corporate governance code. Beginselen van deugdelijk ondernemingsbestuur en best practice bepalingen (Dutch corporate governance code. Principles of good governance and examples of best practice), 2009.
- Principles 1.2, 1.3, 1.4 and 1.5 Monitoring Committee Corporate Governance Code. Dutch corporate governance code. Proposal for review, 2016.
- Cyber Security Council, Cyber security guide for boardroom members, 2015. www.cybersecurityraad.nl/binaries/Cybersecurity_Guide%20UK_vdef_tcm56-79492.pdf.
- NEN-ISO/IEC, Information technology— Security techniques —Information security Management systems — Requirements (ISO/IEC 27001), 2013.

Sources *The role of employees:*

- NEN-ISO/IEC, Information technology— Security techniques —Information security Management systems — Requirements (ISO/IEC 27001), 2013.
- NEN-ISO/IEC, Information technology— Security techniques — Code of practice for information security controls (ISO/IEC 27002), 2013, amongst others paragraphs 7, 11.2 and 16.1.

SUMMARY

Every business that uses ICT has duties of care in the field of cyber security, even if ICT plays only a supporting role within the business. Poor cyber security can seriously disrupt your business and damage your reputation. And failure to comply with your duties of care can also render you liable. From both a financial and a legal perspective therefore, compliance with these obligations is crucial. Ultimately, this is the responsibility of the board of directors or (in the case of smaller businesses) the director.

This guide offers businesses a measure of guidance on the fulfilment of their duties of care in the field of cyber security. It gives only a brief outline of these duties, however, and should only be used for information purposes and to check your level of compliance. This guide is no substitute for professional advice. If your business is subject to the obligations outlined in this guide, you are advised to engage a specialist lawyer or a security expert.

This summary gives an overview of the main duties of care in the field of cyber security. The obligations are described in more detail in the guide itself.

CYBER SECURITY CHECKLIST

Personal data is information that relates to an individual.
A company that collects or processes this data has various duties of care.

Checklist of duties of care deriving from the processing of personal data (Chapter 3):

- [ ] Your business must take cyber security into account before it starts to process personal data (privacy-by-design, including security-by-design).
- [ ] Your business must carry out a risk analysis before it starts to process personal data. If there are major risks for the data subjects concerned, your business must carry out a privacy impact assessment.
- [ ] Your business must collect and store only necessary data (data minimisation).
- [ ] Your business must keep the dissemination of and access to personal data to a minimum.
- [ ] If a third party processes personal data on your business's behalf, your business must conclude an agreement with that party. Amongst others, this agreement must require the third party to take security measures.
- [ ] Your business must take appropriate technical and organisational security measures.
- [ ] Your business must regularly check that the measures taken are still adequate. Your business must have an effective procedure for reporting, resolving and following up security incidents.
- [ ] Your business must report breaches involving personal data (data leaks) to the Data Protection Authority (Autoriteit Persoonsgegevens) within 72 hours. If there is a high risk that the data breach will have adverse consequences for the data subjects concerned, your business must also notify the data subjects of the breach.
- [ ] Following a data breach, your business must take measures to limit the impact of the breach and to prevent similar breaches from occurring in the future.
- [ ] Your business must keep a record of the security measures that it takes.
- [ ] Your business must document its processing of personal data.
- [ ] If your business collaborates with third parties when processing personal data, you must ensure that these parties also fulfil the duties of care in the field of cyber security. For this purpose, your business must conclude an agreement with such parties.

Your business is responsible for the ICT that it uses. The same applies even if this ICT plays only a supporting role.

Checklist of duties of care deriving from the use of ICT (Chapter 4):

- [ ] Your business must conclude agreements about cyber security with other companies in the chain.
- [ ] Your business must be aware of the risks associated with the use of its ICT.
- [ ] Your business must establish which risks are acceptable on the basis of a cost-benefit analysis.
- [ ] Your business must set aside a budget for cyber security. When defining this budget, you must take the identified risks into account.
- [ ] Before your business starts using new ICT, it must establish whether the cyber security of this ICT meets your requirements.
- [ ] Your business must conclude clear agreements with the suppliers of the ICT that you use.
- [ ] Your business must implement technical and organisational security measures.
- [ ] Your business must take measures to protect its ICT against viruses and malware.
- [ ] Your business must have a system for ensuring that security patches are implemented quickly and on a regular basis.
- [ ] Your business must have regulations in place to ensure that its ICT is used securely.
- [ ] Your business must secure its physical ICT and data carriers against theft.
- [ ] Your business must protect access to its ICT at minimum by means of a password and preferably through a two-factor authentication.
- [ ] Your business must comply with relevant security standards, codes of conduct or certification mechanisms.
- [ ] Your business must document how its ICT has been protected.
- [ ] Your business must check that its cyber security is still adequate, or arrange for a third party to do so.
- [ ] Your business must check for the occurrence of security incidents, or arrange for a third party to do so.
- [ ] Your business must check that the measures taken have been consistently implemented and are being complied with, or arrange for a third party to do so.
- [ ] Following an incident, your business must investigate the incident, how it was able to occur and the severity of its consequences.
- [ ] Your business must document security incidents.
- [ ] Your business must take steps without delay to resolve the incident and to prevent or limit (further) negative consequences.
- [ ] Your business must find out whether you need to report the security incident, e.g. because you are required to do so under the terms of an agreement or because personal data (Chapter 3) has been leaked.
- [ ] Following an incident, your business must take steps to prevent similar incidents occurring in the future.

If your business provides products or services with an ICT application, it must ensure an appropriate level of cyber security.

Checklist of duties of care relating to products or services with an ICT application (Chapter 5):

- [ ] The product must be 'secure enough' for normal use.
- [ ] The purchase agreement, negotiations and marketing must create realistic expectations. They must not state or suggest that the level of cyber security is greater than it actually is or that support for a product will be provided for longer than is actually the case.
- [ ] The business must warn the customer if the level of cyber security is lower than the customer might expect or if support for a particular product is shortly to be withdrawn.
- [ ] Purchase agreements with other companies must contain provisions that specify in detail the parties' rights and obligations in the field of cyber security.
- [ ] Your business must conclude agreements with its suppliers and intermediaries. These agreements must specify the obligations in the field of cyber security and must assign responsibility in the event of an issue with the security of a product or service.
- [ ] Your business must establish who is affected by the cyber security of the products and services with an ICT application that it develops and supplies.
- [ ] Your business must be aware of the risks associated with a defect in the cyber security of its products or services.
- [ ] Your business must establish on the basis of a cost-benefit analysis which risks associated with its products or services are acceptable.
- [ ] Your business must conclude agreements with parties upon whom the cyber security of its products and services is in part dependent. These agreements must specify the obligations in the field of cyber security and must assign responsibility in the event of an issue with the security of a product or service.
- [ ] Your business must take cyber security into account at the development stage (security-by-design).
- [ ] Your business must encourage the development of properly protected products and services through organisational measures.
- [ ] Your product or service must have built-in technical security.
- [ ] Your product or service must comply with relevant security standards, codes of conduct or certification mechanisms.
- [ ] Your business must take measures to prevent unauthorised modification of the ICT or the disabling of security.
- [ ] Your business must log changes to the product or service.
- [ ] Your business must document how the product or service has been protected.
- [ ] Your business must check the cyber security of the product or service on a regular basis.
- [ ] Your business must update the cyber security of a product or service for a specific period of time if it is no longer adequate.
- [ ] Your business must use a system to ensure that security patches are installed by users.
- [ ] Your business must encourage users to report security incidents. Such incidents must be investigated. You must take measures to prevent similar incidents occurring in the future.
- [ ] Your business must offer users support in the event of a security incident.
- [ ] Users must be warned (it must be possible to warn users) if the level of cyber security is inadequate.

All businesses must promote cyber security within their business.

Checklist of duties of care relating to the organisation of your business (Chapter 6):

- [ ] Your business must draw up policy guidelines or protocols relating to cyber security. You must distribute these policy guidelines to employees and update them where necessary. You must monitor compliance with these guidelines.
- [ ] Your business must inform and train any employees who are involved with ICT. The scope and nature of this training must be tailored to the employee's role and responsibilities.
- [ ] It must be clear who is responsible for security within your business and who the contact is for queries relating to security and the reporting of security incidents.
- [ ] Employees must know to whom they can and must report security incidents. They must be encouraged to do so as a matter of course, amongst others by creating a culture of alertness, by making cyber security a topic of discussion and by rewarding employees for reporting a security incident (that they have not deliberately caused themselves). There must be a procedure for reporting incidents.
- [ ] Details of these security incidents, how they were resolved and over what time frame must be forwarded to management.

CSR Cyber Security Council

Colofon

This guide was produced on behalf of the Cyber Security Council by Pieter Wolters and Professor Corjo Jansen from the Business & Law Research Centre, Radboud University.

The authors would like to thank the CSR guidance committee for their valuable comments: Chair Professor Lokke Moerel (Tilburg University, Morrison & Foerster LLP, Cyber Security Council). Members: Liesbeth Holterman (trade association Nederland ICT), Danny ter Laak (Public Prosecutor's Office), Reinout Rinzema (law firm Ventoux Advocaten), Peter van Schelven (law firm BIJ PETER – Wet & Recht), Ronald Verbeek (digitalisation platform CIO Platform Nederland) and Maurice Wessling (Dutch consumers' association Consumentenbond). They would also like to thank Elly van den Heuvel (Cyber Security Council), Eline Attema (Cyber Security Council), Martin Bobeldijk (Cyber Security Council), Myrthe Bronsdijk, Mireille Hildebrandt and Paul Verbruggen for their invaluable support.

Layout: BKB, Printing: Xerox/OBT, Concept and advice: Turnaround Communicatie

Nijmegen, February 2017

www.cybersecurityraad.nl

CSR Cyber Security Council