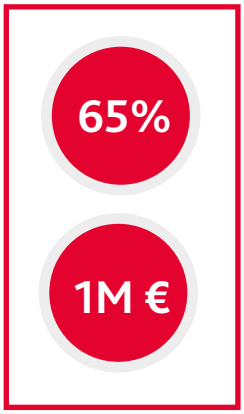
A PRAGMATIC APPROACH TO ENHANCING CYBER SECURITY

BDO

INTRODUCTION

A computer virus paralyses your network, a hacker blocks access to your online shop, phishing gives a hacker access to all your customers' personal data: cyber incidents can completely disrupt your business and cause serious damage.

It is estimated that **65%** of companies were attacked last year, and that when that attack was successful, the damage was considerable, amounting to an average of **1 million euros**. The question is therefore not whether you are going to be attacked, but when you will be attacked and whether you will be ready to respond appropriately.



And then we are only talking about the known cyber attacks: obtaining sensitive information usually remains undetected, hackers deliberately leave behind as few traces as possible. It is doubtful whether incidents of this type are re-veiled by the average SME.

On 25 May 2018, the GDPR (General Data Protection Regulation), the European legislation for the protection of personal data, was added to the mix. Perhaps the proposed fines (up to 4% of turnover) are a deterrent, but the legislation will certainly result in a greater visibility of security incidents with damage to reputation amongst others as a consequence.

Cyber security has recently become one of the top 3 of directors' concerns, so lack of awareness is no longer an excuse. The continuous flow of articles in the press about cyber security incidents makes everyone wonder whether it can also happen in their own organisation and whether adequate security measures have been taken. When this question is asked internally, the answer from IT often remains vague and inadequate: "measures have been taken, but something unexpected can always happen". The result is that only a few managers and directors can rest assured that their organisation is adequately protected against cyber security incidents.

Nevertheless, there is a lot of information and documentation available about cyber security, good examples are the "Cyber security guide for SME" and the "Belgische gids voor Cyberveiligheid / Guide Belge de la cybersécurité " (only available in Dutch and French). However, these documents are rather theoretical and particularly describe the "what" and not the "how": the concrete measures to achieve better cyber security. That is the purpose of this white paper: to indicate what must be done in concrete terms to tackle the main cyber risks that your organisation faces and to offer a pragmatic roadmap to an enhanced cyber resilience.

The following questions will be answered:

- What can be the **impact** of a cyber attack on my company?
- What are the most common types of **cyber attacks** and which vulnerabilities are exploited?
- What **measures** do we need to take and with what priorities should we best approach them?
- How can the **BDO cyber services** be of assistance?

WHAT CAN BE THE IMPACT OF A CYBER ATTACK ON MY COMPANY?

A cyber attack can cause enormous damage to your organisation:

- **Financial.** A cyber attack can lead to direct financial losses, for example a phishing attack that leads to money being transferred to the hacker, but also to indirect financial losses which are caused, on the one hand, by the cost of resolving the incident itself as quickly as possible and, on the other hand, by the potential loss of customers.
- **Operational.** A cyber attack can disrupt computer systems to such an extent that they can no longer support day-to-day business operations. This disruption of business operations will of course also have financial consequences.
- **Reputation.** A cyber incident has a negative impact on the company and can damage a reputation which has been built up carefully over many years in the blink of an eye. This damage to reputation will eventually lead to financial losses due to direct impact on turnover and additional costs incurred in rebuilding the reputation after the incident.

What can happen? The damage caused by a cyber incident can be reduced to the acronym "CIA" (Confidentiality, Integrity and Availability):

- **The confidentiality** of data can be impaired. Concretely: sensitive information can fall into the wrong hands or into the public domain.
- **The integrity** of data can be impaired. Concretely: due to incidents (intentional or unintentional), unauthorized modification of data can occur making it unusable or leading to errors.
- **The availability** of systems and information can be compromised. Concretely: systems can go down and remain unavailable for a long period of time, thus disrupting business operations.

To estimate the potential impact on your own organisation, you need to ask yourself what are the most critical IT assets of the organisation and what can happen to them as a result of a cyber incident. A couple of examples:

In a hospital, the medical patient file is the most critical asset. If unauthorised persons gain access to the medical patient file, the patients could suffer serious damage. Consider, for example, the medical file of a well-known person, which is leaked to the press. Furthermore, it could lead to heavy fines from the Data Protection Authority (GDPR).

In a technology company (e.g. biotech or IT tech), the principal asset is often the company's Intellectual Property (IP). If this was to be stolen, the company's entire competitive advantage could be lost. In this way, many business secrets have already ended up in the wrong hands.

In a production company, the production systems are often the most critical, while in a logistics company it is of course the logistics systems. If these systems go down, it can lead to interruptions of the production lines and the supply chain.

In a retail or B2C company, information about the consumer is very critical, all the more so when profiling of consumer behavior is performed or when payment data is stored.

These are the principle IT assets (systems and information) which need to be secured in order to avoid incidents. And when incidents do happen, good recovery plans and incident response procedures need to be in place to ensure that the impact is reduced. IT is often not fully aware of which systems are the most critical from the business point of view. This exercise should therefore be carried out jointly by business and IT.

WHAT ARE THE MOST COMMON TYPES OF CYBER ATTACKS AND WHICH VULNERABILITIES ARE EXPLOITED?

To know how to protect ourselves, we first need to understand what we need to protect ourselves from. Since most organisations have similar cyber risks, here below we provide an overview of the most common and successful cyber attacks and the vulnerabilities that are being exploited. These vulnerabilities must be addressed by taking appropriate measures. These are outlined in the following section.

Organisations fall victim to cyber attacks every day, but what actually happens? Cyber attacks can take many forms, from phishing and malware to exploiting vulnerabilities and ransomware. The potential threats can be very different, but they all have one thing in common: they all represent a significant business risk.

Malware

Malware is used to force a way into users' computers. Malware refers to many types of malicious software, such as viruses. Malware can do many things, such as take control of your computer, monitor your actions on your computer and steal data. Malware is often distributed via phishing emails, where the attacker asks you to download and open a seemingly harmless file or attachment (.docx, .pdf, etc.) that contains malicious code. The malware will then spread quickly to other computers within the same network and organisation.

Measures: up-to-date anti-virus, advanced "endpoint protection", user awareness, security monitoring.

Ransomware

A specific type of malicious software (malware) that encrypts all your data and makes it inaccessible. When this happens, a sum (ransom) is requested to be paid to decrypt your files (which in the end does not always happen). The most famous versions of ransomware are Cryptolocker and WannaCry. Just as with malware, ransomware is often distributed via phishing emails and will spread quickly to other computers.

Measures: up-to-date anti-virus, advanced "endpoint protection", a detailed backup plan, patch management, anti-spam and anti-phishing solutions, user awareness, security monitoring.

Vulnerabilities and unpatched software

This should be one of your top concerns, because software which is not up-to-date is one of the main cyber threats for an organisation. There are 2 types of vulnerabilities: known and unknown. Known vulnerabilities are published on the internet and there is a good chance that an attacker will know and use them. Unknown vulnerabilities, or zero-day vulnerabilities, are less likely to affect your organisation. Software suppliers periodically provide patches to disable known vulnerabilities. Patches should therefore be installed as quickly as possible in order to reduce the risk of cyber incidents.

Measures: vulnerability assessment, patch management, penetration testing.

Social Engineering

A technique used to mislead and manipulate users in order to gain access to, for instance, their computer, credentials and bank information. Social engineering is a type of psychological manipulation. The attacker will persuade you to undertake a number of actions or to provide information that may seem innocent to you, by pretending to be someone else.
There are many forms of social engineering; phishing emails, invoice fraud, CEO fraud, fake social media profiles, etc.

Measures: user awareness, anti-spam and anti-phishing solutions, website filtering, multi-factor authentication, password management.

Human error

Not all security incidents or data leaks are caused by attackers. In reality, many incidents are caused by human error and could have easily been avoided. A user accidentally sends information to a wrong person or email address, computers and smartphones are lost or stolen, passwords are written on post-its or shared with other colleagues - these are just a few examples. In recent years, human error has represented more than half of the data leaks. In principle, they are easy to avoid, but the reality is that human behavior and habits are the most difficult to influence.

Measures: user awareness, disk encryption (including disks in laptops), password management, identity and access management (IAM), network access rules, application hardening, logging, behavioral monitoring.

(Distributed) Denial of Service

A (D)DoS attack can most easily be explained as a motorway that cannot handle a massive amount of unexpected traffic, causing a traffic jam that nobody can escape from. This is what happens when a website, web shop, login page or service becomes the victim of a (D)DoS attack. If you flood a website with more traffic than it was built for, you will overload the server and make the website unavailable for the purpose for which it is intended. The difference between a DoS and a DDoS attack lies in the number of computers that simultaneously perform the attack.

Measures: adequate network configuration, anti-DDoS service/solution, network monitoring, incident response and management

WHAT ARE THE MOST IMPORTANT MEASURES TO PREVENT CYBER SECURITY INCIDENTS AND HOW SHOULD WE PRIORITISE THEM?

Now that we know what the most common cyber attacks are, we can determine the measures to protect ourselves against them. The problem is that there are many measures to be taken to protect ourselves against a cyber attack. However, we cannot do everything at once and time and resources are limited. Moreover, the cost, complexity and risks covered by the measures can also be considerably different.

This is why we suggest a model with 3 maturity levels: (1) basic, (2) prudent and (3) best practice. This model is based on the generally accepted best practice framework of the Centre of Internet Security (CIS), which allows actions to be prioritised which collectively offer a good protection against the most popular types of cyber attacks. BDO offers a tailored service for each maturity level, which will be explained in the next section.

Good cyber security includes preventive measures, as well as reactive procedures in the event that the preventive measures have proven to be inadequate, so that the damage suffered as a result of the cyber attack can be repaired as quickly as possible and the impact on the organisation is limited.

MATURITY LEVEL 1: BASIC

- **Password management:** strong passwords are the basis for security, and must be compulsory for all users within the organisation. Passwords must be sufficiently long and complex, chosen by the users themselves and regularly changed. After a number of attempts using incorrect passwords, accounts should be temporarily blocked. The importance of strong passwords, which are not to be shared with others, must be made clear to users (see further awareness training).
- **Identity access management (IAM):** users must only have access to the applications, functionality and data in line with their business needs. Too broad access rights can lead to data leaks and misuse.
- **Management of admin accounts:** administrator accounts provide unlimited access to systems and applications and only a few employees (typically from the IT department) should have access to them. Proper management of these admin accounts and their passwords is important, especially when third parties (IT suppliers) also have access to these accounts.

- **Active Directory management:** the security of the Windows environment is managed in Active Directory. Since Windows is the primary Operating System in most organisations, access to the IT systems and the network is specified in Active Directory and appropriate management of this is very important.
- **Firewall management:** the firewall is often the first layer of protection facing the Internet and hackers. They search for vulnerabilities in the configuration and inconsistencies in the firewall rules.
- **Back-up and recovery:** good tools and procedures should be put in place so that critical data and systems are backed up at regular intervals which can be restored in the event of problems.
- **Malware protection:** malware is a more generic name of what is more commonly known as viruses. A good malware solution, that is regularly updated and implemented, protects the organisation against the installation, distribution and execution of malicious code.

In a basic security assessment we examine the IT environment of your organisation and analyse the extent to which these elementary security measures are in place. We then make concrete recommendations to cover the main cyber security risks faced by the organisation.

MATURITY LEVEL 2: PRUDENT

- **Awareness training:** people are the weakest link in cyber security: they make mistakes, they cannot be "patched" and human behaviour and habits are the most difficult to influence. Employees must therefore be trained to understand the importance of cyber security and to recognise dangerous situations so that they can be guided towards safer behaviour.
- **Patch management:** attackers often want to exploit known vulnerabilities in the software of systems and network devices. That is why it is important to install the latest patches regularly.
- **Vulnerability management:** attackers also want to exploit vulnerabilities in the configuration of systems and network devices. Vulnerability management ensures that these vulnerabilities are identified, assessed and resolved.
- **Device management:** active management of the security configuration of mobile devices, laptops, servers and workstations.
- **Network security and remote access for employees and partners:** your network should be managed so that only authorised devices can access the network and non-authorised devices are prevented from accessing the network.
- **Security logging:** using security logging at network and application level, actions are registered so that suspicious and/or unauthorised actions can be identified and appropriate action can be taken in a timely manner.
- **Incident response:** be prepared to respond to cyber incidents from the moment of first detection of an attack.
- **Disaster recovery plan (DRP):** be prepared to rebuild your entire IT environment from zero in the event of serious calamities which also include a major cyber attack.
- **Inventory and control of hardware and software:** active management (taking inventory, follow-up and correction) of all software and hardware assets within the organisation's network so that only authorised software and hardware is allowed.

In an advanced security assessment, we check the extent to which these additional security measures are in line with best practice. We use specialised software to identify the most important "vulnerabilities" in your network and devices. Furthermore, we can also assist you in preparing a Disaster Recovery Plan and incident response procedures and we can also provide security awareness training for your employees.

MATURITY LEVEL 3: BEST PRACTICE

- **Multi-factor authentication:** the use of various authentication techniques in addition to passwords (fingerprint, face recognition, ID card, token, etc.) in order to verify the identity of the user.
- **(Periodic) penetration testing:** with this, a controlled external cyber attack is carried out at the request of the customer within a formally agreed framework, using the techniques and tools that hackers use. This allows to assess what damage could be caused by a hacker and how this can be prevented.
- **Security monitoring:** The continuous monitoring of the organisation's network and systems facilitates the timely identification of suspicious activities based on signals and patterns to allow the organisation to respond adequately. This includes end-point, server and network monitoring.
- **Database security and operating software hardening:** the use of advanced tools and processes to prevent direct access to data in order to ensure the confidentiality and integrity of sensitive information.
- **Application hardening:** ensuring optimal security for sensitive applications, whereby standard configurations and passwords are modified.
- **Encryption:** the use of encryption to secure data (database encryption), e-mail traffic, data carriers, etc.

BDO has specialised "ethical hacking teams" who carry out penetration tests at the request of customers. It goes without saying that clear agreements are made (scope, techniques used, etc.) so that the potential negative impact is kept under control. The monitoring of your network can also be performed by BDO's Security Operations Centres (SOCs).

THE BDO CYBER SERVICES

Cyber security will only increase in importance in the coming years, as indicated by the increase in the number of cyber security incidents. This is driven, among other things, by the rate of digitisation of our society and the increased focus on data privacy. Since a cyber incident can cause considerable damage (both tangible and intangible) it is important that adequate security measures are in place in relation to your organisation's key assets. Unfortunately, these insights in many organisations often comes too late and action is only taken after a cyber incident has occured.

Cyber security is a complex topic, requiring many factors to be taken into account and many measures to be taken. In fact, this is probably one of the reasons why so many organisations are reluctant to take decisive action. Perfect security unfortunately does not exist and even after making considerable investments in cyber security, cyber incidents can still affect your organisation. That is why it is important to apply a risk-based approach, focussing first on the high priority and high risk elements. Based on a maturity model, we establish a step-by-step plan to achieve an enhanced cyber security.

A security assessment is used to determine the maturity level of your organisation, on the basis of which an action plan is prepared with very clear and concrete actions, so that together we can raise the cyber security maturity level of your organisation and put your mind at ease.

What can you expect from us?

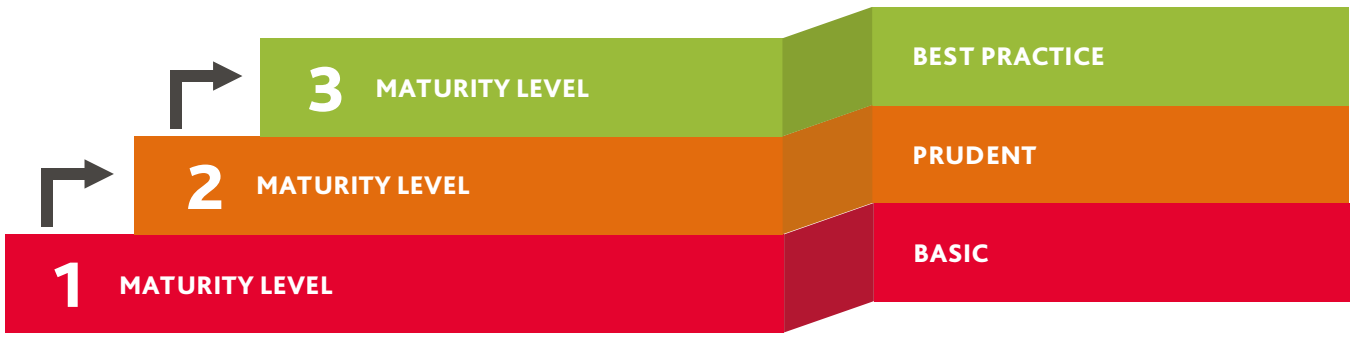
Finger on the pulse - As independent consultants, we evaluate your existing environment taking into account the specific context of your company.

We perform a mapping of your strengths and weaknesses in a structured way, and using easy to understand language so that you have a good idea of the existing risks.

First things first - Our approach is gradual, first we make sure that the biggest vulnerabilities in the existing security are addressed. Only when a solid foundation has been laid do we go a step further with the definition of additional checks.

Sounding board - It is not easy for non-technical people to gain insights into actual cyber risks. In our role as independent experts, we are a sounding board for management and make sure that you continue to see the forest through the trees.

Cyber Darwinism - While evolutions used to be rather slow, in today's world the pace is frantic. However, the starting point remains the same: only those who can adapt shall survive. We will gladly guide you in the making of the right choices in your cyber evolution.



IF YOU WOULD LIKE MORE INFORMATION ABOUT OUR CYBER SECURITY SERVICES, PLEASE CONTACT...

Muzaffar Soomra
Partner
Audit & Assurance Services
E-mail: msoomro@bdo.ky
Tel: +1 (345) 943 8800

Richard Carty
Director
Risk Advisory Service
E-mail: rcarty@bdo.ky
Tel: +1 (345) 943 8800