

BELGIAN CYBER SECURITY GUIDE

PROTECT YOUR INFORMATION



This Guide and the accompanying documents have been produced jointly by ICC Belgium, FEB, EY, Microsoft, L-SEC, B-CENTRE and ISACA Belgium.

All texts, layouts, designs and elements of any kind in this Guide are protected by copyright ©.

Extracts from the text of this Guide may be reproduced for non-commercial purposes only, provided that the source is specified.

ICC Belgium, FEB, EY, Microsoft, L-SEC, B-CENTRE and ISACA Belgium disclaim any liability for the content of this Guide.

It is not intended to be an exhaustive guide to potential cyber threats or mitigations.

The information provided:

- is exclusively of a general nature and not geared towards the specific situation of any individual or legal entity;
- is not necessarily complete, accurate or up to date;
- does not constitute professional or legal advice;
- does not replace expert advice.
- does not provide any warranty for secure protection.



FOREWORD

CYBER SECURITY . . . MISSION CRITICAL FOR EACH AND EVERY BUSINESS

Dear reader,

Our objective in this booklet is to provide you more comfort on a subject that is very important and in the news: information security.

Every day all sorts of cyber criminality or cyber misbehaviour pop up around the globe. Many simply ignore it or hide it, for some it is a source of great concern. Several serious cyber security incidents have occurred lately in our own country. It has become increasingly clear that some foreign governments are ready to invest heavily in gathering valuable information. Neither ignorance, negligence or panic are appropriate when it comes to facing the phenomenon of cybercrime.

In business we have to seize opportunities and manage risks with wisdom. Each and every entrepreneur or manager knows what knowledge, technologies or processes make his company strong or even unique and therefore at the same time vulnerable. Precisely those valuable assets must be

protected by good information security governance. By the same token such governance will help to protect the company against severe damage stemming from all sorts of bad habits and negligence that start to develop in the current wave of social media and personalized devices and apps.

Let your drive for more protection lead to a new dimension in your company's culture and to a new company competence: an information security reflex in the ever changing digital environment.

This booklet takes you through the key elements of the subject and provide you with related checklists which will put you on the right track and make it easier for you to implement the advice provided.

We hope it will be useful for all people responsible in companies in our country.

Rudi Thomaes

Secretary General of ICC Belgium

Philippe Lambrecht

Secretary General of FEB



TABLE OF CONTENT

FOREWORD	3
WHY DO WE NEED A CYBER SECURITY GUIDE?	6
HOW TO USE THIS GUIDE?	9
10 KEY SECURITY PRINCIPLES	11
A. VISION	12
Principle 1: Look beyond the technology	12
Principle 2: Compliance is not enough	13
Principle 3: Translate your security ambition into an information security policy	14
B. ORGANISATION AND PROCESSES	15
Principle 4: Ensure top management commitment	15
Principle 5: Create a visible security role in your company and embed personal responsibility	16
Principle 6: Remain secure when you outsource	17
C. MINDSET	18
Principle 7: Ensure security is an enabler for innovation	18
Principle 8: Keep challenging yourself	19
Principle 9: Maintain focus	20
Principle 10: Be prepared to handle security incidents	21

10 “MUST-DO” SECURITY ACTIONS	23
Action 1: Implement user education & awareness	24
Action 2: Keep systems up to date	25
Action 3: Protect information	26
Action 4: Apply mobile device security	27
Action 5: Only give access to information on a “need to know” basis	28
Action 6: Enforce safe surfing rules	29
Action 7: Use strong passwords and keep them safe	30
Action 8: Make and check backup copies of business data and information	31
Action 9: Apply a layered approach against viruses and other malware	32
Action 10: Prevent, detect and act	33
SECURITY SELF ASSESSMENT QUESTIONNAIRE	35
SECURITY CASE STUDIES	53
Case study 1: Large national company (industry) trading internationally	54
Case study 2: Medium size retailer with online presence	55
Case study 3: Accounting SME	56
Case study 4: Belgian start-up	57
INFORMATION SECURITY IN BELGIUM – CONTACT DETAILS	59
OVERVIEW OF MOST COMMON CYBER AND INFORMATION SECURITY FRAMEWORKS	65
BIBLIOGRAPHY	66
ACKNOWLEDGEMENT	68



WHY DO WE NEED A CYBER SECURITY GUIDE?

**THIS SECTION IS NOT MEANT TO SCARE YOU,
ALTHOUGH IT MIGHT JUST DO THAT!**

Security risks on the rise

Every day we are both on a personal and on a company level exposed to threats originating in cyberspace. In most cases we are not even aware of these threats, or if we are aware, we do not react on them in an appropriate manner. The media reports daily on information security incidents and the impact they have on us, either as individuals or companies. These incidents are only the tip of the iceberg and we are all far more exposed than we believe we are, and unfortunately the risks on the internet are increasing. Information security risk can be seen as the multiplication of three factors: assets, vulnerabilities and threats (assets are exposed by vulnerabilities that may get exposed to threats).

Unfortunately, all three factors have seen a significant increase over the last years:

1. Information¹ and information systems are assets. We have more electronic information than ever before and depend on the correct, i.e. secure functioning of the systems that store and process them.
2. We have added cloud, social media, mobile, other new tools and emerging technologies. This technology evolution will continue and further increase our dependence on their proper functioning. However, these technologies have also brought new vulnerabilities which companies were not always ready to deal with.
3. Last but not least, the number of cyber threats has grown. The sophistication of these threats and their effectiveness have also seen a worrying increase.

So, only bad news to bring? Not really. But still.

The good news is that, over the last few years, greater awareness of the problem has developed, leading to several appropriate countermeasures. A set of good initiatives have already been launched on government and institutional level, but perhaps not yet sufficiently taken on board in the corporate world.

In the corporate world, there is still much uncertainty on the “what” and “how to do” in order to mitigate risks coming from cyber threats. Typically some more initiative is taken in larger, international companies, although medium-sized and family owned businesses are equally subject to the same threats and exposures. Even in larger companies, information security initiatives are often not properly sponsored by the highest level of the company. However, we believe information security should be on the agenda of every single company - independent of size, complexity and nature of its business – and of every individual within that company.

Many companies protect their physical valuables – plant, machinery, personnel – very well. Mostly it is a matter of common sense and even habit to install physical security, safety and health instructions in their operations. However, information is valuable too and its theft, loss, misuse and unauthorized modification and disclosure can all have serious impact and consequences. Company knowledge and data are frequently the most important assets of any company. Corporations must ensure the confidentiality, integrity and availability of their data.

These three security objectives correspond with three key questions: “*Who sees the data?*”, “*Have the data been corrupted?*” and “*Can I access the data when I need it?*”

Also you have a responsibility

It is not expected that directors become experts in cyber security. Nevertheless, they are bound to a duty to protect the corporate assets. They will thus delegate the responsibility to their management teams and external experts to ensure that cyber security remains a regular topic for the board and that the necessary actions are taken to protect the information.

Handling personal data in electronic format implies significant obligations for the company. It is indeed the company that is responsible for the data it manages, and it must therefore ensure a level of security that is appropriate. To this end, the company must take relevant measures to protect the data against accidental or unlawful destruction and to prevent unauthorised use or alteration of data.

In addition to other sanctions which it may incur, the law provides for penal measures. The draft EU Data Protection Regulation will increase the severity of these measures and the company may be ordered to pay significant damages to affected persons.

Under the draft EU Data Protection Regulation, in case of misuse by third parties of personal data held by the company, loss of data or any other breach thereof, the company should inform the Privacy Commission without delay, as well as the person concerned when the data breach is likely to adversely affect the privacy.

Time to act

Being victim of an information security incident may have many consequences, not limited to loss of

data or information. The effects on your company's reputation may last a long time and have deep financial consequences.

The assertion that protecting company information is everyone's responsibility is not enough. Make this tangible at all layers of your company and embed good security principles in the day-to-day work. These principles should be common-sense and pragmatic in order to sustain their impact and to allow implementation in both big and small companies avoiding a “one size fits all” approach.

Professional information security governance is a matter of

- (A) creating a company vision and principles on the topic, that should be translated into an information security policy,
- (B) inserting this policy into the organisation and processes by defining proper roles and responsibilities,
- (C) creating the right culture, behaviour and mindset by implementing good information security principles.

This mix should allow your company to achieve sustainable results in the information security space. Individual responsibility and basic discipline, rather than sophisticated protection technologies, are the very first and easiest actions that can significantly improve your information security.

We will never be 100% secure but that should not stop us from trying. This guide, written by people out of the corporate world, should help companies in starting their journey towards a better and sustainable information security.

¹ Sensitive information of a company may include: financial data, HR data, customers and suppliers data, price lists, minutes of the Board,...



GET STARTED

HOW TO USE THIS GUIDE?

START
HERE





A. VISION

**B. ORGANISATION &
PROCESSES**

C. MINDSET

10 SECURITY KEY PRINCIPLES

There are a number of key principles that are to be considered a basis for sound information security practice. Nevertheless, the approach to information security may differ from company to company depending on the nature of the business, risk level, environmental factors, regulatory requirements and size of the company. Hence, these principles apply to all companies independent of size or industry.

This guide presents **10 key principles** in three information security governance areas:

(A) vision,

(B) organisation & processes and

(C) mindset,

completed with a set of “must-do” **security actions**.

The suggested principles and actions in this guide will significantly strengthen the resilience of a company against cyber attacks and limit the impact in the event of a breach.



1.

— LOOK BEYOND THE TECHNOLOGY —

Think of information security in its broadest sense, not just in terms of information technology.

Based on experience², 35% of security incidents are a result of human error rather than deliberate attacks. More than half of the remaining 65% of security incidents that were the result of a deliberate attack, could have been avoided if people were handling information in a more secure manner.



This clearly indicates that information security needs to be seen as a combination of people, processes and technology. It is important that we recognise that information security is a business wide issue, not just an IT issue. Implementation of security measures should not be limited to the IT department but rather be reflected throughout the company in all its undertakings. The scope and vision of information security therefore includes people, products, plants, processes, policies, procedures, systems, technologies, networks and information.

In a mature company, information security is viewed as a business requirement that directly aligns with strategic goals, enterprise objectives, corporate policies, risk management, compliance requirements and performance measurements. Managers across your company should understand how information security serves as a business enabler.

Some of the benefits of looking beyond the technology and focus on information security as a business enabler, are:

- **Strategic:** improvement of the corporate decision making through the better visibility of risk exposure.
- **Financial:** reduction of losses leading to financial benefit.
- **Operational:** adequate contingency plans for the company.

²EY – 2012 Global Information Security Survey - Fighting to close the gap

2.

– COMPLIANCE IS NOT ENOUGH –



Companies are subject to many laws and regulations, many of which require the implementation of appropriate security controls. Laws and regulations address privacy, control over the financial statement process, consumer protection focus and the security of specific data. They are often supplemented by industry specific regulations or security standards and frameworks.

Compliance with these laws, regulations and standards has led to improved information security. However, too often the compliance effort remains the sole objective.

As the compliance is always focused on specific topics, the comprehensive risk-based approach is often missing. E.g. privacy efforts focus only on the protection of personal data and control over financial statements will mainly look at the integrity of financial data.

We must therefore understand two important aspects:

- **First of all**, being compliant does not necessarily imply being secure. Security objectives coming from laws, regulations and standards are always a subset of the overall company security objectives. With that in mind, implementing good business security practices will almost certainly facilitate or lead to compliance, whilst at the same time satisfying the business' needs.
- **Secondly**, security efforts should be aligned and where possible integrated with compliance and other mitigating efforts. This to avoid too many different overlapping initiatives and responsibilities.



3.

— TRANSLATE YOUR SECURITY AMBITION INTO AN INFORMATION SECURITY POLICY —

Information security is a business issue, not just a technology issue. The reason companies want to protect information and information systems should be for sound business purposes. A security policy framework ensures the company's vision in terms of security is translated into practice. Typically, this occurs via a top level policy and its supporting guidelines and standards, which eventually are embedded into operational procedures.

Corporate information security policies provide several benefits:

- helping companies demonstrate their commitment to protect their vital information assets,
- providing a standard baseline of security across the company for all business units and staff, and
- increasing security awareness.

The security policy framework is the foundation for the approach and activities around security.



4.

— ENSURE TOP MANAGEMENT COMMITMENT —

The information security function should have sufficient commitment within the company to enable an adequate company-wide response to the current and upcoming security threats. Therefore, the top management team should visibly engage in the management and oversight of the company's cyber security policy. They should ensure adequate resources – both in terms of financial budgets and people - are allocated to the protection of the company. A formal sign-off of the company security policy demonstrates an active support.



The management team should understand and support the important nature of mitigating cyber-related risks as an essential element for success and safeguarding intellectual property. Protecting your knowledge is key in order to deliver products or services to your customers in a competitive way.

The effectiveness and adequacy of the implementation of the information security measures should be formally reported:

- on a regular basis to the highest security authority in your company
- and at least once a year to the management team and the board of directors.

This reporting should be based on a number of information security indicators and metrics and should provide insights how well your company is protecting its assets. Assessing progress and effectiveness of the measures is essential for informed decision-making regarding information security policy and investments.



5.

— CREATE A VISIBLE SECURITY ROLE IN YOUR COMPANY AND EMBED PERSONAL RESPONSIBILITY —

In order to manage information security in an effective and efficient manner, appropriate security governance has to be defined and implemented. The appropriate people need to be accountable for information and its protection and should have the right authority, tools and training to achieve this. There should be a function leading and facilitating information security initiatives, while the accountability of security remains shared across the company.

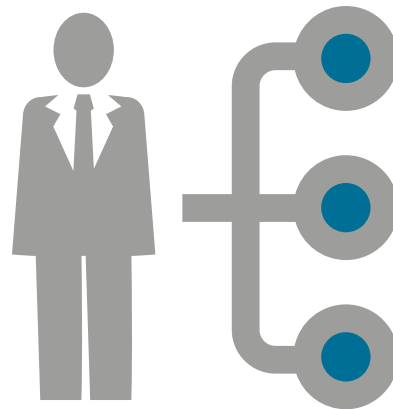
Even the small companies should have someone within or outside who regularly checks the adequacy of the information security and formally takes the responsibility for information security. Though this might not be a full time role in small companies, it is nevertheless an important one that might prove vital in the survival of the company.

In large companies, the allocation of functions, roles and responsibilities should be a deliberate mix of individuals and (virtual) working groups and committees. Each team member should clearly know its responsibility and accountability. Proper documentation and communication is essential in this case.

It is necessary to take efforts to train staff and inform them of their responsibilities, as well as the threats they might be exposed to. An important threat they should be trained on, is *social engineering*. Social engineering is the technique of manipulating people into performing actions to divulge sensitive or confidential information.

Empower selected personnel to share appropriate information with peers and other stakeholders within the industry, both to help build leading practice and warn of potential upcoming attacks.

Although often referred to as the *weakest link* when it comes down to information security, transform your people into being the *greatest asset to good security*, by creating information security awareness that leads to effective skills.



6.

— REMAIN SECURE WHEN YOU OUTSOURCE —

Supported by ever improving interconnection and communication means, value chains have become very integrated and have brought a lot of additional benefits to a company. Outsourcing, offshoring and new collaboration models with third parties have become a standard part of the way business is done.

However, third parties that are not adequately protecting information or information systems may become a serious liability to a company's business operations, reputation and brand value.

It is good practice to encourage suppliers, especially IT service providers, to adopt as a minimum the information and information security principles applied within the originating company but also challenge them to prove that these are secure. This can be done by conducting audits or requesting service providers to present a formal independent third party report covering information security practices. Special attention should be paid to review and understand service level agreements, in particular for system availability and restoration metrics.

In the current age of cloud services, this principle is more than ever valid. Cloud services are solutions whereby you use an outside service provider to store, process or manage data over a network like the Internet with a very high degree of flexibility and real-time monitoring.

IT service providers may bring information security solutions as well. You can inquire about additional services a third party service provider and especially

cloud service providers can provide around information security. These services may include backup-and-restore and encryption, which may be very interesting to small businesses.

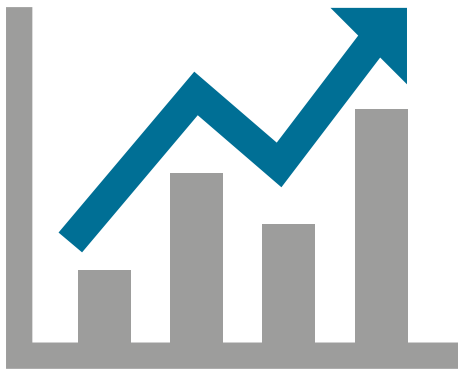
Make sure access to activity logs of outsourced services is available. They are essential for a proper analysis and evaluation of threats.





7.

— ENSURE SECURITY IS AN ENABLER FOR INNOVATION —



An adequate security approach not only protects the company but can enable a move into new technologies. Risk aversion should not block the introduction of new technologies. Adequate assessment of the threats of new technologies should be balanced them against the benefits they may bring.

When new innovative solutions and devices are taken on board, appropriate security measures have to be taken into account as early as possible in the adoption period. Ideally this takes place during the identification of business requirements. The security by design principle should be applied to ensure adequate security is built in from the start of the development and acquisition of new tools and applications.

People who make innovations happen in a company should either have a sufficient security insight, or involve one or more security experts, to embed information security in the design of each new solution to ensure the best fit.

8.

— KEEP CHALLENGING YOURSELF —



Security threats evolve constantly, creating a moving target. Policies and procedures may become out of date or are simply ineffective in practice.

Periodic assessment of a company's resilience against cyber threats and vulnerabilities enable measurement of the progress and adequacy of security activities. This can be done through internal and/or independent assessments and audits, such as penetration testing and intrusion detection. Moreover, they can help to improve the company culture. Companies should allow people to make mistakes and stimulate an open conversation on security incidents, so people are not afraid to report security incidents when they happen.

Next to those assessments, active engagement with peers across the company's industry, the wider business community and law enforcement can help to maintain an understanding of current and emerging threats.



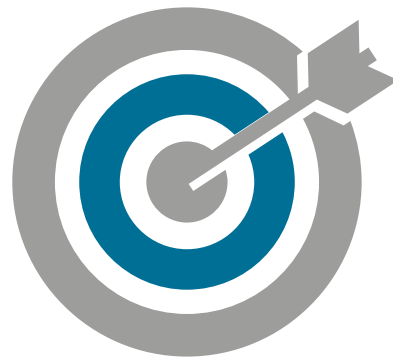
9.

— MAINTAIN FOCUS —

In today's knowledge economy, information has become particularly valuable. Identifying that asset and subsequently trying to tackle its vulnerabilities and threats can be an enormous task.

You should focus your security efforts specifically on the protection of the most valuable information where loss of confidentiality, integrity or availability would seriously harm the company.

This does not mean that other information assets can be ignored in terms of security. It implies that a risk-based approach with focus on the “crown jewels” of the company is the most efficient and effective approach to practice information security. At the same time, it recognizes that 100% risk elimination is not possible, nor required.



10.

— BE PREPARED TO HANDLE SECURITY INCIDENTS —

It's not necessarily bad having a security incident; it's the response that counts. In the current threat and vulnerability environment, you should not wonder "if" but rather "when" you will be victim of a security incident and how well you are prepared for that. Your company should be prepared both organisationally as well as technically to cope with such security incidents in order to minimise the business impact. Ideally appropriate specialised third parties who can assist in the containment and remediation of the security incident(s) will have been proactively identified before anything goes wrong.

A good incident response, including an appropriate communication strategy, can make the difference between business process down time of less than a day or several days long, between a "fait-divers" of 10 lines on page 7 and the headline on page 1 of the news papers.

It is essential that security incidents are appropriately communicated internally and as the case may be, externally. Moreover, you must keep in mind that reporting to the adequate authorities is the way to improve the overall security landscape and that it is, in some cases, mandatory.





**PREVENTION
IS ALWAYS BETTER
THAN REACTION**



10 “MUST-DO” SECURITY ACTIONS

This action list is very much focused on protecting the company against security incidents. Obviously, detecting, containing, responding to and recovering from an incident is also important. For practical guidance, we suggest to look at the overview and contact list of this guide.



1.

– IMPLEMENT USER EDUCATION & AWARENESS –

Information security is an issue impacting the whole company. The same people who create and handle the information of a company play a major role in safeguarding that information. When they don't handle information correctly, they not only become a source of security incidents but also make it very easy for attackers to succeed.

Creating awareness on the most important cyber threats and security issues is essential throughout the company on a continuous basis. **Examples of information security awareness topics are:**

- Communicating safely and responsibly
- Using social media wisely
- Transferring digital files in a safe way
- Proper password usage
- Avoiding losing important information
- Ensuring only the right people can read your information
- Staying safe from viruses and other malware
- Who to alert when you notice a potential security incident?
- Knowing how not to be tricked into giving information away

This will ensure that all personnel who have access to information and information systems understand their daily responsibilities to handle, protect and support the company's information security activities. Security aware handling, motivation, and compliance as such can become the accepted, expected cultural norm. Repeating information security messages to staff over time is the best way to develop the desired security skills and attributes.

As most staff members also use internet for private purposes their education should not be limited only to the use of company information. It is important that they understand how to protect their privacy when using Internet for private purposes.

General cyber security information and awareness for end users can be found on www.safeonweb.be, an initiative of CERT.be (the federal cyber emergency team) and on <http://www.enisa.europa.eu/media/multimedia/material>, an initiative of ENISA. You are authorised to use all this information, videos, infographics... for education purposes within your company.



2.

– KEEP SYSTEMS UP TO DATE –

Many of the successful hacking attempts and virus breaches abuse system vulnerability for which solutions and corrections were available, often even more than a year prior to the incident.

Systems and software, including networking equipment, should be updated as patches and firmware upgrades become available. These upgrades and security patches fix system vulnerabilities that attackers could abuse.

Wherever possible and available at reasonable commercial terms, use automated updating services, especially for security systems such as anti-malware applications, web filtering tools and intrusion detection systems.

In order to ensure all relevant systems are subject to the best protection, having an inventory that lists the systems along with a definition of the minimum baseline of security that needs to be applied to them, is a good idea.

Users should only accept valid security software updates directly sent by the original vendor. Hence, they should never take any software update action suggested in an external email.





3.

– PROTECT INFORMATION –

More than ever, the information security strategy should be focused on the data rather than on the security technology. Network perimeter security and traditional access control are no longer sufficient, especially when information is stored in less trusted environments, such as the Internet or portable media.

Different encryption techniques are available and have proven their effectiveness in specific circumstances (whether it's data storage, data transmission or data transport), for example:

- E-mail sent over the Internet to business partners, clients and others are always in clear text. Therefore companies should provide the means to encrypt e-mails when sensitive information is being transmitted.
- Portable devices such as laptops, USB keys and smartphones can be particularly easy targets for theft or can be lost. Therefore companies should ensure these are either encrypted by default (laptops and smartphones) or that users have the means to encrypt data stored on them (USB keys).



4.

— APPLY MOBILE DEVICE SECURITY —

Mobile devices create significant security and management challenges, especially when they hold confidential and sensitive information or can access the corporate network:

- Data loss
- Social engineering attacks
- Malware
- Data integrity threats
- Resource abuse
- Web and Network-based Attacks
- ...



The BYOD (Bring Your Own Device) concept is very appealing to a lot of organisations and employees, but it has the inherent disadvantage of increasing the risk of exposing sensitive company information. Therefore adopt a clear position on which device may access the company network and/or information and adapt the appropriate security policy and procedures.

Users should always protect their mobile devices with a strong password. Companies should enable and/or enforce users to configure the appropriate mobile device security settings to prevent criminals from stealing information via the device. These devices must have their software kept up-to-date, especially the security software, in order to remain protected against the latest versions of malware and viruses.

Additionally, there should be reporting procedures for lost or stolen equipment and where possible remote wiping functionalities to delete all company information from lost or stolen devices. **Users must also be aware they have to adopt reflexes to check their surrounding before or while using their mobile devices, as well a set of adapted strategies:**

- Installing adequate email security solutions
- Avoid opening unexpected text messages from unknown senders
- Avoid opening unidentified links
- Avoid chatting with unknown people



5.

– ONLY GIVE ACCESS TO INFORMATION ON A “NEED TO KNOW” BASIS –

Access should only be granted on a need to know basis in order to ensure confidentiality, integrity and availability. No one in an organisation should have access to all data systems. Employees should only be given access to the specific data and information systems that they need for their job. Administrative privileges (superuser rights) should only be given to a few trusted IT staff. Nowadays, there are options which do allow system administrators to do their job without having access to the data. Moreover, all responsible managers should receive, review and validate (at least annually) an overview of all users (internal and external) who have access to applications and data of their department.

Additionally, employees should not be able, without prior authorisation, to install any software on their company laptops and desktops. Neither should they have the ability to change pre-installed security settings and security software. Such access is subject to a very high risk of incidents and should therefore be considered as privileged and only be allowed when really needed.



6.

— ENFORCE SAFE SURFING RULES —



The company’s internal network should only be able to access those services and resources on the Internet that are essential to the business and the needs of your employees. Though the use of the Internet for private purposes should not necessarily be completely blocked, this should be limited to services and websites that typically do not pose a security risk. Services and websites that bring an increased risk of malware to the PC or the company network (e.g. peer-to-peer file sharing and pornographic websites) should be blocked. There are easy to use internet website monitoring tools which use automatic categorisation and allow access in different modes (never, always, during certain hours, up to a certain volume, etc.). It is essential that these surfing rules are transparent to all users in the organisation, including a mechanism to unblock business websites which might have had access denied.

Risks involved in surfing on malicious websites are not limited to viruses and spyware. It will also make the company more vulnerable to phishing³, by raising the risk that the employee’s personal information gets stolen. Another risk is the exposure to copyright infringement, related to the illegal copying or downloading of copyright protected software, videos, music, photos or documents.

Some browsers also have the ability to identify fraudulent websites by default. **Every device going online should be running the latest version of the browser it uses and persons should be educated to the basic tips to identify suspicious websites like:**

- Check for a contact section with an address, phone number and/or e-mail that can be verified, as well as a privacy policy.
- Check for the destination of hyperlinks by rolling on the link and looking (mostly) at the bottom left corner of your browser where the real website address is displayed.
- Checking for ‘https://’ at the beginning of the web address before entering personal information.

³ <http://en.wikipedia.org/wiki/Phishing> : the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication



7.

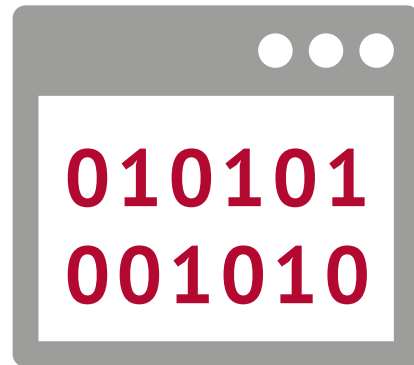
— USE STRONG PASSWORDS AND KEEP THEM SAFE —

Passwords are the principle means by which we protect our information. Therefore, it is key that strong passwords are used. In order to ensure passwords are strong, you must implement and impose a number of principles:

- Users should have their own unique user ID and passwords and not share these.
- Password length and/or complexity should be imposed to ensure passwords are difficult to guess but always easy to remember.
- Users are forced to change their passwords periodically (every 3 months is a good practice).
- Users should have different passwords for different applications.
- Users should not mix personal and professional passwords.

Consider also implementing multiple authentication methods that require additional information beyond a password to gain entry, especially when such access is subject to increased risk (e.g. remote access).

In multi-factor authentication, companies decide to use a combination of elements, such as *things I know* (e.g. password or PIN), *things I have* (e.g. a smartcard or SMS) and *thing I am* (e.g. fingerprint or iris scan). In taking the decision about which combinations to use, companies should take into account regulatory constraints and staff acceptability factors.



8.

— MAKE AND CHECK BACKUP COPIES OF BUSINESS DATA AND INFORMATION —

Just as critical as protecting the confidentiality and integrity of data, is backing it up. In the event that information is stolen, altered, erased or lost, the availability of a backup copy will be crucial.

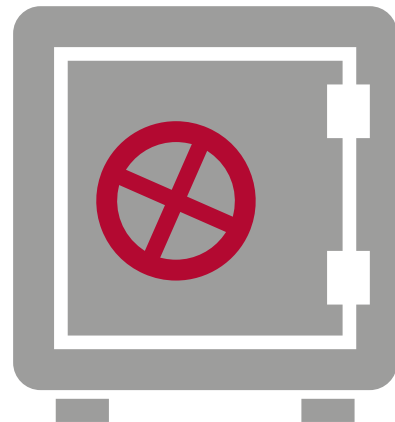
A policy should be put in place that specifies:

- which data are backed up and how;
- how often data are backed up;
- who is responsible for creating backups;
- where and how the backups are stored; and
- who has access to those backups.

In taking those decisions, make sure that legal and regulatory requirements for the retention of information are understood and followed.

At the same time one should keep in mind that physical media such as a disc, tape or drive used to store data backup are vulnerable as well. So backups must enjoy the same level of protection as the source data, especially with regard to physical safety as those items are easily moved.

One of the main issues in backup management is validating the content of the business data and information contained in the backup files. Therefore implement a discipline of regularly restoring the backup in order to verify the effectiveness, completeness and the speed to recover the data. In case third parties are used for the storage of information (e.g. cloud-services), they should ensure back-up provisions are made for that information.





9.

— APPLY A LAYERED APPROACH AGAINST VIRUSES AND OTHER MALWARE —

Because of the many different types of machines and users with different needs, an effective protection against viruses, spyware and other malicious software requires a layered approach to a company's defence. Antivirus software is a must, but should not be a company's sole line of defence. A combination of several techniques to protect against viruses is necessary to ensure adequate security.

Combining the use of web filtering, antivirus protection, proactive malware protection, firewalls, strong security policies and user training, significantly lowers the risk of infection. Consider using different brands of technology for similar functions (e.g. different vendors for malware protection software solutions). Keeping protection software up to date along with the operating system and applications increases the effective security of systems.



10.

— PREVENT, DETECT AND ACT —

Companies are often not aware that an information security incident is happening. Company systems are invaded and infected months or years before someone detects the intrusion⁴, if they ever do.

Companies should invest in a combination of intrusion detection and intrusion prevention systems. The tools are as strong as the quality of their implementation and the training of the users. Seek experienced parties for advice and support when this knowledge is not present in your company. Beyond technology, professionals with a particular interest in cyber security might benefit from partnerships at different levels, with the industrial sectors, with the government or, at a global level, with initiatives like the World Economic Forum’s Partnering for Cyber Resilience.

Companies should always seriously consider reporting information security incidents to the federal cyber emergency team (CERT.be) at cert@cert.be. Reporting to the CERT is vital to identify if the incident is isolated or not. An attack can be horizontal (companies from the same sector are targeted too) or vertical (subcontractors are targeted too) or can be a security threat related to a particular software or hardware. The CERT will be able to provide some information and advice related to the incident, that can help the victim to take effective countermeasures.

Organisations who become a victim of (cyber) crime should also file a complaint with the police. The local police is not specialised and is rather a point of contact for traditional crime. In case of cybercrime

(hacking, sabotage, espionage), it is better to directly contact the Federal Computer Crime Unit (FCCU), especially when it concerns an attack on a vital or critical IT-infrastructure. It is also a possibility to independently contact the public prosecutor’s office. Moreover it helps law enforcement to build a better picture of the cyber threat to businesses in Belgium.

When dealing with a security incident and in particular a case of cybercrime, the (IT) responsables should ensure a proper safeguarding of evidence from the start. Guidelines for data acquisition in security incidents⁵ for investigation purposes by ICT staff or in case of malware infection⁶, are available online on the website of the CERT-EU.



⁴ <http://www.verizonenterprise.com/DBIR/2013/> -Verizon 2013 Data Breach Investigations Report

⁵ http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_004_v1_3.pdf

⁶ http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_11_003_v2.pdf



Background text consisting of various alphanumeric strings (hexadecimal and decimal) such as 25BE7, 86C, 2C, A1C8, 8, 2C, ABA3F, BB1D, 2, 8, B, AC44A468490, 95BFBC56059, 277B13, 7, 7, A, D, 0, 8, 7, 9, 0, 4, 4, 9, 4, 6, 8, 0, 7, C, 4, B, 6, 4, 3, 7, F, D, 0, 5, 2, D, D, 4, 6, F, 2, F, 4, 2, 5, 7, 3, 8, 6, C, 4, 2, C, C, 0, 7, 3, C, D, 3, D, F, 6, 0, 7, 3.

SHORT AND EASY

SECURITY SELF ASSESSMENT QUESTIONNAIRE

The following section presents a simple checklist as a tool for top management to help guide their internal review of their company's cyber resilience capabilities and to enable them to ask the right questions to the teams involved in these initiatives. The questions asked in the tool can help them to identify specific strengths and weaknesses – and paths to improvement within their respective company.

At the same time, this self assessment questionnaire can be used as a checklist by companies that are just beginning in their information security initiatives, and want to use the questions and answers as a basis for planning their cyber resilience capabilities.

For each of the questions below, companies should choose from the provided options the one that is best reflecting the current practices of the company. Each of the options has been given a bullet colour, where:




- This is the least desirable response; Improvement should clearly be considered.
- Additional improvement is possible to better protect the company.
- This answer is the best reflection of resilience against cyber threats.

Further, the presence of a *more specific checklist under each question* will help you to identify and document the status of a set of basic information security controls for your company.

Companies can use the referenced principles and actions in the two previous chapters as guidance for improving their resilience related to each of the specific questions.



1. DO YOU EVALUATE HOW SENSITIVE INFORMATION IS WITHIN YOUR COMPANY?

-  No, but we have a firewall to protect us from theft of information.
-  Yes, we understand the importance of our information and implement general security measures.
-  Yes, and we have an information classification model and know where our sensitive information is stored and processed. We implement security measures based on the sensitivity of the information.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Are your sensitive data identified and classified?		
Are you aware of your responsibility regarding the identified sensitive data?		
Are the most sensitive data highly protected or encrypted?		
Is the management of personal private information covered by procedures?		
Are all employees able to identify and correctly protect sensitive and non sensitive data?		




LINK TO RELEVANT PRINCIPLE



POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE



2. DO YOU PERFORM INFORMATION SECURITY RELATED RISK ASSESSMENTS ?

-  We do not perform risk assessments.
-  We perform risk assessments but not on any specific information security related topics
-  We perform risk assessments on specific information security topics

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Do you address vulnerability results in order of high risk to low risk?		
Are events that could cause interruptions to business processes identified and is the impact of the potential related interruptions assessed?		
Do you have a current business continuity plan that is tested and updated on a regular basis?		
Do you regularly perform a risk assessment to update the level of protection the data and information need?		
Are areas of risk identified throughout your business processes in order to prevent information processing corruption or deliberate misuse?		

LINK TO RELEVANT PRINCIPLE






POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE





3. AT WHAT LEVEL IS INFORMATION SECURITY GOVERNANCE IMPLEMENTED?

-  There is no information security governance in place.
-  Information security governance is installed within the ICT department since that's where the information needs to be secured.
-  Information security governance is installed at the corporate level to ensure an impact on the entire company.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Do board members allocate an information security budget?		
Is information security part the existing risk management of the directors?		
Does top management approve the information security policy of the company and communicate it by an appropriate way to the employees?		
Are board members and top management informed on a regular basis of the latest developments in information security policies, standards, procedures and guidelines?		
Is there at least one officer part of the management structure in charge of the protection of data and the privacy of personal information?		




LINK TO RELEVANT PRINCIPLE



POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE



4. DO YOU HAVE AN INFORMATION SECURITY TEAM OR A DEDICATED INFORMATION SECURITY FUNCTION WITHIN YOUR COMPANY?

-  We do not have an information security team or specific roles & responsibilities concerning information security.
-  We do not have an information security team but we have defined specific information security roles & responsibilities within the company.
-  We have an information security team or a dedicated information security function.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Does an identified information security specialist or team coordinate in house knowledge and provide help to the management in decision making?		
Is the identified information security specialist or team responsible to review and systematically update the information security policy based on significant changes or incidents?		
Has the identified information security specialist or team enough visibility and support to intervene in any information-related initiative in the company?		
Are there different managers responsible for separate types of data?		
Is the information security policy feasibility and effectiveness, as well as the information security team's efficacy, regularly reviewed by an independent body?		

LINK TO RELEVANT PRINCIPLE






POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE





5. HOW DOES YOUR COMPANY DEAL WITH INFORMATION SECURITY RISKS FROM SUPPLIERS WHO CAN ACCESS YOUR SENSITIVE INFORMATION?

-  We have a relationship based on mutual trust with our suppliers.
-  For some contracts we include information security related clauses.
-  We have processes in place to validate access for suppliers and specific security guidelines are communicated and signed by our suppliers.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Are contractors and suppliers identified by an ID badge with a recent picture?		
Do you have policies addressing background checks for contractors and suppliers?		
Is access to facilities and information systems automatically cut off when a contractor or supplier ends his mission?		
Do suppliers know how and to whom to immediately report in your company any loss or theft of information?		
Does your company ensure suppliers keep their software and applications updated with security patches?		




LINK TO RELEVANT PRINCIPLE



POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE



6. DOES YOUR COMPANY EVALUATE COMPUTER AND NETWORK SECURITY ON A REGULAR BASIS?

-  We do not perform audits or penetration tests to evaluate our computer and network security.
-  We do not have a systematic approach for performing security audits and/or penetration tests but execute some on an ad hoc basis.
-  Regular security audits and/or penetration tests are systematically part of our approach to evaluate our computer and network security.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Do you test on a regular basis and keep records of identified threats?		
Do you have procedures in order to evaluate human threats to your information systems, including dishonesty, social engineering and abuse of trust?		
Does your company request security audit reports from its information service providers?		
Is the utility of each type of stored data also assessed during the security audits?		
Do you audit your information processes and procedures for compliance with the other established policies and standards within the company?		

LINK TO RELEVANT PRINCIPLE






POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE





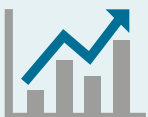
7. WHEN INTRODUCING NEW TECHNOLOGIES, DOES YOUR COMPANY ASSESS POTENTIAL INFORMATION SECURITY RISKS?

-  Information security is not part of the process for implementing new technologies.
-  Information security is only implemented in the process for new technologies on an ad hoc basis.
-  Information security is included in the process for implementing new technologies.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
When considering implementing new technologies, do you assess their potential impact on the established information security policy?		
Are there protective measures to reduce risk when implementing new technologies?		
Are the processes to implement new technologies documented?		
When implementing new technologies, could your company rely on partnerships, in order that collaborative efforts and critical security information sharing is occurring?		
Is your company's information security policy often considered as a barrier to technological opportunities?		




LINK TO RELEVANT PRINCIPLE



POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE



8. DOES INFORMATION SECURITY TAKE PLACE WITHIN YOUR COMPANY?

-  We put trust in our employees and do not consider information security guidance as added value.
-  Only our ICT personnel receives specific training for securing our ICT-environment.
-  Regular information security awareness sessions are organised for all employees.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Are some information security awareness sessions adapted to the activity field of the employees?		
Are employee taught to be alert to information security breaches?		
Does your company have a guideline for users to report security weakness in, or threats to, systems or services?		
Do employees know how to properly manage credit card data and private personal information?		
Do third party users (where relevant) also receive appropriate information security training and regular updates in organisational policies and procedures?		

LINK TO RELEVANT PRINCIPLE



POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE





9. HOW DO YOU USE PASSWORDS WITHIN THE COMPANY?

- ✗ We share passwords with other colleagues and/or no policy exists for the safe usage of passwords nor for the regular change of passwords.
- All employees, including the management, have unique passwords but complexity rules are not enforced. Changing passwords are optional, but not mandatory.
- ✓ All employees, including the management, have a personal password that must meet defined password requirements and must be changed regularly.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Did your company establish and enforce a globally-accepted password policy?		
Can you assure all passwords in your company are not stored into easily accessible files, bad or blank, default, rarely changed even on mobile devices?		
Do you feel well protected against unauthorized physical access to system?		
Are users and contractors aware of their responsibility to protect unattended equipments as well (logoff)?		
Have employees been taught how to recognise social engineering and react to this threat?		

LINK TO RELEVANT PRINCIPLE



POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE



10. IS THERE A COMPANY POLICY IN PLACE FOR THE APPROPRIATE USE OF THE INTERNET AND SOCIAL MEDIA?

- ✘ No, there is no policy in place for the appropriate use of the internet.
- Yes, a policy is available on a centralised location accessible to all employees but has not been signed by the employees.
- ✔ Yes, a policy for the appropriate use of the internet is part of the contract / all employees have signed the policy.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Are there general communication guidelines and processes for employees in the company, including relation to the press and social media?		
Is there a disciplinary process for employees violating the company's communication guidelines?		
Does an identified communications responsible or team screen the Internet in order to assess e-reputation risks and status?		
Has your company assessed its liability for acts of employees or other internal users or attackers abusing the system to perpetrate unlawful acts?		
Has your company taken measures to prevent an employee or other internal user to attack other sites?		

LINK TO RELEVANT PRINCIPLE



POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE





11. DOES YOUR COMPANY MEASURE, REPORT AND FOLLOW-UP ON INFORMATION SECURITY RELATED MATTERS?

- ✘ We do not monitor, report or follow-up on the efficiency and adequacy of our implemented security measures.
- Our company has implemented tools and methods to monitor, report and follow-up the efficiency and adequacy of a selection of our implemented security measures.
- ✔ Our company has implemented the necessary tools and methods to monitor, report and follow-up on the efficiency and adequacy of all our implemented security measures.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Are audit trails and logs relating to the incidents maintained and proactive action taken in a way that the incident doesn't reoccur?		
Does your company verify compliance with regulatory and legal requirements (for example: data privacy)?		
Has your company developed some own tools to assist the management in assessing the security posture and enabling the company to accelerate its ability to mitigate potential risks?		
Does an information security roadmap including goals, progress evaluation and potential collaborative opportunities exist in your company?		
Are monitoring reports and incidents reported to authorities and other interest groups such as a sector federation?		

LINK TO RELEVANT PRINCIPLE

POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE

12. HOW ARE SYSTEMS KEPT UP-TO-DATE WITHIN YOUR COMPANY ?

- ✘ We rely on automatic patch management, provided by the vendor, for most of our solutions.
- Security patches are systematically applied on a monthly basis.
- ✔ We have a vulnerability management process in place and continuously seek information concerning possible vulnerabilities (for ex. through a subscription on a service that automatically sends out warnings for new vulnerabilities) and apply patches based on the risks they mitigate.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Is vulnerability scanning a regular scheduled maintenance task in the company?		
Is application system reviewed and tested after change in operating system?		
Can users check themselves the existence of unpatched applications?		
Are users aware that they also have to keep up-to date the operating system and applications, including security software, of their mobile devices?		
Are users trained to recognize a legitimate warning message (requesting permission for update, or from fake antivirus) and to properly notify the security team if something bad or questionable has happened?		

LINK TO RELEVANT PRINCIPLE



POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE





13. ARE USER ACCESS RIGHTS TO APPLICATIONS AND SYSTEMS REVIEWED AND MANAGED ON A REGULAR BASIS?

- ✘ Access rights to applications and systems are not consistently removed nor reviewed.
- Access rights to applications and systems are only removed when an employee is leaving the company.
- ✔ An access control policy is established with regular reviews of assigned user access rights for all relevant business applications and supporting systems.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Is access to electronic information systems and facilities limited by policies and procedures?		
Does your company rely on a privacy policy stating the information it collects (for example about your customers: physical addresses, email addresses, browsing history, etc), and is done with it		
Do the policies and procedures specify methods used to control physical access to secure areas such as door locks, access control systems or video monitoring?		
Is access to facilities and information systems automatically cut off when members of personnel end employment?		
Is the sensitive data classified (Highly Confidential, Sensitive, Internal Use Only,...) and its granted users inventoried?		

LINK TO RELEVANT PRINCIPLE

POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE

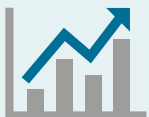
14. IN YOUR COMPANY, CAN THE EMPLOYEES USE THEIR OWN PERSONAL DEVICES, SUCH AS MOBILE PHONES AND TABLETS, TO STORE OR TRANSFER COMPANY INFORMATION?

- ✘ Yes, we can store or transfer company information on personal devices without the implementation of extra security measures.
- A policy exists that prohibits the use of personal devices to store or transfer company information but technically it is possible to do so without implementing extra security measures.
- ✔ Personal devices can only store or transfer company information after the implementation of security measures on the personal device and/or a professional solution has been provided.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Does your company rely on a well accepted Bring Your Own Device policy?		
Are mobile devices protected from unauthorised users?		
Are all devices and connections permanently identified on the network?		
Is encryption installed on each mobile device to protect the confidentiality and integrity of data?		
Is the corporate level aware that while the individual employee may be liable for a device, the company is still liable for the data?		

LINK TO RELEVANT PRINCIPLE






POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE





15. HAS YOUR COMPANY TAKEN MEASURES TO PREVENT LOSS OF STORED INFORMATION?

-  We have no backup/availability process in place.
-  We have a backup/availability process but no restore tests have been performed.
-  We have a backup/availability process in place that includes restore/resilience tests. We have copies of our backup stored in another secured location or are using other high-availability solutions.

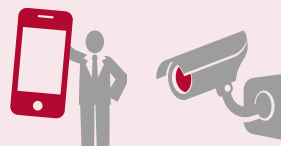
The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Are there enough members of the staff able to create retrievable backup and archival copies?		
Is the equipment protected from power failures by using permanence of power supplies such as multiple feeds, uninterruptible power supply (ups), backup generator etc.?		
Are the backup media regularly tested to ensure that they could be restored within the time frame allotted in the recovery procedure?		
Does your company apply reporting procedures for lost or stolen mobile equipment?		
Are employees trained on what to do if information is accidentally deleted and how to retrieve information in times of disaster?		

LINK TO RELEVANT PRINCIPLE



POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE



16. IS YOUR COMPANY PREPARED TO HANDLE AN INFORMATION SECURITY INCIDENT?

- ✘ We won't have any incidents. In case we have, our employees are competent enough to cope with it.
- We have incident management procedures, however not adapted to handle information security incidents.
- ✔ We have a dedicated process to handle information security incidents, with the necessary escalation and communication mechanisms. We strive to handle incidents as efficient and effective as possible so we learn how to better protect ourselves in the future.

The following 5 questions are intended to provide you some basic information security checks for your company.

	Yes	No
Does your process address different types of incidents ranging from denial of service to breach of confidentiality etc., and ways to handle them?		
Does your company have an incident management communication plan?		
Do you know which authorities to notify and how in case of incident?		
Does your company have contact information sorted and identified for each type of incident?		
Do you rely on an Internal Communication responsible for contacts with employees and their families?		

LINK TO RELEVANT PRINCIPLE



POTENTIAL ACTIONS TO IMPROVE YOUR RESPONSE





CASE STUDIES



SECURITY CASE STUDIES

For each of the case studies, a descriptive text is given how a company applied (or didn't apply) some of the previously mentioned principles and actions. These show that the principles and actions are independent of the size and complexity of an organisation.



1.

– LARGE NATIONAL COMPANY (INDUSTRY) TRADING INTERNATIONALLY –

The business is specialised in shaping and grinding component parts for machinery. They rely heavily on specialised computers in the manufacturing environment. In the manufacturing hall there are only a few desktop computers, directly connected to the corporate internal network, which is mainly used for administrative activities. The service maintenance crew of the company started using desktops as a more efficient way to transfer programme updates to the manufacturing environment. However, during office breaks, the service maintenance crew also uses the same desktops to browse the internet, playing games and updating their social networking activities. As could have been predicted, vicious spyware got installed on one of these machines. The spyware sent data from the desktop to the malicious host about the activities of the desktop computer. It downloaded additional malware that included a time sensitive mechanism that blocked the machines infected with it from booting, unless a key was inserted.

The service maintenance crew continued their day to day activities and upgraded the manufacturing machines, thus spreading the malware into the complete operational environment of the organisation. After one week three specialised computers in the manufacturing department did not start up anymore just like all of the infected desktop machines in the manufacturing hall.

A specialist technical security adviser was hired to investigate the desktop computers. He discovered an array of different malware and ransomware applications running “behind the scenes”. A keylogger was incorporated in the spyware, designed to log all the key strokes of the computer

user. This was identified as the way cyber criminals had managed to gain access to the system to install the time bomb. An internet security package was properly installed on the computer which included anti-virus and anti-spyware. However, it was discovered that automatic updates were not switched on and scans were not regularly executed to check the “security health”. As a result the infection wasn’t able to spread any further than the manufacturing hall, and the infected machines.

On the infected desktop machines a message appeared, that required the business to wire transfer an amount to a specific bank account in order to receive a special digital key that would unblock the mechanism. Due to the fact that the manufacturing capacity was significantly reduced, and the ransom amount was only limited and far less than the cost of installing spare systems, the management team quickly decided to wire transfer the amounts due. Immediately after this mini-project, computer machines were completely cleaned by the specialist technical adviser and reinstalled for operational use. The company decided not to take any further legal action or report the matter to law enforcement.

However, top management decided to explain its internal policies on information security also to the people on the manufacturing floor. The company did inform this specific incident to its partners, suppliers and competitors, and laid the foundation for a trust relationship with those partners to exchange information on a regular basis on similar incidents.

2.

— MEDIUM SIZE RETAILER WITH ONLINE PRESENCE —

This company is a large international retailer, with operations in Belgium and abroad. With over 6 million customers in Europe, customers have created their own profile with personal data. Data is also stored on users preferences, historical data and interests by the retailer. In order to protect the sensitive data from hackers and malware, the company decided to protect all its websites. The company works on a daily basis to maintain and market their products, serve their customers, and find ways to continuously upgrade functionalities and add services.

The operational website handles thousands of transactions daily, and uses different brands of technology to properly manage these transactions. The company is using fraud detection mechanisms to detect (potential) fraudulent transactions and performs continuous testing on the underlying technologies, based upon known vulnerabilities.

When risks are detected, they will be raised automatically and instantaneously. A specialist team of developers, security professionals and company representatives are meeting on a regular basis to discuss potential risks and to check whether vulnerabilities were resolved by taking appropriate measures.

The company decided to automate parts of its security management process, due to the nature of their activities and the risks they incur on their websites. The company also decided to constantly revise additional programming by having code review done by 3rd parties and ensure sufficient testing, even after functionalities were published. The infrastructure is regularly being adapted in line

with constantly changing requirements and needs, and in order to remain agile in their market. The systems require patching almost on a daily basis. The company allows for an external scan on their infrastructure, that reports on existing and potential vulnerabilities.

The company faces constantly multiple attempts from hackers and legitimate users, trying to access personal data or other sensitive information. The company accepts that, based on the nature of their business, there will come a day that also they will be hacked, and has prepared its management team and procedures to mitigate the risks and communications accordingly.



3.

— ACCOUNTING SME —

The business is a small family owned company of accountants with a list of longstanding SME's and very large corporate clients. In 2012 the company was hit by a series of malware, combinations of viruses and trojan malware, which spread via freely downloadable software. The virus corrupts files rendering them useless. The virus targeted specifically Microsoft Word documents and Excel spreadsheets. For a company reliant on the Microsoft Office package, the virus is extremely damaging. The virus disables the security features of installed anti-virus software allowing further infections from other viruses.

It was discovered that the virus was spread via freely downloadable software, that was intended to actually protect the user from malicious threats, called Defense Center.

The software came from an internet website and, started infecting the local machine once it was installed by the employee. This malicious software installed a piece of code (called "Trojan") that allowed the authors of the malware to hack directly into the machine once the malicious software had sent a notification to all the parents with all relevant data on how to connect to it.

Every time a user opened an office document, the malware infected the documents and continued spreading the virus via the company's email contacts. The receivers have a normal attitude to open attachments from a person they trust. Only the partners which had recent malware updating mechanisms in place, were capable of detecting the malware inside the attachments. The receivers were luckily contacted by the company, in order to avoid further damage.

The malware spread so fast through the network to other computers in the company that all computers without exception were infected. The malicious software started to destroy all .xls (spreadsheet) and .doc (word document) files stored on the hard drives, replacing them with the text "DATAError". The loss of client data could cause total failure and bankruptcy of the company. Fortunately the company possesses an effective backup system; at the end of each week, all data was collated from each employees computer over the network and copied onto a new DVD, then properly dated and stored safely offsite. Although all of the data from each computer had been lost, it could be recovered from the backup DVDs. The business was able to recover the majority of files from the backup, although, they still lost three full days of work following the most recent backup.

The infected email bypassed the network security as it was downloaded by a trusted user, behind the firewall. The consequences highlighted a need for proper staff training in dealing with internet sources and a review of the resilience procedure to increase frequency and a regular audit to ensure files could be retrieved.

4.

— BELGIAN START-UP —

The young company is a fully automated demand response aggregator that offers grid operators aggregated curtailable power, which can provide relief when excess power demand endangers the stability of the grid. It sources this power from industrial power consumers who have the ability to briefly curtail their industrial process without negative impact on their output. The start-up's proprietary technology platform, enables end-to-end automation of the service.

The need for security

The need for information security at the start-up is motivated by two key elements:

1. **Technological coupling to mission critical systems.** The technology platform is connected to control centres of grid operators as well as automation systems of utilities and industrial facilities, both of which count as some of the most mission critical and sensitive targets of cyber attacks. A security breach would severely damage the reputation and business prospects of the start-up.
2. **Sensitive proprietary information.** As a technology start-up, the key differentiation of the company is provided by its proprietary technology. As such, it needs to carefully guard this information from competitors and other external parties.

Awareness of management and staff

- Board of Directors has repeatedly highlighted the need for focus on security, encouraging management to define clear policies and protect trade secrets and intellectual property.
- Handling of confidential information: principles and procedures defined and communicated.
- The company's R&D team follows proper guidelines on strong authentication, password

encryption and focus on security in every step of the development process.

Headlines of the start-up's action programme to implement information security

Current approach:

1. Technical measures:
 - a. The technology platform is hosted in data centres implementing state-of-the-art security measures.
 - b. The critical clients are connected over a dedicated network, other clients through IPsec tunnels, with strict firewall rules applied.
 - c. Access control to the technology platform is enforced by a combination of hardware tokens and strictly managed, strong passwords.
2. Organisational measures: all documents are labelled according to confidentiality level, 'need to know'-basis implemented.
3. Procedural measures: different authorisation levels to the technology platform are defined per user group. The specific challenge for a small company such as this start-up is that it cannot afford dedicated security staff. For this reason also, external audit was sought during 2013 to do a structural review and risk assessment of the start-up's security level.

Medium-term focus:

1. A specialist in energy security will perform a full security GAP/risk analysis;
2. The start-up will invest time and effort over a full year to prepare for this certification, focussing on implementation of procedures, creating awareness and developing a sustainable model to regularly review security;
3. ISO 2700X: the start-up aims to obtain the ISO 27001/2 certificate in 2014, as a pro-active step towards becoming a more cyber secure enterprise.



CONTACT AND OVERVIEW LIST

INFORMATION SECURITY CONTACTS IN BELGIUM

All contact details are kept up-to-date on www.b-ccentre.be.

The contact list is split between the public bodies and organisations on one side, and some private not-for-profit organisations on the other. The description of the information security role of each selected organisation, in both categories, has been most the time provided by the organisation itself. When you need more information on the information security services provided by a commercial firm, we invite you to consult the firm's website, as for example www.ey.com/BE/ or www.microsoft.com/belux/.

NAME	CONTACT DETAILS	INFORMATION SECURITY ROLE
PUBLIC BODIES AND ORGANISATIONS		
B-CCENTRE	<p>www.b-ccentre.be Belgian Cybercrime Centre of Excellence for Training, Research and Education Sint-Michielsstraat 6 3000 Leuven Belgium +32 16 32 07 82 contact@b-ccentre.be</p>	<p>The Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE) is a large-scale umbrella joint venture against cybercrime in Belgium, coordinated by the Interdisciplinary Centre of Law and ICT at the KU Leuven. The B-CCENTRE is the main platform for collaboration and coordination with regard to cybercrime matters in Belgium. It combines expertise of academic research groups, industry players and public organisations into a broad knowledge network. Its main activities encompass interdisciplinary fundamental research, organisation of training and awareness raising through education.</p>
CERT.be	<p>www.cert.be Federal Cyber Emergency Team Louizalaan 231 Avenue Louise 1050 Brussels Belgium +32 2 790 33 33 cert@cert.be</p>	<p>CERT.be is the primary Belgian contact point for dealing with cyber-security threats and vulnerabilities affecting Belgian interests. ICT professionals can approach CERT.be free of charge and in complete confidentiality to report cyber incidents (hacked data and network infrastructure, phishing, cyber attacks, etc.). CERT.be also provides citizens and companies with advice on using the Internet safely. More information is available on www.cert.be (for companies) and www.safeonweb.be (for citizens).</p>



NAME	CONTACT DETAILS	INFORMATION SECURITY ROLE
PUBLIC BODIES AND ORGANISATIONS		
CRID	<p>www.unamur.be/droit/crid Centre de Recherche Informatique et Droit Rue de Bruxelles 61 5000 Namur Belgium +32 81 72 40 00</p>	<p>CRID was created in 1979 to improve the IT and law field.</p> <p>CRID has been involved in many cyber-security research projects and has published several white papers on this topic.</p>
ENISA	<p>www.enisa.europa.eu http://cybersecuritymonth.eu/ European Network & Information Security Agency Science and Technology Park of Crete Vassilika Vouton, 700 13 Heraklion Greece +30 28 14 40 9710 info@enisa.europa.eu</p>	<p>The European Network and Information Security Agency (ENISA) is the EU's response to cyber-security issues of the European Union. As such, it is the 'pace-setter' for Information Security in Europe, and a centre of expertise.</p> <p>The objective is to make ENISA's web site the European 'hub' for exchange of information, best practices and knowledge in the field of Information Security.</p>
FCCU	<p>www.polfed-fedpol.be/crim/crim_fccu_nl.php Federal Computer Crime Unit Notelaarstraat 211 Rue du Noyer 1000 Brussels Belgium +32 2 743 74 74</p>	<p>The Belgian Federal Computer Crime Unit (FCCU) is responsible for combating ICT- and cyber-crime with the aim to protect all citizens in the cyber world against all forms of "traditional" and "new" crime.</p> <p>This assignment also includes: combating other criminal phenomena with specialised investigative support in IT environment.</p> <p>Also telecommunications fraud and payment card fraud are among the competencies.</p>
FEDICT	<p>www.fedict.belgium.be Federal Public Service Information and Communication Technology Maria-Theresiastraat 1 rue Marie-Thérèse 1000 Brussels Belgium +32 2 212 96 00 info@fedict.belgium.be</p>	<p>Fedict has launched several internet security awareness campaigns and advises many Belgian governmental agencies on information security.</p>

NAME	CONTACT DETAILS	INFORMATION SECURITY ROLE
PUBLIC BODIES AND ORGANISATIONS		
IBPT-BIPT	<p>www.bipt.be Belgian Institute for Postal services and Telecommunications Ellipse Building - Bâtiment C Koning Boudewijn II laan 35 Boulevard du Roi Albert II 1030 Brussels Belgium netsec@bipt.be</p>	<p>The Belgian Institute for Postal services and Telecommunications (BIPT) supervises both the postal sector and the telecommunication sector, now called electronic communications. BIPT carries out tasks of economic regulation, technical organisation and compliance with the regulatory frameworks.</p> <p>BIPT is involved in the security of public networks and of publicly-accessible electronic communications services.</p>
ICRI	<p>www.law.kuleuven.be/icri Interdisciplinary Centre for Law and ICT Sint-Michielsstraat 6 3000 Leuven Belgium +32 16 32 07 90 adminicri@law.kuleuven.be</p>	<p>The Interdisciplinary Centre for Law and ICT (ICRI) is a research centre at the Faculty of Law of the University of Leuven and has been involved in many information security research projects and has published several white papers on this topic.</p> <p>ICRI is coordinating the B-CENTRE activities.</p>
NATIONAL BANK OF BELGIUM	<p>www.nbb.be National Bank of Belgium de Berlaimontlaan 14 avenue de Berlaymont 1000 Brussels Belgium +32 2 221 21 11 info@nbb.be Specific Operational Functions in the field of prudential supervision tf@nbb.be</p>	<p>The National Bank of Belgium has published detailed guidelines for all financial institutions on information security.</p>
PRIVACY COMMISSION	<p>www.privacycommission.be Belgian Data Protection Authority Drukpersstraat 35 rue de la Presse 1000 Brussels Belgium +32 2 274 48 78 commission@privacycommission.be</p>	<p>The Belgian Data Protection Authority has as core mission to ensure that privacy is respected when personal data are processed. It is a Belgian federal body, working closely together with the Flemish Supervisory Commission for Electronic Administrative Data Flows since December 2009. The Belgian Data Protection Authority has published clear guidelines on how to properly handle privacy incidents in cyber world.</p>
SECURITY OF THE STATE	<p>justitie.belgium.be/nl/overheidsdienst_justitie/organisatie/onafhankelijke_diensten_en_commissies/veiligheid_van_de_staat/ +32 2 205 62 11 info@vsse.be</p>	<p>Security of the State, the civil intelligence and security of Belgium, has as one of its functions: protecting the fundamental values and interests of the state. The Security of the State assists Belgian companies to protect against cyber attacks.</p>



NAME	CONTACT DETAILS	INFORMATION SECURITY ROLE
PRIVATE ORGANISATIONS		
AGORIA	<p>www.agoria.be Agoria Diamant Building A. Reyerslaan 80 avenue A. Reyers 1030 Brussels Belgium +32 2 706 78 00 Ferdinand.CASIER@agoria.be</p>	<p>Agoria, the Belgian federation for the technology industry, supports its 1.700 member companies in the fight against cybercrime through regular events and workshops.</p> <p>The information provided is mainly aimed at CEOs who wish to integrate cyber security aspects in their business strategy.</p>
BELTUG	<p>www.beltug.be Belgian Telecom User Group Knaptandstraat 123 9100 Sint Niklaas Belgium +32 3 778 17 83 Info@beltug.be</p>	<p>BELTUG has a special interest group on security where its members meet and discuss all topics linked to IT security.</p> <p>BELTUG organised a lot of round tables and published several white papers on information security.</p>
FEB / VBO	<p>www.vbo-feb.be Federation of Enterprises in Belgium Ravensteinstraat 4 rue Ravenstein 1000 Brussels Belgium +32 2 515 08 11 info@vbo-feb.be</p>	<p>The Federation of Enterprises in Belgium (FEB) represents more than 50,000 companies, accounting for 80% of employment in the private sector.</p> <p>The FEB is a privileged partner of several public bodies in a number of action programmes to protect the national economy. It has joined ICC Belgium to take the initiative on editing a cyber security guide for all Belgian companies.</p>
FEBELFIN	<p>www.febelfin.be FEBELFIN Aarlenstraat 82 rue d'Arlon 1040 Brussels Belgium +32 (0)2 507 68 11 info@febelfin.be</p>	<p>Febelfin, the Belgian Financial Sector Federation, supports its 268 members in the fight against cybercrime through information sharing and co-operation with all involved stakeholders. Febelfin maintains a special website www.safeinternetbanking.be and has launched several internetbanking security awareness campaigns with provoking videos.</p>
ICC BELGIUM	<p>www.iccbelgium.be Belgian committee of the International Chamber of Commerce Stuiversstraat 8 rue des Sols 1000 Brussels Belgium +32 (0)2 515 08 44 info@iccwbo.be</p>	<p>The International Chamber of Commerce (ICC) is the largest business organisation in the world. Its global ICC Commission on Digital Economy holds discussions regarding cybercrime issues and possible development of ICC guidelines focused on jurisdictional issues faced by global businesses.</p> <p>On the other hand, through its dedicated crime-fighting division (Commercial Crime Services) based in UK, policymaking bodies and other initiatives, ICC combats all types of crime affecting business, including cybercrime.</p>

NAME	CONTACT DETAILS	INFORMATION SECURITY ROLE
PRIVATE ORGANISATIONS		
ISACA	<p>www.isaca.be ISACA Belgium Koningsstraat 109-111 b.5 rue Royale 1000 Brussels Belgium +32 2 219 24 82 president@isaca.be</p>	<p>ISACA is an international not-for-profit knowledge association with more than 110.000 individual members in 160 countries researching value and trust topics around information and technology, including information and information security.</p> <p>ISACA advances and validates skills and knowledge through the Certified Information Security Manager (CISM) and Certified in Risk and Information Systems Control (CRISC) credential.</p> <p>ISACA created COBIT for information security, a business framework that helps enterprises in all industries and geographies govern and manage their information security.</p> <p>ISACA has a large collection of information security white papers, surveys and audit programs.</p>
ISPA	<p>www.ispa.be Rue Montoyerstraat 39 b 3 1000 Brussels Belgium +32 2 503 22 65 Info@ispa.be</p>	<p>ISPA Belgium is the association of Internet Service Providers active in Belgium. By bringing together not only access and service providers, but also hosting and transit providers, ISPA ensures that the potential of the Internet for consumers and businesses in Belgium can be fully achieved.</p> <p>ISPA organises workshops and events on the topic of cyber security, and is involved in multiple projects that contribute to a safer use of the internet in Belgium.</p>



NAME	CONTACT DETAILS	INFORMATION SECURITY ROLE
PRIVATE ORGANISATIONS		
L-SEC	www.lsec.be Leaders in Security Kasteelpark 10 3001 Heverlee Belgium +32 16 32 85 41 info@lsec.be	<p>LSEC is a not-for profit European association, located in Belgium active in information security awareness raising and education over 10 years. The association brings together experts from the ICT security industry, ICT security researchers, and end users to actively collaborate in projects to support the overall improvement in cyber security in Europe. Thought leadership activities organized by LSEC on a monthly basis inform business executives, security managers and security experts on ongoing challenges, best practices and innovative approaches on cyber security and information security.</p> <p>LSEC is an active partner in EC FP7, Horizon 2020 and supports the Digital Agenda. LSEC supports the governments of the Member States with active contributions on policy making and sharing of expertise. LSEC has operations in Belgium, the Netherlands and UK and works with partners in other European Member States. LSEC operates botvrij.be and provides a platform for industry ISACs.</p> <p>www.lsec.be is the portal to information security experts and expertise in Belgium.</p>

INFORMATION SECURITY OVERVIEW LIST

In order to start with, or further improve your information security, we refer you to consult one or more of the following globally recognized good practices, standards and frameworks:

NAME	ORGANISATION	WEBSITE
ISO 22301:2012	ISO	http://www.iso.org/iso/home.html
ISO 27XXX series	ISO	http://www.iso.org/iso/home.html
COBIT5 for information security	ISACA	www.isaca.org/cobit
SP800 series	NIST	http://csrc.nist.gov/publications/PubsSPs.html
Standard of Good Practice for Information Security	ISF	https://www.securityforum.org/tools/sogp/
CIIP and NCSS	ENISA	http://www.enisa.europa.eu/activities/Resilience-and-CIIP
Information security Training Techniques	SANS	http://www.sans.org/reading-room/
BSIMM	BSIMM	http://www.bsimm.com
GAISP	GAISP	http://all.net/books/standards/GAISP-v30.pdf
Good Practice Guidelines	BCI	http://www.thebci.org/index.php/resources/the-good-practice-guidelines
ISAE 3402 and SSAE 16	AICPA	http://isae3402.com/
DMBOK	DAMA	http://www.dama.org
SABSA TOGAF	Open Group	http://www.opengroup.org/togaf/
OCTAVE	CERT	http://www.cert.org/octave/
EBIOS	ANSSI	http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/
PAS 555:2013	British Standards Institute	http://www.itgovernance.co.uk/shop/p-1356-pas-555-2013-cyber-security-risk-governance-and-management.aspx
Information Technology Security Evaluation Criteria / Manual	Bundesamt für Sicherheit in der Informationstechnik	https://www.bsi.bund.de/EN/Topics/topics_node.html



BIBLIOGRAPHY

Allen & Overy. (2012). *EU and U.S. propose new cybersecurity strategies*. London, United Kingdom

Retrieved from

<http://www.allenoverly.com/publications/en-gb/Pages/EU-and-U-S--propose-new-cybersecurity-strategies.aspx>

Bergsma, K. (2011). *Information Security Governance*.

Retrieved from

<https://wiki.internet2.edu/confluence/display/itsg2/Information+Security+Governance>

Bescherm je bedrijf.

Retrieved from

<http://www.beschermjebedrijf.nl>

CERT-EU. (2012). Incident Response – Data Acquisition Guidelines for Investigation Purposes version 1.3.

Retrieved from

http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_004_v1_3.pdf

CERT-EU. (2011). Security White Paper 2011-003 - Guidelines for handling common malware infections on Windows based workstations.

Retrieved from

http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_11_003_v2.pdf

CESG. (2012). *10 Steps to Information security*. Gloucestershire, United Kingdom

Retrieved from

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

Cyber Security Strategy.be.(2012). Belgium.

Retrieved from

<http://www.b-ccentre.be>

EYGM Limited. (2012). *Fighting to close the gap: Ernst & Young's 2012 Global Information Security Survey*.

Retrieved from

[http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/\\$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf](http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf)

Federal Communications Commission, Information security Planning Guide, 2012

Federal Communications Commission. (2012). *Information security Planning Guide*. Washington, DC:

Retrieved from <http://www.fcc.gov/cyber/cyberplanner.pdf>

Information Security Governance Guide.

Retrieved from

<http://searchsecurity.techtarget.com/tutorial/Information-Security-Governance-Guide>

ISACA. (2013). *Transforming Cybersecurity: Using COBIT® 5*. USA

Retrieved from

<http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Transforming-Cybersecurity-Using-COBIT-5.aspx>

Ministerie van Veiligheid en Justitie. (2011). *De Nationale Cyber Security Strategie (NCSS)*. Den Haag, the Netherlands

Retrieved from

<http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking/de-nationale-cyber-security-strategie-definitief.pdf>

Nationaal Cyber Security Centrum. (2013). *Cybersecuritybeeld Nederland*. Den Haag, the Netherlands

Retrieved from

<https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-3/1/NCSC+CSBN+3+3+juli+2013.pdf>

Open Web Application Security Project (OWASP).

Retrieved from <https://www.owasp.org>

Safe on Web.

Retrieved from <http://www.safeonweb.be>.

SANS, Information Security Management, ISO 17799 Audit Check List 1.1, August 2003

World Economic Forum. (2012). *Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines*. Geneva, Switzerland

Retrieved from

http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

EYGM Limited. (2013). *Under cyber attack: EY's 2013 Global Information Security Survey*.

Retrieved from

[http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/\\$FILE/EY-GISS-Under-cyber-attack.pdf](http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf)



ACKNOWLEDGEMENT

DRAFTING GROUP:

B-CENTRE

**Belgian Cybercrime Centre of Excellence for
Training, Research and Education,
ICRI KU Leuven - iMinds**

*Mennens, A.
Smeulders, C.*

EY Belgium Advisory

*Deprez, A.
Dewulf, K.
Wulgaert, T.*

FEB - Federation of Enterprises in Belgium

*Dammekens, A.
Darville, C.*

ICC Belgium - Belgian committee of the International Chamber of Commerce

*Bodard, K.
Deré, J.
Maes, M.
Thomaes, R.*

ISACA Belgium

Vael, M.

L-SEC

Seldeslachts, U.

Microsoft Belgium

*Dekyvere, K.
Schroder, B.*

SWIFT

Cross, R.

STEERING COMMITTEE:

BIPT-IBPT

CERT.BE

ELECTRABEL

ENISA

FCCU

FEBELFIN

FPS Economy

Guldentops, E.

IBJ-IJE

ISPA

UMICORE

VSSE

graphic design & production:
www.in-depth.be

publisher:
ICC Belgium
Stuiversstraat 8 rue des Sols
1000 Brussels
Belgium
+32 (0)2 515 08 44
info@iccwbo.be
www.iccbelgium.be

BELGIAN CYBER SECURITY GUIDE PROTECT YOUR INFORMATION

This Guide and the accompanying documents have been produced jointly by ICC Belgium, FEB, EY, Microsoft, B-CENTRE and ISACA Belgium.