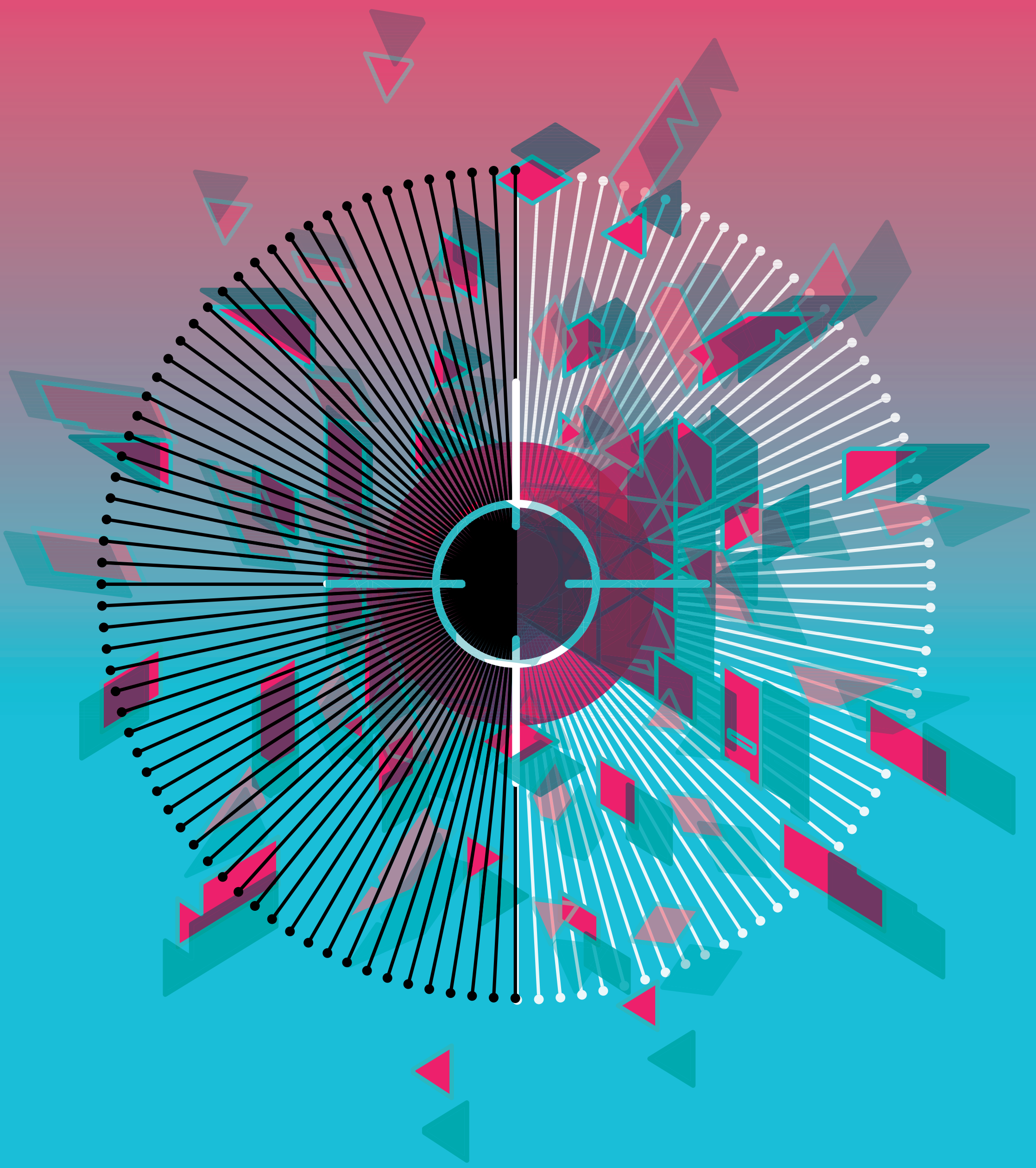
CENTRE FOR
CYBER SECURITY
BELGIUM

CYBER SECURITY
COALITION.be

CYBER SECURITY
INCIDENT MANAGEMENT GUIDE



ABOUT

The Cyber Security Coalition is a unique partnership between players from the academic world, the public authorities and the private sector who have joined forces in the fight against cybercrime. Currently more than 100 key players from across these 3 sectors are active members contributing to the Coalition's mission and objectives.

The Coalition responds to the urgent need for a cross-sector collaboration to share knowledge and experience, to initiate, organise and coordinate concrete cross-sector initiatives, **to raise awareness among citizens and organisations**, to promote the development of expertise, and to issue recommendations for more efficient policies and regulations.

The objective of this guide is to raise awareness within companies of all sizes about the importance of planning the management of cyber security incidents ahead of time.

This Guide and the accompanying documents have been produced by the Cyber Security Coalition.
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. The Cyber Security Coalition disclaims any liability for the content of this Guide.
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.*

EXECUTIVE SUMMARY

This Guide aims to draw attention to the importance of planning how to manage a cyber security incident ahead of time.

Cyber security incident management is not a linear process; it's a cycle that consists of **preparation**, **detection**, incident **containment**, **mitigation and recovery**. The final phase consists of drawing lessons from the incident in order to improve the process and **prepare for future incidents**. During this cycle, **communication** with both internal and external stakeholders is of critical importance.

Many organisations may not have the necessary in-house expertise and skills to respond adequately to a cyber security incident. When they are facing an incident, they may need to call upon **experts** to contain the incident and/or to carry out forensic investigations. This does not mean that they cannot do anything themselves. On the contrary, there are a lot of things that can and should be done before an actual incident occurs.

Drawing up an organisation's **cyber security incident response plan** is an important first step in cyber security incident management. It is also crucial that **top management validates** this plan and is **involved** in every step of the cyber security incident management cycle.
The following elements should be included in the cyber security incident response plan:

- What needs to be protected? Which information, systems, network, products, …?;
- Identification and assignment of **responsibilities**;
- In-house capabilities or contracts with **external experts** for incident response and/or forensic investigation;
- The **equipment and technology**;
- A basic **containment** strategy: disconnect the systems immediately in order to recover as quickly as possible? Or take the time to collect evidence?
- A **communication** strategy for both internal and external stakeholders and for authorities such as law enforcement, the National Data Protection Authority and the competent authorities for reporting Network and Information Security (NIS) incidents.

Operators of essential services (OES) and digital service providers (DSP), as described in the Belgian Network and Information Security Act of 7 April 2019, are subject to specific obligations concerning the security of their information systems and the defence against and reporting of incidents. The information in this Guide may assist in taking the right measures to comply with the latter.

Finally, organisations should consider taking out a cyber insurance policy. The cost of cyber security incidents often amounts to hundreds of thousands or even millions of euros. A reliable cyber insurance policy will cover at least part of this cost.

CONTENTS

FOREWORD

There are only two types of companies: those that have been hacked and those that will be.

Robert Mueller

The Internet is revolutionising the way we do business: the amount of data that we transfer over the Internet and our dependency on it being available keeps on increasing. It is crystal clear that connecting to the world not only brings great opportunities but also generates new risks. Cybercrime is big business and even the smallest malicious attack can seriously damage an organisation's reputation, productivity, ICT system, etc.

No organisation should think it is safe from cybercrime. Cybercriminals do not just target large organisations. On the contrary, a small organisation may be a more interesting victim because of the information it processes or even the partners it works with.

This Guide draws attention to the importance of knowing that one day or another your organisation could be the target of a cyber attack. And when that happens, you need to be prepared! A good cyber security incident response plan can make the difference between a cyber security incident and a cyber security crisis. The pace at which an organisation is able to recognise, analyse and respond to an incident will influence the damage done and the cost of recovery.

Such a cyber security incident response plan should not be limited to technology! Processes, people and other organisational aspects are also important elements to take into consideration.

Reading this Guide will not make you an instant expert in cyber security incident management. Why not? Because it takes time and experience to build up the necessary expertise to be able to efficiently handle cyber security incidents. So, bear in mind that it often involves a growth process of trial and error.

Jan De Blauwe
Chairman of the Cyber
Security Coalition

Miguel De Bruycker
Managing Director Centre for
Cyber Security Belgium (CCB)

BASIC PRINCIPLES & KEY DEFINITIONS

While reading this Cyber Security Incident Management Guide, you should keep the following basic principles and key definitions in mind.

KEY DEFINITIONS

At the end of this Guide you will find a complete glossary. Hereafter we will highlight a number of definitions that are key to understanding the scope and content of this Guide.

CYBER SECURITY EVENT
A cyber security change that may have an impact on organisational operations
(including mission, capabilities, or reputation).

CYBER SECURITY INCIDENT
A single or a series of unwanted or unexpected cyber security events that are likely to compromise organisational operations.

CYBER SECURITY INCIDENT MANAGEMENT
Processes for preparing, detecting, reporting, assessing, responding to, dealing with and learning from cyber security incidents.

1. There is no simple one-size-fits-all solution

Always keep in mind that every organisation is different. When it comes to Cyber Security **there is no one-size-fits-all solution**. What will work for your organisation will depend on its mission and goals, the kind of infrastructure and information you are protecting, available resources, etc. Finally, recognise that some techniques will only be learned with **time and experience**. This should not, however, stop you from getting started!

2. Top management's commitment

Cyber security incidents are a risk that should be incorporated in the overall risk management policy of your organisation. Furthermore, managing cyber security incidents does not just mean applying technology. It also requires the development of a plan that is integrated into the existing processes and organisational structures, so that it enables rather than hinders critical business functions. Therefore, top management should be **actively involved** in defining an organisation's cyber security prevention and incident response plan, because top management's explicit support through appropriate internal communication and the **allocation of personnel and financial resources** is key to the success of the plan.
A well-informed top manager will be aware both of the risks of cybercrime and of his/her own **exemplary role** in encouraging all members of the organisation to assume their responsibility.

3. Involve every member of your organisation

It is often said that humans are the weakest link when it comes to cyber security. Having said that, it is also important to realise that the members of your organisation have great potential to help you detect and identify cyber security incidents. Make sure that every member of your organisation is **aware of your cyber security incident response plan and of their own role** within it, even if this just means informing the right person about the ICT anomalies they stumble upon.

4. Keep an offline copy of the documents you need during an incident

Bear in mind that when a cyber security incident occurs, you may not always have access to the files on your computer. It is always a good idea to keep a **hard copy/offline copy** of any document you are likely to need during a cyber security incident or crisis.

5. Don't link backups to the rest of your system

When it comes to backups, not only is it crucial to have them, it's also very important to have a **backup that is not linked in any way to the rest of your system**. If your backup is linked to your system, chances are that the infection of your system also spreads to your backup, which makes your backup useless.

6. The importance of logging and keeping those logs for a certain period of time (up to 6 months)

Logs can help you to trace back the origin of the cyber security incident. This is not only important to be able to identify the cybercriminal; it can also help your organisation to get back to business as soon as possible.

7. Keep your cyber security response plan and all related information and documents up to date!

8. Make sure you take all legal aspects into account when managing a cyber security incident

Evidence will only be admissible in court if it has been collected in respect of all applicable laws and regulations. Furthermore, in some cases you have a duty to report to the authorities or relevant people, e.g. the National Data Protection Authority or the relevant competent body for reporting Network and Information Security incidents.

9. Document every step of a cyber security incident

In times of crisis, don't just rely on your head! Make sure you write down any action that is taken, such as the reporting of the incident, the collecting of evidence, conversations with users, system owners and others, etc. This documentation is your 'time machine'. When something goes wrong it may allow you to look back and evaluate where and why the problem started. Furthermore, documenting the cyber security incident response will ensure that the knowledge regarding what is going on is not just in a few people's heads.

01 PREPARING FOR A CYBER SECURITY INCIDENT

1. DRAFT A CYBER SECURITY INCIDENT RESPONSE PLAN AND KEEP IT UP TO DATE

When facing a cyber security incident, an organisation should be able to react in a prompt and appropriate manner. This is why it is important to decide how you will handle certain situations ahead of time instead of when you encounter them for the first time during an incident. Make a plan (on paper, not just in your head) to limit damage, to reduce costs and recovery time and to communicate with both internal and external stakeholders.

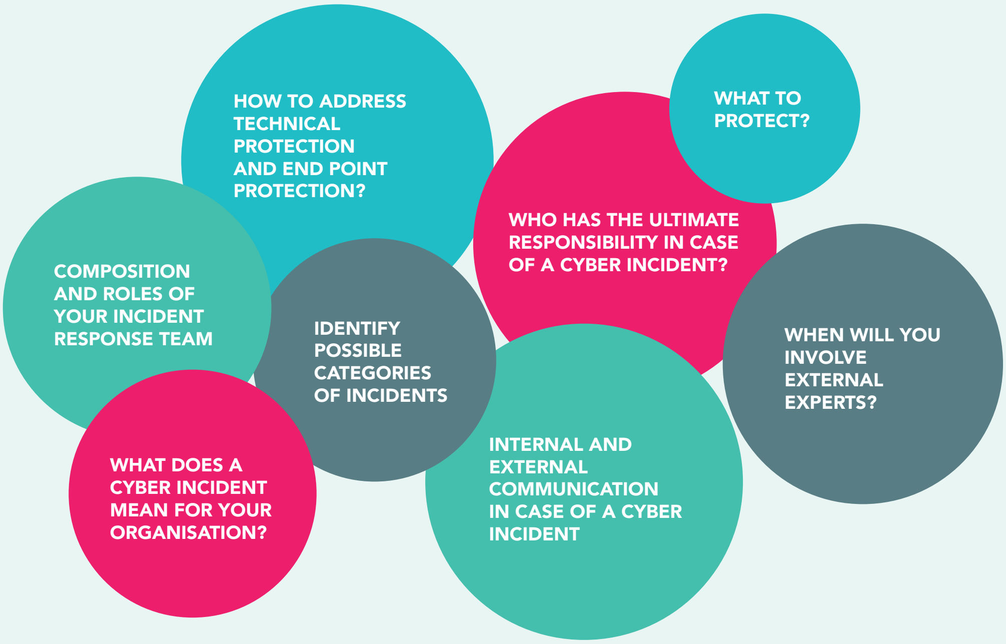
REVIEW YOUR CYBER SECURITY INCIDENT RESPONSE PLAN

A cyber incident response plan is not a static document. It is important to integrate it into your business processes and to review and update it regularly, on a yearly basis and as part of the post-incident review.

CYBER SECURITY INCIDENT RESPONSE PROCEDURES

Building on your cyber security incident response plan, you can define a number of standard operating procedures for common incidents that are likely to occur within your organisation. Such a procedure should explain step by step how a specific issue can be tackled. These quick response guides for likely scenarios should be easily accessible.

KEY ELEMENTS OF A CYBER SECURITY INCIDENT RESPONSE PLAN



HOW TO ADDRESS TECHNICAL PROTECTION AND END POINT PROTECTION?

WHAT TO PROTECT?

WHO HAS THE ULTIMATE RESPONSIBILITY IN CASE OF A CYBER INCIDENT?

COMPOSITION AND ROLES OF YOUR INCIDENT RESPONSE TEAM

IDENTIFY POSSIBLE CATEGORIES OF INCIDENTS

WHEN WILL YOU INVOLVE EXTERNAL EXPERTS?

INTERNAL AND EXTERNAL COMMUNICATION IN CASE OF A CYBER INCIDENT

WHAT DOES A CYBER INCIDENT MEAN FOR YOUR ORGANISATION?

II. CONTENT OF A CYBER SECURITY INCIDENT RESPONSE PLAN

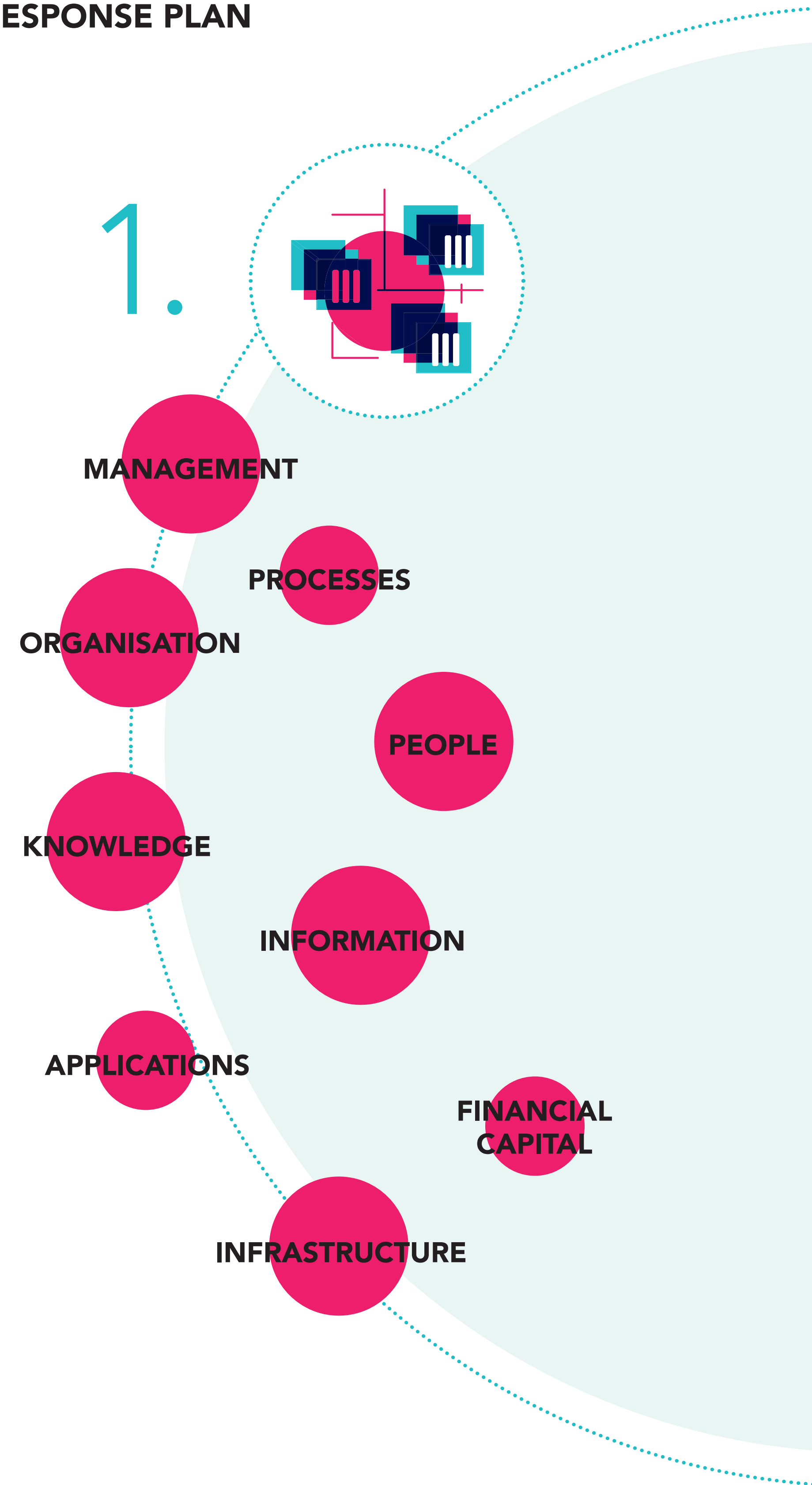
KNOW WHAT TO PROTECT

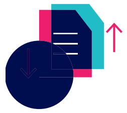
Identify your assets and potential threats

When hit by an incident, the first questions that will arise are: which assets are at risk and which of those assets are vital for your business activities? You will have to decide which assets need your attention first in order to remain in business and keep the damage to your business as minimal as possible.

That's why it is crucial to **identify, document and categorise your organisation's 'vitals**': the assets your organisation depends on to conduct its core activities. This will help you identify where to apply which protective measures and to take quick and justified decisions during the incident management process.

The following list gives you an idea of what those 'vitals' could be: management, organisation, processes, knowledge (e.g. intellectual property has been stolen), people, information (e.g. data sets have been stolen or altered), applications (e.g. website is down or defaced, infrastructure (e.g. system and/ or network connections are down), financial capital (e.g. bank accounts).
It's also a good idea to identify vulnerabilities and potential threats.

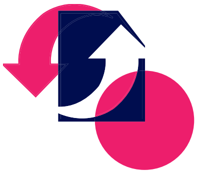




2. How to identify, document and categorise your organisation's vitals, vulnerabilities and potential threats

A. Identify the business and the resources that need to be protected

- Determine which of your core business activities enable your organisation to exist and achieve its corporate objectives and generate income: produce goods, sell goods, deliver goods, etc.
- For each of those activities, identify which ICT systems (databases, applications, control systems) and network connections are supporting them
- Determine also where these ICT systems are located: on your own servers or in the cloud?
- When identifying these assets, don't forget flows of information to third parties (suppliers, clients, etc.) or industrial control system flows.

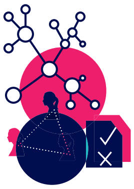


B. Identify your crown jewels

Determine now which assets, data, processes or network connections are so important for your organisation that if you lose (control of) them, you are in big trouble or even out of business

C. Assign business priorities for recovery

This act of prioritising will determine the order in which the systems will be re-established. In most cases the underlying network will need the highest priority, as this is not only the path by which your system administrators reach your assets but also the path that cyber criminals use to attack your systems. As long as criminals can use your network connections, any other recovery activity might be undone by them. When assets are equally high priority, parallel recovery activities might be considered.



D. Document how your systems work and keep this documentation up to date

Ensure that the way your systems work is documented and that this
information is kept up to date and available on the incident response team's documentation systems. Absolutely essential documents are:

Network Scheme displaying the network architecture with internal network segmentation and the different gateways to external networks, DMZ, VPN, IP-address ranges used. This scheme should also include the different security devices in place that might contain logging information of network activity (firewalls, (reverse) proxy servers, intrusion detection systems, security incident event management systems). For larger companies with complex networks, it is also necessary to have a high level version of the network architecture so that you can quickly get an idea of the network in case of emergency.

Equipment and services inventory. This inventory will include, for the vital assets in your environment, all the different servers and the network components used for delivering the different corporate services. As some of these (physical) servers might be servicing multiple business functions, it is important to know which services are running on which server.

Account and access lists. At all times it is important to know who has the right to access, use and/or manage your network and the different systems in it. This will allow you to detect any strange or abused accounts during an incident.

Make sure your systems are not just a bunch of cables and computers to you! It is crucial that your system manager knows how your network works and is able to explain it to experts, police, etc.

III. ASSIGNING RESPONSIBILITIES AND CREATING A CYBER SECURITY INCIDENT RESPONSE TEAM

ASSIGNING RESPONSIBILITIES AND ROLES TO PEOPLE WITH THE RIGHT SKILLS

It is important that the roles and responsibilities in case of a cyber security incident are documented in your cyber security incident response plan. When drafting the description of these roles and responsibilities, you should ask yourself the following questions:

1. Who is the internal contact point for cyber security incidents? And how can he/she be contacted?
2.What are the different incident response tasks? And who is responsible for doing what?
3. Who is managing the incident from the business/technical side? This should be someone within your company with decision-making authority, who will follow the incident from start to finish.
4. Who will liaise with senior management?
5. Who can engage the external incident response partner?
6. Who can file a complaint with law enforcement/inform the regulatory bodies?
7. Who is entitled to communicate with the press and external parties?

You will realise that in order to adequately address a cyber security incident, different skills are needed to take on the different responsibilities and necessary roles in an efficient incident response.

SKILLS	RESPONSIBILITIES	ROLES
Incident management	Managing the cyber security incident from the moment of its detection until its closure.	Cyber security incident response manager
Business decision capability	Assessing the business impact and acting upon it. Engaging the right resources. Taking decisions on how to proceed, e.g. deciding if the internet connection of a compromised system can be shut down and when is the most appropriate time. Deciding when to start clean-up activities. Deciding whether to file a complaint.	Management
Network management capabilities	Technical know-how on the organisation's network (firewall, proxies, IPS, routers, switches,…). Analysing, blocking or restricting the data flow in and out of your network. IT operations, information security and business continuity.	ICT technical support staff
Workstation and server administrator capabilities (admin rights)	Analysing and managing compromised workstations and servers.	ICT technical support staff
Legal advice	Assessing the contractual and judicial impact of an incident. Guaranteeing that incident response activities stay within legal, regulatory and the organisation's policy boundaries. Filing a complaint.	Legal department/ company lawyer
Communication skills	Communicating appropriately to all relevant stakeholder groups. Answering customers, shareholders, press questions immediately.	Communications or public relations department
Forensic skills	Gathering and analysing evidence in an appropriate way, i.e. so that the evidence is admissible in a court of law.	ICT technical support staff
Physical security	Handling the aspects of the incident that are linked to • the physical access to the premises • the physical protection of the cyber infrastructure.	Security Officer
Crisis management	Crisis management	Crisis manager

CYBER INCIDENT RESPONSE TEAM

In an ideal world every organisation has an incident response team that is convened whenever there is an incident. Of course, the size of the company determines the size and structure of the incident response team. Smaller companies that do not have the resources for an actual team could designate a first responder – ideally someone with business decision capability – from among their personnel. In case of a cyber security incident, he/she should contact external help but will remain the person ultimately responsible for the incident response within the organisation.

The composition of this incident response team will be determined by the different skills that are needed to handle an incident (see also: table on page 11). For smaller companies, some of these skills may have to be sourced outside the organisation by the first responder.

A MINIMAL INCIDENT RESPONSE TEAM SHOULD INCLUDE THE FOLLOWING ROLES

INCIDENT RESPONSE MANAGER

The person that will manage the incident as soon as it is brought to their attention until it has been contained and remediated. He/she will liaise the investigation of the indicators, the with management, and possibly with other internal staff and with external resources to handle the incident. This person has to have knowledge about your organisation's business activities because they will be the first to take business decisions.

ICT TECHNICAL SUPPORT STAFF

This person needs to have a good knowledge of your ICT infrastructure as they will be responsible for the investigation of the indicators, confirmation of the incident and developing the technical solutions to manage the incident.

YOUR ORGANISATION'S SIZE AND NATURE WILL DETERMINE IF MORE ROLES ARE NECESSARY

Smaller organisations often have the flexibility to quickly engage corporate management in order to manage the incident. This is not the case for larger organisations that might have to handle several incidents in a more autonomous mode, in which case corporate executives will only be engaged in incident response actions when a very serious incident occurs.

Larger organisations. The bigger your organisation, the more differentiated the composition of your incident response team will have to be. For larger organisations, in addition to the incident response team, a crisis management team composed of corporate management representatives might be set up to take over the responsibility for strategic and business-related decisions and communications when confronted with serious incidents. This will enable the incident response manager to focus more on the technical issues of the incident.

CERTAIN ORGANISATIONS MUST APPOINT A DATA PROTECTION OFFICER OR A CONTACT POINT

The General Data Protection Regulation (GDPR) obliges certain organisations to appoint a Data Protection Officer or 'DPO'. More specifically those organisations involved in processing personal data and that require regular and systematic observation on a large-scale of those concerned, or are charged with large-scale processing of special categories of data, for example, health-care data, or criminal convictions or offences.

The Network and Information Security (NIS) Directive requires operators of essential services (OES) and digital service providers (DSP) to appoint a contact point for the security of network and information systems in order to allow seamless communication with the competent authorities in the case of incidents.

IV.

CALL UPON EXTERNAL EXPERTS

EXPERTS ON CYBER INCIDENT RESPONSE

Whether your organisation is an SME or a large organisation, it is costly to develop and maintain all the necessary expertise and skills for incident response in house. This is especially true for forensic and legal advisory cyber security incident response skills. So bear in mind that it might be more cost-effective to call upon external cyber security incident response partners to close the gap in your organisation's skills base.

- Professional incident responders with their knowledge of possible threats and scenarios might reduce the **time** for diagnosing the incident.
- They take a forensically sound approach so that any evidence will be secured and documented according to a **legally valid** chain of custody. This evidence can then be presented later in court if necessary.
- They have experience of doing things in the right order and have the **tools** for recovering traces from RAM memory, virtual machines, hard disks and networks.
- These experts will help you to identify **the causes** of the incident and will offer advice on how to contain, eradicate and remediate the incident.

WHEN TO CONTACT AN EXPERT?

A. DURING THE PREPARATION PHASE

VS

B. WHEN A CYBER SECURITY INCIDENT OCCURS

You can either contract and retain a cyber security incident response partner during the preparation phase, or wait until an actual cyber security incident occurs. Bear in mind that establishing such a contract takes time and effort. **So if you are sure you will need external help, it might be better not to wait.** This way you will win precious time at the beginning of the cyber security incident. Several specialised consulting firms for incident response services and law offices offer subscriptions that keep their incident response capabilities on retainer for the subscriber. Furthermore, most of these include training sessions with your incident response team to facilitate cooperation between them when an incident occurs.

CERTAIN AUTHORITIES MIGHT BE OF HELP TO YOUR INVESTIGATION

Other parties like industry regulators, the National Data Protection Authority, the Centre for Cyber Security in Belgium (CCB), Cert.be department, and law enforcement (police and magistrates) might be of importance when you're confronted with a cyber security incident of a criminal nature or in case of a personal data breach. Some legislation even obliges you to inform these parties when you have detected an incident of a specific nature (see also: page 31, Reporting to authorities).

These parties can often help with information on the threat and with practical guidelines based on previous incidents they have handled. Do bear in mind, though, that the objective of law enforcement is to identify and catch the attacker. It is not their task to get your business up and running again. It is also possible that the most effective way to catch the attacker is not necessarily the same as the fastest way to get back to business as usual.

Furthermore, most of these investigations are covered by professional secrecy, which makes it rather difficult to obtain information about their results. They might, however, disclose information that will help you to identify the attacker and their modus operandi, which may speed up the analysis of your cyber security incident.

The police might ask your organisation not to shut down your system right away. If you do, the attacker will notice and retreat, which often makes it impossible to trace them afterwards. However, for your organisation the fastest way to get back to business might be to shut down immediately and start with a clean slate.

V. EQUIP YOUR ORGANISATION TO ADDRESS A CYBER SECURITY INCIDENT

YOUR NETWORK OF EXPERTS – MAKE A CONTACT LIST

Seeking help from the right professionals at the right time is crucial during an incident, as it might help limit the physical and reputational damage to your company. A contact list that includes all of these people or organisations will help you in this process. This list contains the names, roles, contact and backup details of the different members of the cyber incident response team, the external parties on retainer, law enforcement, etc.

Contact information that is recorded should include landline and mobile phone numbers, business e-mail addresses (including public encryption keys for confidentiality & integrity of communications) and physical addresses for traditional mail and packages. Make sure you also have alternative contact options (secondary e-mail addresses, fax numbers), because it is possible that the incident response team will not be able to use the internal network during the incident.

This contact information should be available in a central, offline location, such as a physical binder or an offline computer. Next to 'raw' contact information, this emergency information should also include escalation procedures. This information must be both readily available and kept extremely physically secure. One method of securing and making this information readily available is to encrypt it on a dedicated security portable computer that is placed in a secure vault, and limit access to the vault to authorised individuals such as the incident response team leader and the Chief Information Officer (CIO) or the Chief Technology Officer (CTO).

For a comprehensive fill-in form see **Sans Institute**

NAME	ORGANISATION	ROLE	CONTACT DETAILS
Ms. Incident Response Manager	In house/external	Cyber incident response management	Address Telephone E-mail **Weekend and backup** contact info
Mr. Lawyer	In house/external	Legal expert	
Ms. Forensic	External	Forensic expert	
Mr. Police	Law enforcement	Law enforcement	

HARDWARE AND SOFTWARE FOR CYBER SECURITY INCIDENT MANAGEMENT

To improve the maturity and efficiency of the incident response team, the appropriate tools need to be in place. It is important that the incident response team has at is disposal autonomous systems and tools allowing them to handle an incident even if the corporate network has been compromised. This means that when your organisation's systems or networks are no longer available, the incident response team's system still is. Incident procedures and contact lists have to be available on these systems.

VI.

PREPARE YOUR COMMUNICATION STRATEGY

Communication is a **vital component** of every step in the cyber security incident response. You want to control the communication flow to ensure **the right information** is communicated **at the right moment** by the **right senders** to the **right recipients**. This is valid both for internal communication and communications to the outside world. We recommend coordinating all external communications with the Legal and the Public Relations representatives.

WHAT TO COMMUNICATE AND WITH WHOM?

The type of incident and its (potential) impact will define the type of communication that is required. For example, an internal fraud case or internal hacking attempt will most likely not warrant communication with the media to disclose the incident. On the other hand, when the personal data of an organisation’s customers are leaked it would be a good idea to contact at least those customers and the National Data Protection Authority, and to prepare a press statement. Furthermore, all communications should strike the right balance between transparency and protection. In most cases, internal communication will be more transparent than external communication. Even for internal communication, however, a principle of ‘need-to-know’ should be respected.

IDENTIFY INTERNAL AND EXTERNAL STAKEHOLDERS

During the incident response activities, there will be a constant need for information from many different stakeholders. Each of them will need a different type of information. Make your own list of potential stakeholders and ensure that the right contact information is available! (See also the table on page 15.) Note that the organisation should have this contact information available, but does not always need to communicate with all parties.

WHO? INTERNAL STAKEHOLDERS	WHAT? TYPE OF INFORMATION THIS STAKEHOLDER NEEDS
Senior management	What is impacted? What is the response? What is the expected outcome and when will operations be back to normal?
Impacted business managers	When will normal operations be resumed?
Employees	What should an employee do? How long is this situation expected to last?

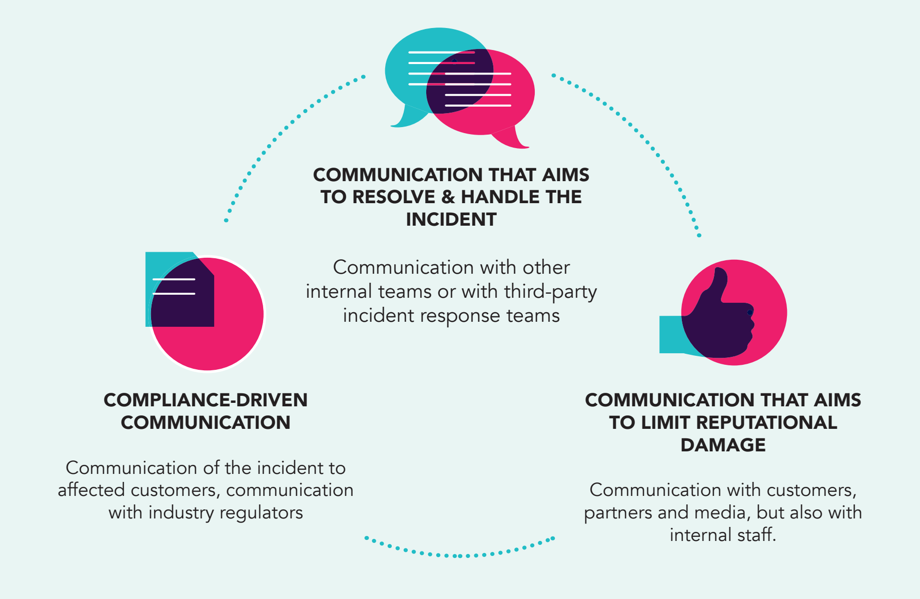
WHO? INTERNAL STAKEHOLDERS	WHAT? TYPE OF INFORMATION THIS STAKEHOLDER NEEDS
Media	A statement on the incident and its impact. For higher profile companies and/or incidents, the media might be involved. Media attention to a security incident is rarely desirable but can sometimes be unavoidable. Media attention can enable your organisation to take a proactive stance in communicating the incident, thereby showing your commitment to and capacity for handling the incident. The communication plan should clearly define the individuals authorised to speak to media representatives (typically public relations or legal departments).
Customers	Are they potentially impacted by the cyber security incident? Were their (personal) data lost or stolen? Are they potentially the primary target of the attack? In some cases there is a legal obligation to contact the industry regulator (see also: page 31, Reporting to authorities).
Suppliers	Are they potentially impacted by the cyber security incident? Are they potentially the primary target of the attack?
Other (partner) cyber security response team	Communication with other incident response teams can provide technical assistance, thereby offering faster resolution (e.g. they might have seen/handled this type of incident before). This type of communication would typically include technical details on the evidence identified.
Internet service provider	Communication with your Internet service provider can provide technical assistance, thereby offering faster resolution (e.g. they might have seen/handled this type of incident before). This type of communication would typically include technical details on the evidence identified.

WHO? INTERNAL STAKEHOLDERS	WHAT? TYPE OF INFORMATION THIS STAKEHOLDER NEEDS
National Data Protection Authority	Was there a data breach? Which data subjects are concerned? In some cases there is a legal obligation to contact the National Data Protection Authority (telecom and GDPR). (See also: page 31, Reporting to authorities).
CCB (Cert.be dept)	Technical details on the evidence identified
Police	Do you wish to file a complaint? If the event caused a substantial impact and there is a suspicion of criminal intent, you might want to report the incident to the law enforcement authorities. They will need legal and technical information.
Industry regulators	What kind of incident? What is the status of the incident? In some cases there is a legal obligation to contact certain authorities or the industry regulator (see also: page 27, Reporting to authorities).

Organisations should bear in mind that once a party has been informed, they will request periodical updates related to the incident in question. There is typically no 'one-off' communication and the communication schedule should take these periodical updates into account.

THE IMPACT OF THE INCIDENT WILL DETERMINE THE COMMUNICATION OBJECTIVES

In order to know what to communicate and to whom, an organisation should assess the (potential) impact of the cyber security incident: e.g. are only internal or also external stakeholders concerned? Is there a data leak? Depending on this impact, your cyber security incident communication will have different objectives, for example:



COMMUNICATION THAT AIMS TO RESOLVE & HANDLE THE INCIDENT

Communication with other internal teams or with third-party incident response teams

COMPLIANCE-DRIVEN COMMUNICATION

Communication of the incident to affected customers, communication with industry regulators

COMMUNICATION THAT AIMS TO LIMIT REPUTATIONAL DAMAGE

Communication with customers, partners and media, but also with internal staff.

ENSURE MULTIPLE COMMUNICATION CHANNELS ARE AVAILABLE

The incident could impact existing communication channels (e.g. compromise e-mail systems). As an organisation, alternative secure communication channels should be available. Several communication methods are available and it is up to the organisation to select the method most suitable for a particular incident.

A **best practice** used by many organisations is to use a conference bridge number that can be set up instantly. The incident response team and all stakeholders should be informed about the access numbers but not about the control number necessary to set up a conference. This is typically done by a crisis manager who is responsible for managing, controlling and organising crisis calls.

POSSIBLE COMMUNICATION METHODS

- E-mail (preferably using PGP for confidentiality and integrity of communications)
- Website (Intranet for employees, public website,…)
- Telephone calls
- In person (e.g. daily briefings)
- Paper (e.g. post notices on bulletin boards and doors, hand out notices at all entrance points)

VII.

CYBER INSURANCE

Certain insurers offer customised insurance policies that are always preceded by an analysis of the risks specific to the organisation in question. This analysis allows the organisation to determine if and to what extent it needs cyber security insurance. The risk analysis will also be used by the insurer to determine the cover required. Factors that are taken into account are:

- business exposure: high technology with exclusive production process and in-depth Research & Development
- type of distribution network: e-commerce
- amount and type of data (critical or not), the existence of a legal framework.

RECOVERY COSTS IN CASE OF LOSS OF DATA

POTENTIAL LOSS OF TURNOVER

ADDITIONAL COSTS ASSOCIATED WITH THE DETECTION AND RESOLUTION OF INCIDENTS

COST OF COMMUNICATION IN THE EVENT OF AN INCIDENT

Compensation is paid out above an excess negotiated with the policyholder. The amounts insured per claim and/or per insurance year are always determined according to the needs of the company and the capabilities of the insurance company.

02 DETECTING AND IDENTIFYING POTENTIAL CYBER SECURITY INCIDENTS

I. CATEGORIES OF INCIDENTS

DEFINE CYBER SECURITY INCIDENT AND RELATED TERMS

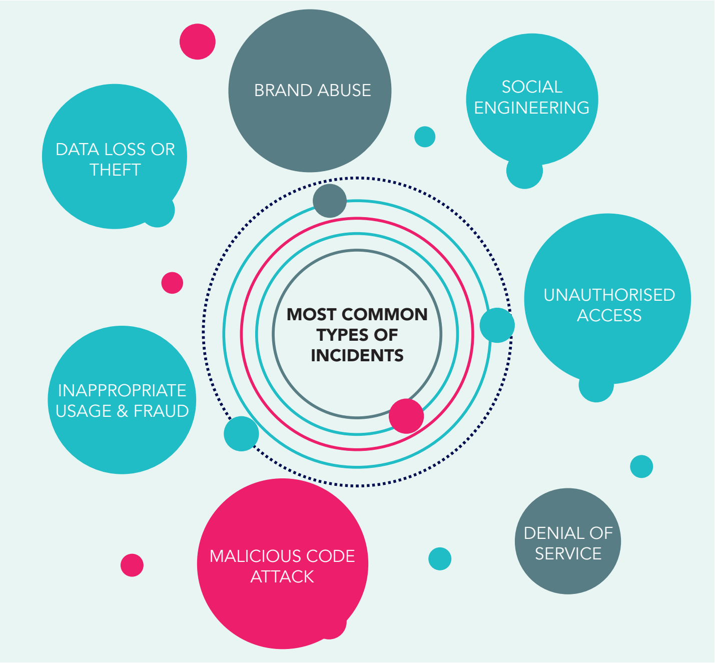
To start with, it is a good idea to define 'cyber security incident' and related terms within your organisation. This will make the communication on the incident a lot more efficient. You can find inspiration for these definitions in the preliminary chapter of this Guide under Basic Principles and Key Definitions. You should, for example, decide when a cyber security event becomes a cyber security incident for your organisation. In other words, what kinds of cyber security events are likely to have an adverse impact on your organisation's activities?

IDENTIFY POSSIBLE CATEGORIES OF CYBER SECURITY INCIDENTS

To be able to detect and identify cyber security incidents, you need to have at least an idea of what you are looking for. Therefore, having a list of the categories of cyber security incidents that are most likely to hit your organisation is no luxury. Furthermore, when you detect a cyber event, it is often difficult to know how bad the consequences will be from the start. This doesn't however change the fact that you have to proceed. Categories of incidents allow you to prioritise cyber events and take decisions accordingly. This section offers a typology of a number of cyber security incidents. The intention is not to present a 'definitive' overview of all types of incidents, but simply to give you an idea of the most common types of incidents (at the time of writing). Incidents can belong to more than one category. A more detailed explanation of these incident types can be found in the Annex.

USB STICK OR USB SPY?
In 2013 Russia hosted a meeting of the G20 leaders. At the end of this event all participants, amongst them Herman Van Rompuy, received a gift bag containing a USB pen drive and a mobile phone charging device. Although the Kremlin has always denied it, both devices were reported to be capable of secretly downloading information, such as e-mails, text messages and phone calls from laptops and phones.

A CRYPTOLOCKER CAN ALSO ENCRYPT YOUR BACKUP
A company receives an e-mail with an invoice in attachment that looks like one from their suppliers. The company's accountant clicks on the attachment and a few seconds later a message appears on his screen: "All your information has been encrypted! If you want the key to unlock the encryption, you need to pay me 1,000 Bitcoins". The company doesn't want to pay the cybercriminal. After all, there is no guarantee that they will actually return the lost data once they have received the ransom. To recover its data, the company decides to restore from a backup. When the company wants do this, the employees notice that, since the backup was linked to the system, it has also been encrypted...



II.

METHODS FOR DETECTING INCIDENT

YOUR ORGANISATION'S PERSONNEL HAS THE POTENTIAL TO DETECT

People are often considered the weakest link when it comes to cyber security. However, they also have the greatest potential to help an organisation detect and identify cyber security incidents. Make sure that every member of your organisation is aware of cyber security risks and of the role that they can play in detecting them. Turn them into your human firewall! Every member of your organisation should know how to report something abnormal on their computer or mobile device. Make sure that the contact details for doing so are readily accessible and that it is easy to contact this person .

To organise incident reporting by personnel (and other partners), make available the following:

- A phone number for reporting emergencies
- An e-mail address for informal incident reporting
- A web-based form for formal incident reporting

TECHNOLOGY AND ENDPOINT PROTECTION

Technology

Technology is one of the main enablers when it comes to your incident detection, investigation, eradication and recovery. When an incident has occurred, ad-hoc deployment of technology is still possible, but your investigation will often be limited to the current events. Implementing the right technology during the preparation phase will allow you to get a comprehensive picture of current and past events. This gives your organisation a better chance of tracing the incident back to its roots.

Endpoint protection

An endpoint is a device that is connected to your organisation's network, such as laptops, smartphones, etc. Each of these devices is a potential entry point for cybercriminals. Therefore, it is important that all of those devices are adequately protected.

DETECTION TOOLS

Each detection tool (e.g. IDS) has a specific purpose and is able to monitor from a different perspective: network-based or host-based. Given the variety of different threats, the tools should be using and be tuned to the correct inputs.

From a network perspective

A good start would be the implementation of an intrusion prevention system, such as Snort network IDS sensor, on the Internet uplink. Additionally, many organisations are unaware that they already have a lot of information that can be used to detect an incident. This can be in the form of:

- access logs to servers and appliances;
- operational logs from systems (e.g. process creation);
- firewall policy logs.

This data can be used to create rules and trends, which help in detecting unexpected or invalid traffic (e.g. traffic to uncommon websites, login attempts by non-existent users, etc.).

To avoid malicious code, keep your software, virus scanners, etc. up to date!

Regularly update your software or install patches when they are available.

Don't use unsupported versions of software such as Windows XP and Windows 2003. Unsupported means that the software is no longer updated and your computer is no longer protected against new, known malware.

From a host perspective

Anti-virus solutions are not sufficient to fend off advanced attacks against endpoints. Many malwares today are polymorphic (they change depending on the behaviour of the host), which makes them hard to detect based on static signatures by classic anti-viruses. Advanced endpoint protection tools investigate suspicious behaviour and can thus be more effective in many cases.
This does not mean however that anti-virus solutions should not be deployed. On the contrary, anti-virus is needed to cover most of the more widely recognised threats.

03 HANDLING AN ACTUAL INCIDENT: CONTAIN, ERADICATE AND RECOVER

In this chapter you will find out what you should do to regain control once you have detected a cyber security incident. Important decisions will have to be taken about how to contain the incident, how to eradicate it and how to recover from it. Validation of these decisions by your organisation's top management is absolutely vital. Incidents can belong to more than one category.

I. CONVENE YOUR CYBER SECURITY INCIDENT RESPONSE TEAM

When an actual incident is detected, it is very important to evaluate the risks quickly in order to take the right measures. The cyber security incident manager should be informed immediately and convene a meeting of the cyber security incident response team, if your organisation has one (see also: page 12, Cyber Security Incident Response Team). The cyber security incident manager and his/her team will report to the CEO, who will have to validate their decisions.

II. SITUATIONAL AWARENESS

After the detection of an incident, it is essential to collect all available information on the activities around the incident's timeframe. Central collection and archiving of security information (e.g. system logs, firewall policy logs) provides the analyst with easy access to this information. Important factors to take into account are integrity of the information and indexation.

A forensic investigation might be required to collect all artefacts and to examine the magnitude and depth of the attack. Tools to create and analyse full disk images, and take (remote) memory dumps of a suspicious machine and write-blockers are useful for performing this analysis.
To detect the magnitude of the incident, the artefacts or the indicators collected as part of the initial investigation can subsequently be used to search for further intrusions on a large scale over all managed devices. Having a central management point that is able to query them can speed up this process. You should also verify if any data have been lost/stolen.

RISK DETERMINATION OF PERSONAL DATA BREACH

A key element in dealing with a personal data breach is determining the risk level of the breach in question. How serious is the breach and the possible consequences for the person whose data was breached? The answer to that question is an important factor in determining the steps to be taken. Each risk level (no risk, risk, high risk) requires a different approach, especially in the context of the notification obligation. Therefore, an exact and consistent risk assessment is the key to effectively addressing a personal data breach. This ensures that the right actions are taken to comply with the legislative provisions.

An assessment of a personal data breach in its entirety makes it possible to formulate an adequate and realistic risk level, and to take the right follow-up steps. In order to be able to evaluate the risks to the rights and freedoms of individuals, a number of elements must be taken into account. The main elements are described below:

Nature and sensitivity of personal data	Sensitive data The more sensitive the personal data, the higher the risk of harm to the affected individuals. Publicity of the data In addition to the sensitivity of the leaked data, the level of publicity already given to the data is also important. It must be checked whether the personal data of the individual was already (publicly) accessible. Linked personal data Data breaches involving health data, identity documents, or financial data, such as credit card information, can all cause damage in their own right, but combined with publicly available information, serious crimes such as identity theft can also be committed. For that reason, linked personal data pose a higher risk than an isolated category of personal data.
Amount of personal data and number of affected individuals	This element looks at the amount of information affected by the breach and the total number of individuals whose data has been affected. The more data and individuals affected, the higher the risks.
Ease of identifying the individuals	This element focuses on how easy it will be for a party with access to the leaked data to identify an individual (possibly after comparison with additional information available). The risk depends on whether individuals can be identified directly without any other personal data, or whether additional information from other categories of data is needed to identify the individuals.
Seriousness of the consequences	The potential harm done to the individuals, and the seriousness of the harm must be determined. Data breaches can be extremely damaging, causing physical harm, psychological stress, humiliation or reputational damage in cases such as identity fraud. If the leak concerns the personal data of vulnerable individuals (e.g. patients, children), a higher risk of damage can be attributed.
xisting mitigating measures	Mitigating measures already in place during the data breach should be taken into account in the overall risk assessment; by asking whether, and how, these measures protect the affected individuals.

Register of data breaches

Due to the principle of liability, all considerations and conclusions arising from the risk assessment must be documented in a data breach register. This register must contain at least the following items:

Date and time of the data breach	The exact date and time the organisation became aware of the personal data breach. This information is important to meet the 72-hour deadline for notification from the data protection authority, and any data subjects.
Timeline and description of the data breach	Descriptions of events related to the personal data breach: when the breach was reported, when the breach (probably) occurred, an overview of the affected systems, and other descriptions.
Contact person	It is important to have a central contact person who is informed about the circumstances of the personal data breach, and who can be contacted in case of follow-up questions. Usually, the person who reported the leak is the data protection officer or the business leader of the affected department.
External parties involved	Contains information about the nature and role of the organisation (controller, processor, joint controller) and the external parties that may be affected and therefore need to be informed.
Risk assessment – motivation and conclusion	Detailed risk analysis and overall risk assessment, based on the elements for determining the level of risk (see section above).
Existing controls and remedial actions	A list of the existing technical and organisational measures, and the measures that will be taken to mitigate existing risks for the affected individuals.
Notifications	A summary of notifications that have been made and to whom (data protection authority, affected individual, third parties).

III.

CONTAINING A CYBER SECURITY INCIDENT

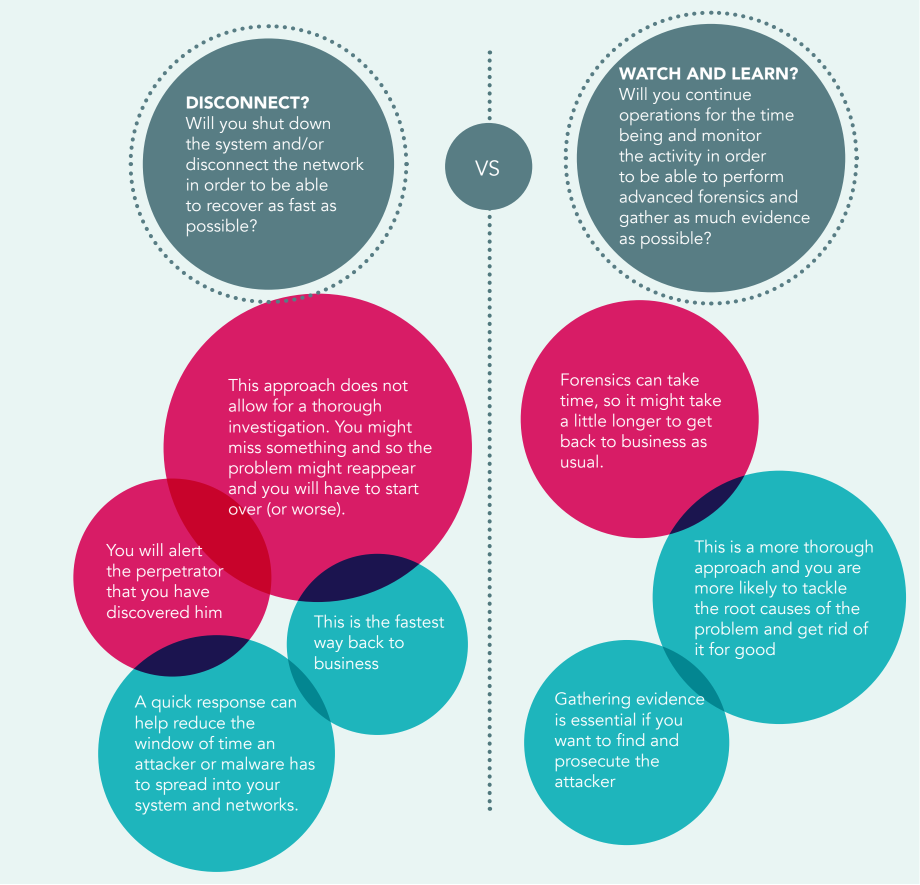
RECOVER QUICKLY OR GATHER EVIDENCE?

Containing a cyber security incident is all about limiting the damage and stopping the attacker. You have to find a way to limit the risk to your organisation while at the same time keeping it running. You need to prevent the incident from spreading further into other systems, devices and networks both within your organisation and beyond.

At the beginning of this phase, your organisation will have to make an important strategic decision: Disconnect the systems immediately in order to recover as quickly as possible? Or take the time to collect evidence against the cybercriminal who penetrated the system?

You will probably have to find a balance between these two options.
Which decision your organisation makes will depend on the scope, magnitude and impact of the incident. The following criteria can help you to evaluate:

❶ What could happen if the incident were not contained?
❷ Is the attack or breach incurring immediate serious damage?
❸ Is there (potential) damage and/or theft of assets?
❹ Is it necessary to preserve evidence? And if so, what sources of evidence should the organisation acquire? Where will the evidence be stored? How long should evidence be retained?
❺ Is it necessary to avoid alerting the hacker?
❻ Do you need to ensure service availability or is it okay to take the system offline? (for example, services provided to external parties)



DISCONNECT?
Will you shut down the system and/or disconnect the network in order to be able to recover as fast as possible?

VS

WATCH AND LEARN?
Will you continue operations for the time being and monitor the activity in order to be able to perform advanced forensics and gather as much evidence as possible?

This approach does not allow for a thorough investigation. You might miss something and so the problem might reappear and you will have to start over (or worse).

You will alert the perpetrator that you have discovered him

This is the fastest way back to business

A quick response can help reduce the window of time an attacker or malware has to spread into your system and networks.

Forensics can take time, so it might take a little longer to get back to business as usual.

This is a more thorough approach and you are more likely to tackle the root causes of the problem and get rid of it for good

Gathering evidence is essential if you want to find and prosecute the attacker

In some cases returning (directly) to business as usual will not be possible at all. When this happens, the objective of containment should be to make the best efforts to return to functionality as usual, i.e. to get the system usable by preserving access for legitimate users, while locking out the attacker.

During an incident, there will be huge pressure to act quickly. But to avoid unnecessary mistakes, it is very important to take a step back and think before you act!

INVESTIGATING: GATHERING EVIDENCE

If you want to tackle the problem at its root and identify the perpetrator for prosecution, you will need to preserve the evidence. To gather evidence, forensic **investigation** must be performed before you eradicate the incident. If you do not have the necessary in- house expertise to perform forensics yourself, call upon external experts who have the right tools to collect the evidence in a legally valid way (see also: page 13, Experts on incident response).

Bear in mind that even if your organisation has a very competent ICT team, you may still need external help in case of a complex cyber security incident. This doesn't mean that your ICT professionals have failed; on the contrary, it means that they have quickly identified the incident is so complex as to necessitate complementary expertise.

TO TACKLE A DDOS ATTACK YOU NEED EXPERIENCE

A DDoS attack is a targeted attack to bring your system down. It therefore has the potential to have a very significant impact on the availability of your system. These attacks are very sophisticated and difficult to get rid of. Most organisations will be unable to solve a DDoS attack themselves and will have to call upon external experts.

In order to be admissible in court, evidence should be collected according to procedures that conform to all applicable laws and regulations. You should avoid compromising evidence. **So, remember the following:**

DO NOT IMMEDIATELY SHUT DOWN YOUR SERVER

- If you shut the server down, you clear out the memory on the server. This means you will not be able to perform memory forensics, because you will have nothing left to analyse.
- You might be destroying crucial evidence, because RAM memory often contains a lot of traces of malware. Before shutting down your server, it needs to be dumped on a USB drive.

DO NOT IMMEDIATELY CUT OFF THE SERVER FROM THE INTERNET

- You might be destroying crucial evidence. An immediate shutdown makes it impossible to determine the extent to which your infrastructure has been compromised, because a server that has been shut down and cut off from the internet no longer communicates with its command and control server on the internet or with other infected workstations/servers in your network.
- You might be alerting the cybercriminal to the fact that you are onto him/her and, at this stage, that is not a good idea.

DO NOT RESTORE YOUR SYSTEM FROM A BACK-UP UNLESS YOU ARE SURE THE BACKUP ITSELF IS NOT INFECTED

Your backup may be infected: ATPs can infect your network for a long period without you noticing. That makes the risk of a backup infection likely. Installing an infected backup could recreate the infection.

DO NOT REINSTALL ON THE SAME SERVER WITHOUT A FORENSIC COPY

MOST COMMON TYPES OF INCIDENTS

At this point it is useful to have the list of the categories of incidents that are most likely to hit your organisation (see also: page 20, Identify possible categories of cyber security incidents). This list should contain the types of incidents that are most likely to hit your organisation and basic instructions on how to resolve such incidents. For an example, take a look at the Annex.

IV.

ERADICATION AND CLEAN-UP

Once the investigation has been concluded, you can start the eradication. In this phase you should remove all components related to the incident, all artefacts left by the attacker (malicious code, data, etc.), and close every hole or vulnerability that was used by the hacker to intrude in the first place.

Don’t start the clean-up before you have a full picture of the incident! This means that should start by determining its root cause. This is not an easy task. Furthermore, you should make sure you have at least looked at all machines with the same vulnerability, as they may also be infected. Whenever the decision is taken to start eradicating the incident, it is important to be fast, synchronised and thorough, in order to give your adversary as little chance as possible (ideally none) to respond.

The eradication can take many forms. It often includes actions such as:

- Running a virus or spyware scanner to remove the offending files and services
- Updating signatures
- Deleting malware
- Disabling breached user accounts
- Changing passwords of breached user accounts
- Identifying and mitigating all vulnerabilities that were exploited
- Identifying security gaps and fixing them
- Informing employees about the threat and giving them instructions on what to avoid in the future
- Informing external stakeholders such as the media and your customers (see also: page 26, Communication During a Cyber Security Incident)

It is also important to inform top management about the eradication and clean-up results and the network situation.

Individual files can be detected, put in quarantine or removed from systems by the anti-virus solution. This solution must be able to accept specific virus definitions that are supplied by you.

Phishing-e-mails can be held back on the mail gateway by blocking on the basis of sender, the mail relay or parts of the content.

IP and domain-based indicators can be blocked based on network traffic, by adding them to access lists, firewall policies or proxy policies. Therefore, it is important to have the necessary capability to implement these changes ad hoc.

V.

RECOVERY

When we talk about recovery, we are referring to restoring the system(s) in order to return to normal operations and (if applicable) remediating vulnerabilities to prevent similar incidents. There are multiple ways to restore following a cyber security incident. All of them have a different impact on recovery time, cost limitations or data loss:

	RECOVERY TIME	COST	DATA LOSS	REMARKS
Clean the malicious artefacts and replace the compromised files with clean versions	Fast	Cost-effective		You might leave undiscovered artefacts behind
Restore from a backup	Medium	Cost-effective		This is only possible if you have a known good backup. In some cases, it is hard to determine the timestamp of the initial incident, or the incident might have been going on for a long time, with no backup from the period before the incident.
Rebuild the system(s) or environment from zero	Slow, not time-efficient	Very costly	Chances of data loss	This is, however, the only way to be 100% sure of getting rid of the perpetrator.

Statistics show that, very often, incidents are only revealed after several months. How far back does your organisation's backup go?

The type of recovery will not only depend on the time and financial means you have at your disposal. It will also depend on the damage the incident has caused to your infrastructure. For example, you might not have an uninfected backup, because even your oldest backup was made after the attacker entered your system. Therefore, it is important to check your backup for viruses, rootkits and backdoors before you restore from it. If no known good backup can be found, then the system must be reinstalled from scratch (including the operating system!). After restoring the system, you need to remediate the vulnerabilities that allowed the perpetrator to access your system.
This will include actions such as: installing patches, both at the operating system and application level, changing passwords, changing accounts, tightening network perimeter security, e.g. changing firewall, boundary router access control lists, etc. and locking down services.

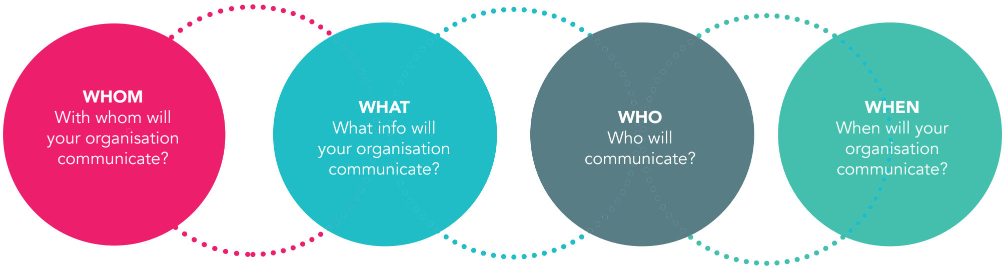
You should also take into account that once a resource has been successfully attacked, chances are that it will be attacked again, or other resources within your organisation might be attacked in a similar manner. Therefore, you should consider improving your defences, for example by applying a higher level of system logging or network monitoring.

Finally, before the system is put back online, it should be validated for both security and business functions. In terms of security, your system can be validated by scanning it with a tool that checks for remaining vulnerabilities. To validate the business functions, the person responsible needs to check that all functions necessary for the business are working properly.

Don't forget: if you don't have the necessary expertise within your organisation, call upon external experts. And don't forget to check if your cyber insurance covers this cost.

04 COMMUNICATION DURING A CYBER SECURITY INCIDENT

When an actual cyber security incident occurs, the cyber security incident response team should immediately draw up a concrete communication plan for the specific incident. Make this communication plan based on the general preparations you already made during the preparation phase (see also page 16: Prepare Your Communication Strategy). You will basically need to answer the questions below and remember that we recommend coordinating all external communications both with the Legal and Public Relations representatives. Think before you communicate!


WHOM
With whom will your organisation communicate?
WHAT
What info will your organisation communicate?
WHO
Who will communicate?
WHEN
When will your organisation communicate?

I. TOOLS

If you are well prepared, your cyber security incident response team will already have a number of tools at its disposal. During the preparation phase (see also: page 15, Prepare Your Communication Strategy), your organisation has drawn up a list of all potential stakeholders to contact (internal, external and official stakeholders) and their contact details (a specific person and his/her backup).

II. INCIDENT-SPECIFIC COMMUNICATION PLAN

WHOM TO COMMUNICATE WITH AND WHAT TO COMMUNICATE TO EACH CATEGORY OF STAKEHOLDERS

The first step in your incident-specific communication plan is to determine with whom you will communicate. In order to do so, you need to identify which potential stakeholders might be (adversely) affected by the cyber security incident you are confronted with and if you are legally bound to notify certain entities such as the National Data Protection Authority or the industry regulator.

- Internal stakeholders: top management, impacted managers, employees
- External stakeholders: media, customers, suppliers, other partners, etc.
- Official stakeholders: National Data Protection Authority, industry regulator, CCB (Cert.be dept), National Crisis Centre, police

When you determine what you will communicate and with whom, a good basic rule of thumb is to communicate on a need-to-know basis only. There will be stakeholders you want to communicate with in order to contain the cyber security incident, and there will be stakeholders you will have to communicate with, either because they pressure you for information (e.g. the media) or because you are legally bound to notify them (e.g. National Data Protection Authority, industry regulators, individuals whose data has been compromised).

PERSONAL DATA

If personal data are lost or stolen (data breach) it is advisable to notify the National Data Protection Authority. In some cases you will be legally obliged to do so. For example:

- Providers of a publicly available electronic communication service (telecom providers) are under a legal obligation to report personal data breaches to the National Data Protection Authority and to the individuals whose data were compromised.
- Under GDPR there is a legal obligation to report any personal data breach that is likely to incur a risk for the individuals whose data was compromised, to both the National Data Protection Authority (within 72 hours) and the individuals whose personal data was compromised.

REPORTING OBLIGATION: NIS DIRECTIVE

OES and DSP have a duty to report all incidents with far-reaching consequences to the CCB (CERT.be dept), the National Crisis Centre, and their sectoral authorities via a secure reporting platform. The CCB acts as a national CSIRT. Whether or not the consequences of an incident are significant must be assessed in light of the availability, confidentiality, integrity or authenticity of the information systems, i.e. the information systems of the OES/DSP.

- Availability refers to the ability of users to access the services of the OES/DSP. A DDoS attack, for example, can paralyse an OES network and jeopardise the availability of the service.
- An example of a confidentiality incident is, for example, a ‘man in the middle attack’, in which data between the users and the OES/DSP is intercepted. Such an incident can also give rise to an obligation to report to the Data Protection Authority (see p. 29).
- An integrity incident occurs when data from an OES/DSP is destroyed during a system crash.
- An incident regarding authenticity occurs, for example, when a provider of domain names can no longer guarantee the authenticity of the domain names with certainty.

It is possible that impact levels and/or threshold values per sector or subsector are determined by Royal Decree, but this has not yet been the case.

Be aware that severe administrative and criminal penalties can be imposed for violations of the reporting obligation.

[1] The European General Data Protection Regulation (GDPR).
[2] The European Directive on security of network and information systems (NIS).

WHEN TO COMMUNICATE?

Once you've established whom you will communicate with and what you will tell them, you need to decide when you will contact them. The timing should be based on the communication's objectives (see also: illustration on page 18).

Timing is important:

- Some stakeholders will need information as soon as possible because they can help contain the cyber security incident (e.g. your organisation's top management, employees);
- Other stakeholders (e.g. National Data Protection Authority) have to be contacted within a certain legally imposed timeframe; and, finally,
- Others (e.g. media) may contact you and in such a case you should have your answers ready.

Bear in mind that in order not to alert the perpetrator that you are onto him/her, it may be necessary to instigate a **no-communication phase** from the moment the incident is detected until the moment when you have a full picture of the incident and an action plan. If the perpetrator is alerted, they will probably retreat and erase all their tracks, or even worse, do some final damage such as stealing the last of your organisation's crown jewels or installing backdoors. In order to avoid a leak during this no-communication phase you can keep a list of people that are aware of the cyber security incident. This will make it easier to discover who is responsible when it appears that information has been leaked. Legal action can be taken against anyone who leaks information.

An NIS incident must be reported without delay. There is no need to wait until all relevant information is available. When it is clear that the incident must be reported, and therefore when at least one criteria is met, this must be done as soon as possible.

REPORTING TO AUTHORITIES

Reporting to authorities is a very specific part of communication. It is important for various reasons:

- As already mentioned above, in some cases there is a **legal requirement** to report data leakage or other security incidents.
- Certain authorities can **help** you. The cyber security incident you are faced with may not be an isolated incident. Authorities may have information that can help you contain your incident more quickly.
- If you want to file a complaint against the criminal behind the cyber security incident, you need to contact the law enforcement authorities. In principle this will be the **police**.
- Furthermore, reporting to the authorities is a necessary step, allowing them to inventorise and measure **cybercrime** in the country. Increased knowledge and understanding of the phenomenon and its prevalence will help to improve the overall security landscape, e.g. through the shaping of preventive measures and counter-measures.

The support of the CCB (CERT.be dept) is offered free of charge and in the strictest confidence, helping with the initial fire-fighting and providing advice on how to solve issues. Report a cyber security incident to cert@cert.be or, if you prefer, by phone: +32 (0)2 790 33 85 (every weekday from 08.00 to 18.00).

After your report, you get a receipt and an incident number. With this incident number, you can always refer to your report. CCB (CERT.be dept) will contact you as soon as possible to answer your questions.

NL EN FR

Voluntary reporting to CCB (CERT.be dept)

Organisations should always seriously consider reporting cyber security incidents to the federal Cyber Emergency Response Team, CCB (CERT.be dept). In order to prevent attacks on other computer systems, CCB (CERT.be dept) is especially interested in what they call 'Indicators Of Compromise' (IOCs). These are artefacts observed on a network or an operating system, indicating that it is very likely there has been an intrusion. Reporting to CCB (CERT.be dept) is vital in order to determine whether the incident is isolated and to make it possible to keep track of threat trends in Belgium. CCB (CERT.be dept) will be able to provide some information and advice related to the incident that can help the victim to take effective counter-measures. Furthermore, the information your organisation provides may help to prevent attacks on other computer systems.

THE FOLLOWING INFORMATION SHOULD BE REPORTED

1. Your contact details
2. The type of incident
3. The date of the incident
4. Is the incident ongoing?
5. How did you notice this incident?
6. What is the impact of the incident?
7. Have you already taken action or measures? If so, which ones?
8. Do you have logs or other useful data?
9. Whom have you already informed?
10. What are you expecting from your report?

Mandatory reporting of NIS incidents

Reports must be made via the NIS reporting platform (https://nis-incident.be/). The platform is accessible via the internet through a secure connection and a unique identification key for each AED and DDV (login/username and password). If the platform is not available, the incident must be reported via the website of the CCB (https://cert.be/nl/een-incident-melden). The platform ensures that the report reaches the CCB, the National Crisis Centre and sectoral government.

The respective sectoral government for each sector is listed below.

Sector	Sectoral government
Energy	Federal Minister responsible for Energy (FPS Economy DG Energy)
Transport	Federal Minister responsible for Transport or Maritime Mobility (FPS Mobility and Transport)
Healthcare	Federal Minister responsible for Public Health (FPS Public Health)
Drinking water	National Committee for the Security of Supply and Distribution of drinking water
Digital Infrastructures	Federal Minister responsible for Economy (BIPT)
Finances	NBB (financial institutions); FSMA (financial trading platforms)

The report includes all available information that enables the relevant persons to determine the nature, causes, effects and consequences of the incident:

- the name and contact details of the provider and the service provided;
- the date and time when the incident occurred;
- the duration of the incident;
- the extent of the geographical area affected by the incident and its cross-border nature, if any;
- the number of affected users;
- information about the nature of the incident;
- the extent of the consequences of the incident, in particular for social and economic activities;
- the importance of the systems or of the information involved;
- the consequences of the incident for international organisations based in Belgium;
- actions taken;
- description of the present situation.

The initial notification, which should be done as soon as possible, is one phase in the notification procedure. In total, the procedure can include three stages:

- The initial report must be made without delay, even if the OES or DSP does not yet have all the relevant information. The purpose of this initial report is highlight the incident and its possible consequences to the CCB, the sectoral government or its sectoral CSIRT, and the NCCN.

- Additional notifications should be sent regularly or as soon as the OES or DSP has new information. The purpose of these additional reports is to keep the CCB, the sectoral government or its sectoral CSIRT, and the NCCN informed of the status of the incident. The OES or DSP then makes a new report on the platform, stating only the new data and the reference number of the initial report.

- A possible final report (at the request of one of the aforementioned authorities) containing all information sent to the CCB, the government sector or its sectoral CSIRT, and the NCCN. The purpose of this final report is to provide an overview of the incident and to draw conclusions from it.

The OES or DSP must keep the CCB and the government sector, or where appropriate the sectoral CSIRT, informed about the evolution of the incident and the remedial actions taken.

Filing a complaint with law enforcement

Law enforcement authorities must be notified as soon as possible after discovery of the cyber security incident, given the volatility of traces and actions that need to be taken (Internet identification, etc.). For prosecution to be successful, the chain of custody needs to be preserved in a legally accepted manner, which requires the evidence to be preserved immediately after the incident has been detected.

Judicial authorities need to possess the available information regarding the incident in order to make a qualification of the offence and to proceed with the identification of the suspect. The information that should be communicated to the police in case of Internet fraud (a ‘traditional’ crime committed by electronic means) may not be entirely the same as the information the police needs in the case of ICT crime (hacking, sabotage, espionage). In the course of the investigation, additional information will be requested, collected and searched for by the investigators. It is of the utmost importance that your services provide the assistance and input requested by law enforcement, to help advance the investigation.

I. Police

If your organisation is impacted by an incident and as such has been the victim of an offence, you can decide to lodge a complaint. By default you should go to your local police station or a police station of your choice. For more complex cases, the local police will get support from the Regional Computer Crime Units (RCCU), specialised in dealing with ICT crime (hacking, sabotage, espionage) and/or the Federal Computer Crime Unit (FCCU). If the case concerns a critical infrastructure or a sector with specific rules, a special procedure may apply.

By default you should go to your local police station or a police station of your choice. Information about police zones is available here:

NL FR

II. Investigating judge

It is also possible to file a complaint directly with a magistrate (investigating judge). This should be an exceptional measure. Furthermore, your organisation will probably have to advance the costs of the investigation because the magistrate is conducting it at your specific request.

REPORTING A PERSONAL DATA BREACH TO THE NATIONAL DATA PROTECTION AUTHORITY

Certain breaches of personal data must be reported to the National Data Protection Authority. As a reminder, by personal data we mean all data relating to a natural person who is or can be identified directly or indirectly. A number, such as an IP address, will therefore also be regarded as personal data in a great many cases.

The notification obligation concerns breaches that pose a risk to the rights and freedoms of the data subjects. An example of this is the loss of confidentiality of a communication, as a result of which invoice data, addresses, etc. are temporarily visible to third parties. In principle, the notification period is 72 hours after the data breach has been identified.

A notification can be sent to the National Data Protection Authority via a secure e-form application. All this information is explained in detail in the manual for the notification form.

NL FR

When your organisation notifies the National Data Protection Authority, the latter will be able to estimate the impact of the data breach in cooperation with the person in charge of processing the data breached and can make recommendations regarding the rules on data processing and the need to secure this. In addition, the person(s) responsible for data processing will have to reconsider the manner in which the data processing is organised and secured, now and in the future. Organisations from specific sectors, such as providers of financial services or electronic communications networks, should bear in mind that they are already subject to an obligation to report to the National Data Protection Authority any incident involving a breach of personal data.

NOTIFYING INDIVIDUALS WHOSE PERSONAL DATA HAVE BEEN COMPROMISED

In certain cases, the individuals whose data are involved in the data breach need to be informed. The person responsible for the data processing has to notify the individuals involved of the data breach via a communication means that guarantees that the information is received as soon as possible. If it is not possible to identify the victims of the breach, the data processor can inform them via public media, while at the same time pursuing the identity of the individuals in order to inform them on a personal basis.

The notification to the individuals involved needs to be clear and easy to understand. The National Data Protection Authority recommends providing as a minimum the following information:

- Name of person responsible for data processing;
- Contact information for further information;
- Short description of the incident during which the data breach occurred;
- (Probable) date of the incident;
- Type and nature of personal data involved;
- Possible consequences of the breach for the individuals involved;
- Circumstances in which the data breach occurred;
- Measures taken by the data processor to prevent the data breach;
- Measures that the person responsible recommends the individuals involved take to limit possible damages.

DATA BREACH

Rex Mundi has obtained your company's data. It contains sensitive information about your clients, so their privacy is at stake. He threatens to publish everything on the internet on his Twitter account.

05 INCIDENT FOLLOW-UP AND CLOSURE: LEARN FROM EACH INCIDENT!

I.

All cyber security incidents, like any other incident, need to be properly closed. Furthermore, it is very important that lessons are learned from each incident in order to evaluate future improvements.

EVALUATION OF LESSONS LEARNED AND FUTURE ACTIONS: ORGANISE A POST-INCIDENT REVIEW

A post-incident review is a very useful document because it shows actual data and real impacts. It can help your organisation to evaluate your cyber incident response plan and budget.

OBJECTIVE

All cyber security incidents should be formally reviewed after the incident resolution to verify if security mechanisms or mitigating controls need to be put in place or adapted to prevent similar incidents in the future.

WHY?

Cyber security incidents can show up serious shortcomings in your security strategy or practice. Every major incident needs to be analysed to evaluate whether lessons for future improvement can be learned.

WHAT SHOULD THIS POST INCIDENT REVIEW LOOK LIKE?

A post-incident review and possible lessons learned must be part of the handling of all cyber security incidents.

Checklist of questions that can help in the evaluation:

- Were the cyber security incident management plan and procedures followed? Were they adequate? Should the plan be adapted on certain points?
- Was information available in time? If not, would it have been possible to have it sooner and how?
- Were there any steps or actions you have taken that might have inhibited the recovery?
- Could your information-sharing with other organisations be improved?
- What corrective actions could prevent similar incidents in the future?
- Are there precursors or indicators that should be monitored to detect similar incidents more easily in the future?
- What additional tools or resources are needed to detect, analyse, mitigate future cyber security incidents?
- Did the cyber security response team have the right organisational authority to respond to the incident? Should you recruit more people or place a consulting firm, lawyer,…on retainer in case of a future cyber security incident?

INCIDENT TRACKING AND REPORTING

It is important to document every incident and the actions you have taken, and to keep all of this documentation together. Similar incidents might happen again and might require the same handling procedures, or a small incident might turn out to be part of a bigger incident that you discover later. Furthermore, it is also necessary to report the incident to relevant stakeholders, both internal and external. Use the results of your post-incident review to determine which stakeholders should be contacted. Internally, the organisation's top management should always be considered a relevant stakeholder and thus receive a documented report on what happened, what actions were taken, where it went well/wrong, etc.

OBJECTIVE

TRACKING
All cyber security incidents and their resolution must be documented.

REPORTING
All cyber security incidents and their resolution must be reported to top management and, if this function exists within your organisation, to the Information Security Officer.

WHY?

TRACKING
Des incidents similaires pourraient se produire et nécessiter d'utiliser les mêmes procédures, ou un incident de moindre importance pourrait faire partie d'un incident de grande ampleur découvert ultérieurement.

REPORTING
La haute direction et/ou les personnes de votre organisation chargées d'analyser les risques dans votre organisation (par exemple, un comité du risque opérationnel ou équivalent) doivent être informées de tout incident de cybersécurité.

WHAT SHOULD THIS TRACKING AND REPORTING DOCUMENT LOOK LIKE?

A documented report must be written for all cyber security incidents and kept together with other cyber security incident reports. You can base this report on the conclusions of the post-incident review.

All major security incidents should be reported immediately to top management. At least once a year all cyber security incidents must be reported and explained to top management and the people within your organisation that analyse your organisation's risks.

GLOSSARY

APT APT is short for Advanced Persistent Threat. It is a set of stealthy and continuous computer hacking processes. In case of an APT, the perpetrator uses multiple phases to break into a network, in order to avoid detection, and harvest valuable information over the long term.

Artefact Artefact is an object of digital archaeological interest.

Asset Any Resource or Capability. Assets of a Service Provider include anything that could contribute to the delivery of a Service. Assets can be one of the following types: Management, Organisation, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.

Backdoor In software or a computer system this is a method of bypassing security mechanisms. It can be used by system administrators or programmers in a legitimate way. But in this Guide we refer to the illegitimate version, namely a secret portal that hackers and intelligence agencies use to gain illicit access to computer systems, while staying undetected.

Back-up Backup procedures are used to copy files to a second medium such as a disk, tape or the cloud. Backup files should be kept at an offsite location. Backups are usually automated using operating system commands or backup utility programs. Most backup programs compress the data so that the backups require fewer media.

Botnet A collection of computers (often tens of thousands) that are operated by one or more persons (called botmasters) using malware. Botnets can be used to send out spam, to start a DDoS attack, to spread malware, etc.

Command and control server A centralised server that can send commands and receive information from the computers that are part of a botnet. The command and control server allows a botmaster to control the group of computers in the botnet remotely.

DDoS DDoS is short for Distributed Denial of Service. In case of a DDoS, a botmaster commands the computers of the botnet to access a determined website. The server of this website will end up overloaded and will stop functioning correctly.

DMZ DMZ is short for demilitarised zone, and refers to the physical or logical subnetwork (zone) that separates an internal local area network from other untrusted networks, such as the Internet. The purpose of a DMZ is to add an additional layer of security. The name is derived from the military term ‘demilitarised zone’, which is an area between nation states where military operation is not permitted.

Host A computer that stores a website or other data that can be accessed over the Internet or that provides other services to a network.

IDS IDS is short for Intrusion Detection System, which is an automated system that aims to detect hacking or unauthorised access to a computer system or network.

IPS IPS is short for Internet Protocol address. It is a numerical label assigned to each device participating in a computer network. IP addresses are used both to identify and locate the device.

Network A telecommunications network that allows computers or other devices to exchange data. The best-known computer network is the Internet.

Patch Patch is a small piece of software, often developed by the producers of specific software in order to update, fix (bugs or vulnerabilities) or improve this software. It allows you to change the software without reinstalling it from scratch.

PGP PGP is short for Pretty Good Privacy, which is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP can be used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and for increasing the security of e-mail communications.

RAM RAM is short for Random Access Memory. RAM is the most common type of data storage found in computers and other devices, such as printers. In a RAM device all data items can be accessed in (almost) the same amount of time, irrespective of the physical location of data inside the memory.

Rootkit A collection of computer software, often malicious, designed with a double objective: (1) to enable access to a computer or areas of its software that would not otherwise be allowed, while at the same time (2) masking its existence or the existence of other software. Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Removal can be complicated or practically impossible.

SNORT Snort is a free and open source network intrusion prevention system and network intrusion detection system. www.snort.org

Spoofing A spoofing attack is a situation in which a person or program successfully poses as another by falsifying data and thereby gaining an illegitimate advantage. For example, e-mail spoofing is the creation of e-mail messages with a forged sender address.

VPN VPN is short for Virtual Private Network. This is a group of computers networked together over a public network such as the Internet. Businesses use VPNs to connect remote data centres or to allow employees to securely access the corporate intranet while travelling outside the office.

Vulnerability A weakness in a system, application, or network that is subject to exploitation or misuse.

Workstation A computer (hardware).

BIBLIOGRAPHY

CERT-EU (2012), *Guidelines of the CERT-EU for data acquisition for investigation purposes*
Retrieved from http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_04_Guideline_ DataAcquisition_v1_4_4.pdf

CREST (2013), *Cyber Security Incident Response Guide*
Retrieved from http://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide. pdf

ENISA (2010), *Good Practice Guide for Incident Management*
Retrieved from https://www.enisa.europa.eu/activities/cert/support/incident-management

FEB, ICC, *B-C Centre, Isaca, EY, Microsoft (2013), Belgian Cyber Security Guide*
Retrieved from https://www.feb.be/en/publications/guide-belge-de-la-cyber-securite_2014-05-26/

ISO/IEC 20000-1 (2011), *Information technology - Service management - Part 1: Service management system requirements*
Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=51986

ISO/IEC 27001 (2013), I*nformation technology - Security techniques - Information security management systems - Requirements*
Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnum- ber=54534

Marsh (2015), *European 2015 Cyber Risk Survey Report*
Retrieved from http://belgium.marsh.com/Portals/95/Documents/15%2010-023%20Europe- an%20 Cyber%20survey%20report.pdf

Microsoft TechNet, *Responding to IT Security Incidents*
Retrieved from https://technet.microsoft.com/en-us/library/cc700825.aspx

NIST (2012), *Framework for Improving Critical Infrastructure Cyber Security – Version 1*.0
Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214. pdf

NIST (2012), *Computer Security Incident Handling Guide – Recommendations of the National Institute of Standards and Technology*
Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

SANS Institute, *SCORE Security Checklist on APT Incident Handling*
Retrieved from https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist. pdf

SANS Institute (2003), *Sample Incident Handling Forms*
Retrieved from https://www.sans.org/score/incident-forms/

SANS Institute (2007), *An Incident Handling Process for Small and Medium Businesses*
Retrieved from https://www.sans.org/reading-room/whitepapers/incident/incident-han- dling-process-small-medium-businesses-1791

SANS Institute (2008), *Incident Handling for SMEs (Small to Medium Enterprises)*
Retrieved from https://www.sans.org/reading-room/whitepapers/incident/incident-handling-smes-small-medium-enterprises-32764

SANS Institute (2008), *Security Incident Handling in Small Organizations*
Retrieved from https://www.sans.org/reading-room/whitepapers/incident/security-inci- dent-handling-small-organizations-32979

ACKNOWLEDGEMENTS

DRAFTING GROUP

Cathy Suykens (Cyber Security Coalition)
Anneleen Dammekens (FEB)
Daniel Letecheur (FEDICT)
Georges Ataya (Solvay Brussels School)
Luc Beirens (Deloitte)
Ferdinand Casier (Agoria)
Phédra Clouner (CCB)
Walter Coenraets (FCCU)
Miguel De Bruycker (CCB)
Dirk De Nijs (ModuleBuilder)
Pedro Deryckere (FCCU)
Nathalie Dewancker (Proximus)
Steven Goossens (Proximus)
Ann Mennens (European Commission)
Philippe Mermuys (Allianz)
Benoit Montens (Assuralia)
Ronny Tronquo (KBC)
Erik Van Buggenhout (Nviso)
Geoffrey Schreiber (KPMG Advisor)
Kara Segers (KPMG Advisor)
Mathieu Tulpinck (Legal consultant)

RESPONSIBLE PUBLISHER

Jan De Blauwe
Stuiversstraat 8
1000 Brussels
Info@cybersecuritycoalition.be
www.cybersecuritycoalition.be

DATE OF FIRST PUBLICATION

January 2016

DATE OF SECOND PUBLICATION

September 2021

ANNEX

Most common incident types and how to neutralise them

INCIDENT TYPE	DEFINITION	POSSIBLE TARGET	VULNERABILITIES THAT MIGHT BE EXPLOITED	POSSIBLE REACTIONS
Social engineering: (spear) phishing, vishing (phone phishing)	Manipulating and tricking someone into revealing information (e.g. password or financial information) that can be used to attack systems or networks	CEO Accounting		
(spear) phishing, vishing (phone phishing)	Attempt to acquire sensitive information (e.g. customer logins & passwords) from customers by impersonating a legitimate and trusted person or organisation.			
Unauthorised access	When a person gains logical or physical access without permission to a network, system, application, data, or other IT resource.	Customer information Credit card information Applications creating or processing payments Websites and services	Password cracked or sniffed Unpatched system vulnerabilities Social engineering Careless users or weak procedures	Patch vulnerabilities or block exploitation Check for malware (rootkits, backdoors, Trojans, …) Change passwords or inactivate accounts Forensic evidence gathering Block (network) access to the targeted resources
Denial of service	Any attack that prevents or impairs the authorised use of networks, systems or applications by exhausting resources.	Mail system Network appliances Application servers Websites and services	Spam filter weaknesses Unpatched system vulnerabilities Weak configuration of systems or appliances	Block traffic Contact ISP Disconnect infected system(s)
Malicious code attack **Ransomware:** is a type of malware that restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive while some may simply lock the system and display messages intended to coax the user into paying.	A malicious code attack is any (large- scale) infection or threat of infection by a virus, worm, Trojan horse, or other code-based malicious entity.	Any server or even appliance in the network could be the target of a malicious code attack, but some systems have a higher risk profile (e.g. systems directly or indirectly connected to the outside world) Any end user workstations could be targeted via e-mail, USB storage devices, visits to websites and web applications, etc.	Unpatched system vulnerabilities (e.g. Flash or JavaScript) Anti-virus not installed, not active or signature file not up to date Inappropriate or imprudent user behaviour (e.g. using infected USB memory device)	Block malicious web traffic Apply patches Update anti-virus signature files Run virus clean-up tool if available Run vulnerability assessment tool to list vulnerable resources Completely reinstall infected system Shut down vulnerable services Shut down or disconnect infected system(s)

INCIDENT TYPE	DEFINITION	POSSIBLE TARGET	VULNERABILITIES THAT MIGHT BE EXPLOITED	POSSIBLE REACTIONS
Inappropriate usage	An inappropriate usage incident is any incident involving an internal employee or contractor violating a code of conduct or a computer policy. Inappropriate behaviour is not always malicious and targeted. Sometimes a user will simply act carelessly or even be completely unaware of the policy or code of conduct he/she has infringed. The inappropriate behaviour will sometimes constitute a serious security incident in itself, but it can also be the cause of or trigger for a serious incident (like malware infection, loss of critical data)	Payment transactions Credit card information Customer commercial and personal information Confidential information in general	Weak management or control of confidential data Bad user password management Lack of segregation of duties, accumulation of access rights Lack of application security or monitoring Lack of procedures or control to enforce policies and codes of conduct	Inform and get advice from Compliance and/or the legal department Inactivate users or withdraw access rights Make forensic copies of logs and other crucial information to trace and prove what happened Check logs and other information for traces of the infringement
Fraud	Fraud is a kind of inappropriate behaviour that is inherently malicious in nature, and aimed at personal enrichment by abusing company systems, applications or information.			
Data loss or theft	This is an incident that involves the loss or theft of confidential information. Information can be confidential because of the value it has for the company, or because it is protected by internal or external regulations. Data loss incidents can have a big financial impact, due to possible financial liability or damage done to the company image, should the information itself or the fact that is has been lost become public or known to the wrong people.	Personal information about employees or customers (protected by privacy laws or concerns) Credit card information Customer commercial information Confidential balance sheet information Confidential information about company strategy, on-going projects and decisions, etc.	Improper handling of portable storage devices (USB memory stick, CD, back-up tape, etc.) Improper handling of mobile equipment (laptop, PC, smartphone, etc.) Improper handling of confidential printed information Breach of clean desk policy	Assess the level of protection of the data, if any (encryption, password protection, specific device required to read the data) Inform and get advice from Compliance and/or the legal department or from your external legal adviser Inform Communications department and management, define a communication strategy Inform the owner of the lost or stolen data
Brand abuse	This is an incident where someone is abusing your brand and registered trademarks.	Registration of DNS names containing the brand Spoofing of website designs Spoofing of e-mail addresses and e-mail templates	Not applicable	Inform police (in case of theft) Request a takedown of the website Inform customers about its existence

VBO
Verbond van
Belgische
Ondernemingen

b·ccentre
BELGIAN CYBERCRIME CENTRE OF EXCELLENCE
FOR TRAINING, RESEARCH & EDUCATION

ICT CONTROL
Your Trusted Advisor

BNP PARIBAS
FORTIS

Solvay Brussels School
Economics & Management

KBC

proximus

Deloitte.

KPMG