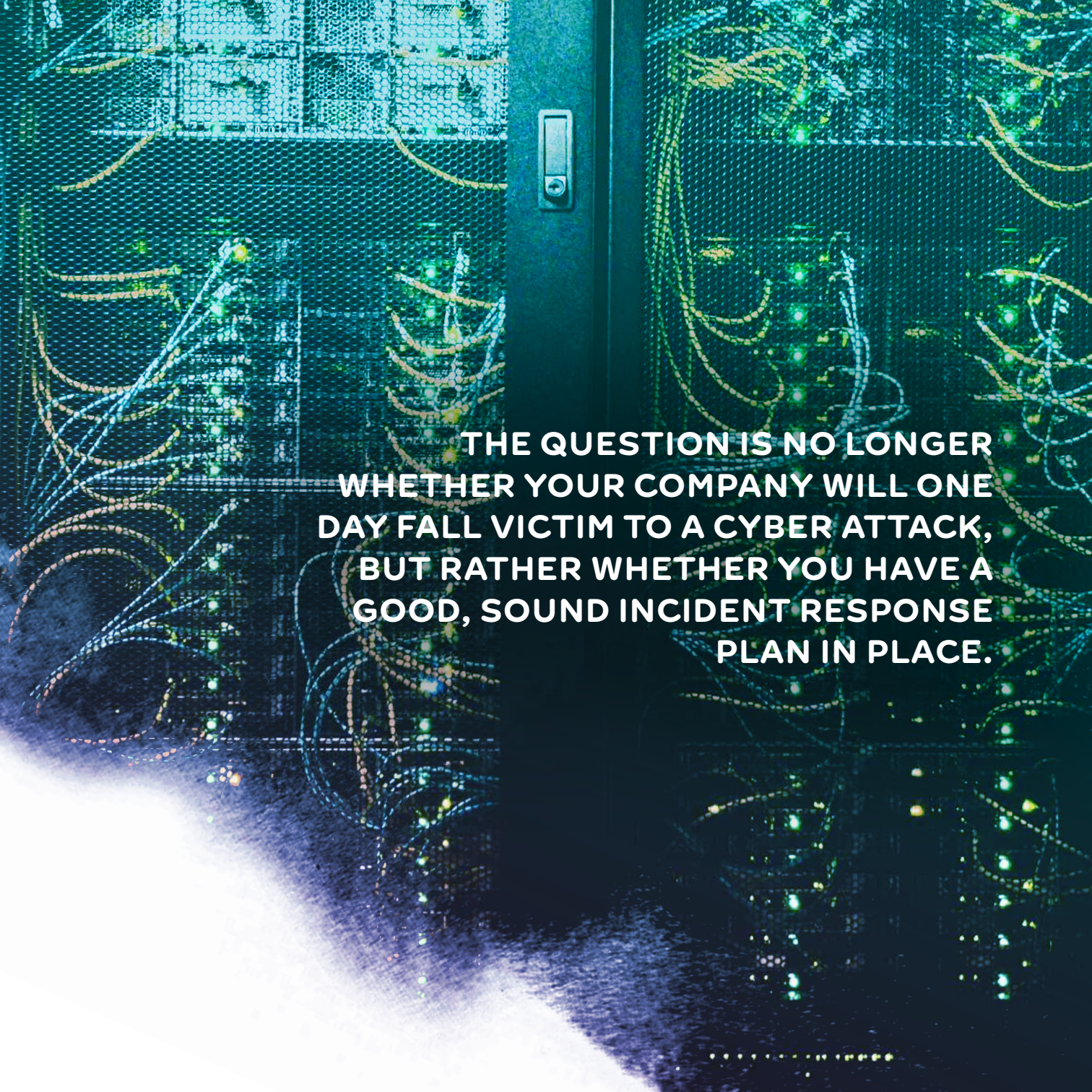




CYBER INCIDENT ROADMAP

A server room with a blue and purple glow. A central door is visible, and the room is filled with server racks and numerous cables, some of which are illuminated with glowing lights. The overall atmosphere is futuristic and high-tech.

**THE QUESTION IS NO LONGER
WHETHER YOUR COMPANY WILL ONE
DAY FALL VICTIM TO A CYBER ATTACK,
BUT RATHER WHETHER YOU HAVE A
GOOD, SOUND INCIDENT RESPONSE
PLAN IN PLACE.**

Cyber attacks are on the rise. Testimonies from many companies that have experienced such attacks highlight the difficulties they encountered, not only during but also after the incidents. Affected companies are totally helpless, forced to deal with an unprecedented situation that typically deprives them of some or all of their digital tools, and even some or all of the critical data they absolutely need in order to continue operating and meet their obligations.

This roadmap aims to provide such companies with guidance regarding their internal organisation and more specifically to help them navigate their interactions with their external contacts, in particular the public authorities, in connection with their legal obligations. How does a company report a cyber incident to the NSSO or the General Administration for Taxation? What steps do they need to take to notify the NEO of planned periods of temporary unemployment owing to a lack of work for economic reasons or owing to technical issues?

Naturally, it is advisable to avoid cyber attacks in the first place and take all relevant preventive measures. This is, of course, the ideal scenario.

Multiple documents are available to help businesses improve their cyber resilience and prevent and cope with cyber incidents. In 2014, FEB partnered with ICC Belgium, EY (Ernst & Young), B-CENTRE, ISACA and Microsoft to launch the Belgian Cyber Security Guide¹ as a means of convincing all companies of the importance of protecting themselves against cyber threats, based on their specific needs. The Cyber Security Coalition², of which FEB is a founding member, has also published an excellent incident management guide³.

The question is no longer whether your company will one day fall victim to a cyber attack, but rather whether you have a good, sound incident response plan in place.

This roadmap aims to provide an overview of the various stages of the incident management process, from identification to resolution, and more specifically to direct you, at every stage, to the organisations, stakeholders and external experts able to help you through this ordeal, protect your business and continue to fulfil your obligations towards public authorities in particular. Rather than being the final version, this roadmap is a work in progress and will therefore be updated regularly after its initial publication in **December 2022**.

Nathalie Raghenò
Senior Adviser,
FEB Competence Centre
Law & Business

Pieter Timmermans
FEB CEO

(1) https://www.feb.be/publications/guide-belge-de-la-cyber-securite_2014-05-26/
(available in Dutch and French)

(2) The Cyber Security Coalition is a unique partnership between academia, the public authorities and the private sector, who have joined forces in the fight against cyber crime. Over 100 key players from these three sectors are currently active members contributing to the Coalition's missions and objectives.

(3) <https://www.cybersecuritycoalition.be/resource/incident-management-guide/>

TABLE OF CONTENTS

01

PREVENTIVE MEASURES

p. 4

02

**CYBER RESILIENCE:
AN IDEAL MINDSET** p. 6

03

**THE INCIDENT
MANAGEMENT
PROCESS** p. 8

- 3.1 Who should you notify? p. 9
- 3.2 Who should you notify within the company? p. 10
- 3.3 Who should you notify outside the company? p. 11
 - 3.3.1 External experts p. 11
 - 3.3.2 Data subjects: customers, suppliers, etc. p. 11
 - 3.3.3 Insurers p. 11
- 3.4 Filing a complaint with the police p. 13

04

LEGAL OBLIGATIONS RELATING TO AN INCIDENT p. 14

- 4.1 General obligations p. 16
- 4.2 Obligations to institutional stakeholders p. 16
 - 4.2.1 DPA p. 16
 - 4.2.2 CERT.be p. 18
 - 4.2.3 FPS Finance p. 21
 - 4.2.4 NSSO p. 22
 - 4.2.5 NIHDI p. 24
 - 4.2.6 NEO p. 26

05

SYSTEM RESTORATION p. 28

- 5.1 Incident mitigation and business continuity p. 29

USEFUL POINTS OF CONTACT p. 30



01

PREVENTIVE MEASURES



DEVISE YOUR INCIDENT MANAGEMENT PLAN IN ADVANCE TO BOOST YOUR RESILIENCE

We are surely all aware of the importance of adequate preventive measures and thorough preparation when it comes to cyber incidents. All staff members must be informed and made aware of this risk, which can have very serious repercussions financially as well as in terms of a company's reputation and organisation.

As such, it is vital that procedures are in place to prepare for a cyber incident.

Companies must be able to take action to restore any critical activities, systems or data affected by an incident - in short, to restore normal operations. Planning and preparations must be completed before an incident and play a key role in effective cyber resilience.



02

CYBER RESILIENCE: AN IDEAL MINDSET

Agoria, the Belgian federation for the technology industry, has extensive expertise in cyber security and threat resilience. When asked, Agoria summed up its vision of cyber resilience using the slogan *ABC for Executive*.

A *Is for Asset Management*

Many of today's business directors and managers share the same major weakness, namely that they do not always have a clear view of which assets and/or IT equipment need to be protected, or whether to focus on protecting their servers, data, applications, or something else. Budgetary restrictions mean that it is unlikely that you would be able to protect everything equally, but you should at least be able to identify your most crucial assets. This type of thinking is often lacking within companies.

B *Is for Business Modelling*

In addition, directors and managers sometimes lack a clear schematic vision of their business. Though often underestimated, business modelling is essential. How is your business structured? When you offer a value proposition to a customer, on which service is it based? Via which application? Hosted on which server? On which network? Having this kind of schematic overview will be an invaluable source of help during a cyber attack.

C *Is for Continuity*

Are you prepared? What is your business continuity plan in the event of an attack? How do you test this plan? Do you have an offline backup of your priority assets? Do you have a plan for communicating with the outside world in a crisis? This is also something many companies fail to consider.

Cyber poverty line

Our main piece of advice is: do not wait for a cyber attack to implement an action plan. There is a minimum level of IT hygiene that every company should maintain, known as the cyber poverty line.

Cyber resilience is an ideal mindset and a working method. All companies should regularly go into attack mode, just as they must have and regularly test a fire evacuation plan. This is especially important because a company that fails to prepare for a potential cyber attack could be considered a company that neglects risk management, which is obviously disastrous for its business and as well as for the image of the company and its directors.

**We also advise consulting Agoria's
*Our recommendations for your cyber security.***

[Click here](#) 

03

THE INCIDENT MANAGEMENT PROCESS

Devising a response plan is a vital first step in preparing for and managing a cyber security incident for any company or organisation. This plan must be approved by the highest management level, which must be involved in all stages of the incident management cycle. Such plans must also be kept up to date.

Response plans include the following:

- An inventory of the assets to be protected (data, systems, networks, products);
- A list of responsibilities and the allocation thereof;
- A list of in-house capabilities or contracts with external expert consultants to develop incident response and/or forensic investigation (digital research and investigation) skills;
- A basic containment strategy: should systems be taken offline immediately to allow for the fastest possible recovery, or should you take the time to gather evidence?
- A communication strategy for internal and external stakeholders and authorities, such as the Data Protection Authority (DPA) and the relevant authorities for reporting incidents affecting network and data security.

3.1 WHO SHOULD YOU NOTIFY?

Having a procedure and lists of the internal and external stakeholders to be notified according to defined scenarios and criteria (such as incident severity) and being aware of the required regulatory and legal notifications are good practices for any company and a key part of its cyber resilience policy.

Which stakeholders might be affected by a cyber security incident? Are you responsible for informing certain entities, such as the DPA?

- Internal stakeholders: top management, executives affected by the incident, employees;
- External stakeholders: media, customers, suppliers, other partners, etc;
- Institutional stakeholders: the DPA, sectoral authority, Centre for Cyber Security Belgium (CCB, more specifically the CERT.be service), the National Crisis Center, the police, etc.

3.2 WHO SHOULD YOU NOTIFY WITHIN THE COMPANY?

When a company is hit by a cyber incident, the right people within the company must be notified quickly.

Like any other risk impacting a company, the board of directors must set out a clear cyber security strategy. Though the board does not have to understand all the technical aspects, it is still responsible for the governance of cyber security risks¹. This includes risk prevention, awareness-raising among staff, cyber risk insurance, and so on. It is worth remembering that under both the General Data Protection Regulation (GDPR) and ICT security standards (such as ISO 27001), among others, boards of directors have overall responsibility for IT security.

Within a company, the board of directors is responsible for guiding the risk management strategy and setting clear and achievable goals to strengthen the organisation's cyber resilience. Cyber security is also a core component of a sound environmental, social and governance (ESG) policy.

Senior management makes the necessary decisions to roll out procedures to prevent cyber incidents and to manage crisis situations. It fosters an organisation within which staff, in particular, are encouraged to report or escalate cyber incidents to management.

In practice, every company and organisation should incorporate an incident response team that can be called upon as soon as an incident occurs. Of course, the size and structure of such a team depends on the size of the company. It may also be more cost-effective and efficient in some cases to use external partners to respond to cyber security incidents and to fill the skills gap within your organisation.

However, smaller companies without the resources to establish such a team can appoint a first responder - normally someone with decision-making authority - from among their staff. In the event of a cyber security incident, this person may seek external assistance but remains responsible for the response to the incident within the organisation.

The composition of the incident response team will be determined by the skills needed to manage incidents. For small companies, the first responder may seek these skills externally and contact the relevant experts.

When a cyber incident occurs, the board of directors must therefore be notified immediately. The heads of all departments that could be involved in handling the crisis should then be convened: first and foremost IT, as well as HR, legal, communications and finance, depending on the incident and the procedure devised by the company.

(1) This responsibility will be expanded further in connection with the NIS 2 Directive.

3.3 WHO SHOULD YOU NOTIFY OUTSIDE THE COMPANY?

3.3.1 External experts

External experts will help you determine the causes of the incident and advise on how to contain and eliminate the incident and prevent it from reoccurring. Other stakeholders, such as sectoral regulatory bodies (e.g. the FSMA, the BIPT or CREG), the DPA, the CCB (CERT.be service) and law enforcement (police and magistrates), can provide valuable assistance when you are dealing with a cyber security incident of a criminal nature or in case of a personal data breach. Under some laws, you are even required to notify these organisations as soon as you identify an incident of a particular nature (see below).

3.3.2 Data subjects: customers, suppliers, etc.

The type of incident and its (potential) impact will dictate the type of communication required.

If certain obligations to customers and/or suppliers cannot be met, these must be identified and the data subjects informed. In such a situation, it is vital that you communicate about the situation to reassure trusted partners.

If the IT system is unavailable, customers can be informed of the rules for using the temporary services and tools that have been put in place.

When the personal data of a company's customers or suppliers are hacked, it is advisable to contact the affected customers and/or suppliers as a minimum and to prepare a press release if necessary. In the event of a cyber incident, if the breach of personal data is likely to pose a high risk to the natural persons whose data have been lost or stolen, the data controller appointed as per data protection regulations (GDPR and privacy legislation) is required to inform the data subjects as quickly as possible, either by contacting them directly or, if this is too complex, through the public media (see below).

3.3.3 Insurers

Assuralia, the Belgian federation for the insurance sector, is very active in the development and promotion of cyber risk insurance. Companies would benefit from taking out such insurance, as it is not uncommon for cyber security incidents to cost hundreds of thousands or even millions of euro. Cyber risk insurance will cover at least part of this cost.

3.3.3.1 Services offered by the insurance sector

There are three main types of service offered by the insurance companies active in this market:

- **Assistance for companies affected by cyber incidents:** telephone helpdesk, IT support (e.g. securing affected systems, investigating causes, restoration, recovering data), public relations or crisis management services, etc;
- **Compensation for damages specific to the insured company:** coverage of costs to maintain or restore normal operation, costs of data recovery - data and software repair, compensation for operating losses, even total or partial coverage of ransom and cyber extortion costs, etc;
- **Compensation for damage to third parties (civil liability):** compensation for any damage caused to customers and suppliers, contractual civil liability insurance (professional civil liability) covering contractual compensation, extra-contractual civil liability to compensate for damage related to the leakage of personal data, a breach of network security, the transmission of malicious programs, etc. Il convient par ailleurs de rappeler que la souscription d'un contrat d'assurance doit être préalable à la survenance du sinistre.

It is also worth remembering that an insurance policy must be taken out before a claim is made.

Please note: such coverage is not offered by all insurers. Moreover, the availability of this level of coverage depends on the profile of the client and their sector of activity. Each policy is tailored to the client.

3.3.3.2 Conditions of access to insurance (points to note)

Taking out cyber risk insurance is subject to conditions for the company applying for insurance: analysis and management of risks, preventive measures aimed at reducing risks (e.g. publication of policies, crisis management plan, audits, intrusion tests), measures to raise awareness and train personnel, etc.

Good security practices are essential here: antivirus protection, firewalls, automatic and regular updates, regular backups stored off-site, multi-factor authentication, regular staff awareness-raising and training courses, etc.

Insurers can also impose other conditions, such as (sub) limits for ransomware and co-insurance with the insured party.

3.3.3.3 What should an insured company do in the event of a cyber attack?

If the company is insured against cyber risks, it should first call the number of the preferred partner specified in the assistance section of the insurance policy, who will coordinate all operations with the company's crisis and IT teams.

If the company is not specifically insured against cyber risks, it may nonetheless be able to rely on more general insurance cover, such as legal protection insurance or operations civil liability insurance (for damage to third parties). The affected company should then submit its claim as soon as possible to its insurance intermediary (broker) or the relevant insurer(s).

3.4 FILING A COMPLAINT WITH THE POLICE

La première démarche essentielle est de déposer une plainte auprès de la police contre l'auteur présumé de l'incident de cybersécurité. Ce dépôt de plainte doit être effectué auprès de la zone de police locale du siège de votre entreprise.

The first key step is to file a complaint with the police against the alleged perpetrator of the cyber security incident. This complaint should be made to the local police zone within which your company's registered office falls.

CyberAid, a platform for registering such complaints that is accessible to all police officers in Belgium, has been available since early 2022, when it was created at the initiative of the director of the Federal Judicial Police. 21 cyber crimes have been registered to date. The police officer documenting your complaint may first ask you a few questions to determine the type of crime involved. The platform will then help them register your complaint efficiently and offers a whole range of practical advice that officers can give to victims.

This platform is also available to all magistrates on request.

04

LEGAL OBLIGATIONS RELATING TO AN INCIDENT

When a company falls victim to a cyber incident, there are multiple external stakeholders who must be made aware of the situation.

The following steps must be taken here to better respond to the situation:

- Keep an offline copy of the documents you will need in the event of an incident. Remember that when a cyber security incident occurs, you may not have access to the files on your computer, so it is always a good idea to keep a hard copy and/or offline copy of any documents you may need during a cyber security incident or crisis.

- Do not link your backups to the rest of your system. You will need to have these available and should also have backups that are not linked in any way to the rest of your system, otherwise you run the risk of the infection on your system also infecting your backups, rendering them unusable.
- Document every step of the cyber security incident. In times of crisis, do not rely on your memory alone! Be sure to document in writing every action taken, e.g. reporting the incident, gathering evidence, conversations with users.

4.1 GENERAL OBLIGATIONS

Once you have established the list of recipients of your communication on the cyber security incident and the content of the information you will disclose, you must then decide when to contact them. This timing depends on the goals of your communication:

- Some stakeholders will need information as soon as possible, as they can help contain the incident (e.g. senior management and company employees);
- Other stakeholders will need to be contacted within a time frame required by law (e.g. the DPA);
- Other stakeholders (e.g. the media) may contact you, in which case you should have your response ready. Bear in mind that, in order to avoid alerting the cyber criminal that you are on their trail, it may prove necessary to say nothing (no communication) between detecting the incident and having a full overview of the incident and an action plan;
- You must also report the incident to the criminal investigation authorities in order to have proof that an incident has actually occurred (see above). This is the document confirming that you have filed a complaint that will be required by the authorities in order to take your statements into account.

The cyber security incident you are facing may not be an isolated case and the relevant authorities may have information that would allow you to contain the incident more quickly.

You should get in touch with the relevant law enforcement authorities as soon as possible after discovering the cyber security incident, given that criminals are difficult to track and there are a number of actions to be taken (identification of their IP address, etc.).

The criminal investigation authorities need all available information about an incident to qualify the crime and identify the suspect. Some of the information to be provided to the police in the case of internet fraud (a 'conventional' offence committed by electronic means) may differ from that needed in the case of computer crime (hacking, sabotage, espionage). During an investigation, investigators will request, collect and search for additional information.

4.2 OBLIGATIONS TO INSTITUTIONAL STAKEHOLDERS

4.2.1 DPA

According to the GDPR, the Data Protection Authority (DPA) must be notified of any data breaches, i.e. security breaches resulting in the accidental or unlawful unauthorised destruction, loss, theft, disclosure, etc. of personal data. This is a legal obligation; failure to comply may result in significant sanctions.

The controller must notify the DPA within 72 hours of becoming aware of a breach.

It is not mandatory to report data breaches that are unlikely to pose a risk to the rights and freedoms of individuals, e.g. if the data are already in the public domain or are sufficiently encrypted and the controller has a backup of the data.

In all other cases, data breaches are reported to the DPA via an electronic form which, once completed, is transmitted via an internet portal. Forms sent by email will not be processed.

The form must be completed in one of Belgium's three national languages, although technical annexes may also be written in English.

<https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles>

(available in Dutch, French and German)

<https://www.autoriteprotectiondonnees.be/publications/mode-d-emploi-relatif-a-l-utilisation-de-formulaires-electroniques.pdf>

(available in French)

Save for some exceptions, where a personal data breach is likely to pose a high risk to the rights and freedoms of a natural person, the data controller is required to inform said person as quickly as possible.

Where it is not possible to identify the victims of a data breach, the controller may inform them via public media. Such notifications should be clear and easy to understand.

The DPA recommends giving data subjects the following information as a minimum:

- The name of the data controller;
- The necessary contact details should they require any further information;
- A brief description of the incident that led to the data breach;
- The (presumed) date of the incident;
- The type and nature of the personal data involved;
- The possible consequences of the data breach for the data subjects;
- The circumstances under which the data breach occurred;
- The measures taken by the data controller to prevent the data breach;
- Measures that the data controller recommends the data subjects take to limit the damage caused.

4.2.2 CERT.be

A Voluntary notification by a company affected by a cyber incident

Should a company not subject to legal obligations in this respect voluntarily report an incident to the federal Cyber Emergency Response Team (CERT.be, the operational service of the CCB), this is not considered a request for intervention. An email response from a CERT.be operator is not guaranteed and depends on the severity of the incident and the status of the company reporting the incident. The CCB provides technical and organisational advice on its website (<https://www.cert.be/en/advisories>) on dealing with a cyber incident, but does not assist companies in taking the necessary action.

(1) NIS: legislation on network and information system security of general interest to public safety.

(2) OES: Operator of Essential Services, a public or private entity active in Belgium in one of the following sectors: energy, transport, finance, health, drinking water or digital infrastructure.

Reporting an incident helps the CCB to collect, analyse, flag up and act on confirmed threats. The content of the reports is automatically extracted and analysed to consolidate knowledge that can then be used to issue warnings and alerts, document known vulnerabilities and facilitate threat analysis.

B Obligation to report incidents affecting Network and Information System Security (NIS¹ applicable to Operators of Essential Services²)

Operators of Essential Services (OESs) are legally required to report cyber incidents to the CCB. Depending on their sector of activity, affected OESs may also be obliged to notify the CCB of other incidents. [The table on page 19](#) provides a summary of these obligations, the deadlines for reporting an incident and the procedure to be followed.

Voluntary notification

What?	To whom?	Deadline?	How?
<p>All incidents having a significant impact on the continuity of an essential service.</p> <p>Voluntary notifications shall not impose on the reporting entity any obligations to which the entity would not have been subject if it had not issued said notification.</p>	The CCB.	As quickly as possible.	Via the methods set out on the website of the Centre for Cyber Security Belgium (CERT.be service): https://cert.be/en/report-incident

Source: CCB, <https://ccb.belgium.be/en>

Obligation to report NIS incidents applicable to OESs (summary)

What?	To whom?	Deadline?	How?
<p>a) OESs that are not supervised by the NBB</p> <p>All incidents having an impact on the availability, confidentiality, integrity or authenticity of networks and information systems vital to the essential service(s) provided by the OES in question.</p>	<p>a) OESs that are not supervised by the NBB</p> <p>Notification sent to three authorities simultaneously:</p> <ol style="list-style-type: none"> 1. The Centre for Cyber Security Belgium (CCB); 2. The National Crisis Center (NCCN); 3. The sectoral authority and/or sectoral CSIRT. 	<p>Without delay, i.e. as quickly as possible</p> <p>The OES in question should not wait until it has all the relevant information about an incident before reporting it.</p> <p>Where the information in an OES' possession indicates that it should report the incident, the OES must do so without delay.</p>	<p>a) OESs that are not supervised by the NBB</p> <p>Fill in the form on the NIS notification platform: https://nis-incident.be</p> <p>This platform then automatically sends the information to the relevant authorities.</p> <p>The platform can be accessed online via a secure connection and an ID unique to each OES.</p> <p>If this platform is unavailable, the OES must report the incident using the methods listed on the CCB website (https://cert.be/en/report-incident).</p>
<p>b) OESs that are supervised by the NBB</p> <p>All incidents having a significant impact on the availability, confidentiality, integrity or authenticity of networks and information systems vital to the essential service(s) provided by the OES in question.</p> <p>The NBB is responsible for gauging the scale of the impact.</p>	<p>b) OESs that are supervised by the NBB</p> <p>Direct notification to the NBB using the methods specified by the same.</p>	<p>b) OESs that are supervised by the NBB</p> <p>Direct notification to the NBB using the methods specified by the same.</p> <p>If the NBB requires an OES to use the notification platform, the CCB and NCCN will also be notified at the same time. If not, the NBB will immediately notify the CCB and NCCN itself.</p>	

Source: CCB, <https://ccb.belgium.be/en>

C Obligation to report NIS incidents applicable to Digital Service Providers¹

Digital Service Providers (DSPs) must also report, as soon as possible, any incident having a negative impact on the security of networks and information systems to the CCB, the National Crisis Center and the FPS Economy.

The table below outlines the obligations relating to such reports.

(1) A Digital Service Provider (DSP) is a legal entity that provides a digital service referred to in Annex II of the NIS Law, has its main place of business in Belgium and is not a micro or small enterprise.

Obligation to report NIS incidents applicable to DSPs (summary)

What?	To whom?	Deadline?	How?
<p>A DSP must report any incident having a significant impact on the provision of the digital service(s) (online marketplace, online search engine or cloud computing service) it offers in the European Union.</p> <p>An incident is any event that has a real negative impact on the security of networks and information systems.</p> <p>Network and information system security refers to the ability of networks and information systems to withstand, at a given level of trust, actions that compromise the availability, authenticity, integrity or confidentiality of the data stored, transmitted or processed, and the related services that these networks and information systems provide or make accessible.</p>	<p>a) Notification sent to three authorities simultaneously:</p> <ul style="list-style-type: none"> - The Centre for Cyber Security Belgium (CCB) - The National Crisis Center (NCCN) - The FPS Economy (sectoral authority) <p>b) A DSP providing a digital service to an OES must also notify, without delay, the OES in question (its customer) of all incidents relating to the digital service(s) provided to this OES and which have a significant impact on the continuity of the OES' essential services (in the event of an incident, the DSP must therefore question all of its customers impacted by the incident and who would be OESs).</p> <p>The OES must then report the incident using the procedures specific to OESs.</p>	<p>The incident must be reported immediately, i.e. as quickly as possible after the DSP has access to the information needed to assess, in whole or in part, the impact of an incident.</p> <p>The DSP in question should not wait until it has all the relevant information about an incident before reporting it.</p>	<p>Fill in the form on the NIS notification platform: https://nis-incident.be</p> <p>The DSP must, at its own initiative, ask the FPS Economy (nis-dsp@economie.fgov.be) to create a login (username/password) to allow it to access the NIS notification platform.</p> <p>This platform then automatically sends the information to the relevant authorities.</p> <p>The platform can be accessed online via a secure connection and an ID unique to each DSP.</p> <p>If this platform is unavailable, the DSP must report the incident using the methods listed on the CCB website (https://cert.be/en/report-incident).</p>

Source: CCB, <https://ccb.belgium.be/en>

During an incident, we often deal with the most urgent matters and lose sight of the fact that rapid action needs to be taken regarding day-to-day management vis-à-vis public authorities or bodies. That is why we have tried, by creating this roadmap, to help you and guide you towards direct points of contact to aid you in getting through an incident while continuing your operations as best you can. When we were developing the roadmap, we worked with the relevant authorities to come up with practical solutions, points of contact and ways to ease existing procedures. This is the first step in a longer process, so we will continue to develop and improve the solutions given here where necessary.

4.2.3 FPS Finance

Owing to the numerous and diverse tax obligations within the FPS Finance and with a view to facilitating the procedure for companies affected by a cyber incident, the General Administration for Taxation (**AGFisc**) also has plans to establish a point of contact for companies to report incidents.

- **Reporting a cyber incident to the tax authorities**

AGFisc will initially serve as this point of contact and will relay reports to the relevant tax authorities.

- For SMEs: secr.pmekmo@minfin.fed.be
- For large companies: goge.beheer.gestion@minfin.fed.be

AGFisc will use the information provided by the company in question to determine the tax obligations actually affected. To this end, affected companies must ensure that they report any cyber incidents to the FPS Finance contact point as quickly as possible.

The company's legal representative, or their proxy, must provide the following information:

- **Details of the data subjects:**
Company name, company number, contact person details.
- **Information about the impact of the cyber incident:**
 - (Estimated) time frame for data recovery;
 - Whether the company is part of a group/a VAT unit
 - Whether the company has any international; exchange obligations (BEPS 13 – CRS/FATCA – DAC).
- **Information about the impact of data regarding the FPS Finance:**
 - Whether the company's MyMinfin account is blocked;
 - Whether there are any problems affecting the mandate/enforcement of the mandate;
 - Whether there is any ongoing monitoring/claims within the FPS Finance.
- **Proof of the cyber incident:**
You must attach a copy of the incident report from the federal police.
- **Which tax obligations are affected?**
Please specify the tax authorities to be contacted. An overview of these obligations is available here: <https://finance.belgium.be/en/enterprises>

If necessary, AGFisc will contact the affected company to ensure that the priority tax obligations (or those that are deemed to be a priority) are indeed taken into account.

The relevant services will then contact the affected company to discuss potential accommodations.

Points of contact:



secr.pmekmo@minfin.fed.be

goge.beheer.gestion@minfin.fed.be

4.2.4 NSSO

Companies are required to make a series of declarations to the National Social Security Office (NSSO). When a company has fallen victim to a cyber incident, it may be unable to make these declarations due to its data being lost or unavailable or its IT system being blocked, for instance.

The main declarations required are listed below.

- 1 Dimona** - The immediate registration of a new employee, whereby an employer indicates the beginning and end of an employment relationship with an employee.
Deadline: before the employee is hired.
- 2 Limosa** - Declaration for posted workers who come to work in Belgium temporarily or partially.
Deadline: before the employee is hired.
- 3 DmFA** - The quarterly declaration whereby the employer provides the NSSO with data on employee wages and performance.
Deadline: within one month following the quarter to which the declaration relates.
- 4 Declaration of works**
(Only applies to certain sectors).
Deadline: before the work starts.
- 5 Checkinetwork** – registration of daily attendance on (certain) sites in the construction and meat sector.
Deadline: every day before the person in question starts work
- 6 Payment of social security contributions**
Deadline: the employer pays the contributions on a quarterly basis. The NSSO must receive these contributions by the last day of the month following the quarter in question.

The NSSO is aware of the difficulties that companies affected by cyber incidents may face and has introduced a procedure for reporting such situations. Reports must be made within 24 hours of the incident being identified, following which the relevant NSSO services will, if necessary, contact the companies concerned and suggest suitable solutions.

4.2.4.1 Reporting a cyber incident to the NSSO

- Fill in the NSSO contact form (available in Dutch, French and German):
<https://www.onss.be/contactez-nous>;
- The report must be made by a legal representative of the company;
- Select *Reporting a cyber incident* as the subject;
- Select *Company* as the profile;
- Complete the following fields: first name, surname, email address, company number, company name;
- Provide the telephone number of the person or team within your company that the authority can contact about this report. Additional contact details can be entered in the *Message* field;

As a reminder, and to avoid any type of fraud or scam, employers who are not local or provincial authorities must pay the amounts due into the following NSSO account:

IBAN: BE63 6790 2618 1108

BIC: PCHQ BEBB

- In the *Message* field, please:
 - Describe the incident;
 - Specify which NSSO obligations (see above) the company is no longer able to fulfil;
 - Indicate whether your company's access to the NSSO should be temporarily blocked (your representative/s will continue to have access);
 - If possible, give the estimated duration of the incident.
- Please note: you must attach a copy of the incident report from the federal police.

4.2.4.2 After you have reported an incident

- You will receive an acknowledgement of receipt;
- Your report will be forwarded internally to the various NSSO departments concerned. If necessary and depending on the problems in question, the NSSO will contact you;
- Once you have submitted your report, you do not need to go through an additional emergency Dimona procedure. Use the same contact form (<https://www.onss.be/contactez-nous>, available in Dutch, French and German) to report the end of the cyber incident as soon as possible.

Point of contact:



www.onss.be/contactez-nous 

This link should also be used for notifications relating to NIHDI obligations.

4.2.5 NIHDI

Companies also have obligations to their insurance organisations (health insurance funds) and the National Institute for Health and Disability Insurance (NIHDI) with a view to ensuring that the affected employees can be compensated by the insurers.

Employers are asked to supply the required information either electronically or on paper. Depending on the document in question, the employer or employee may have to submit it to the insurance body. The main documents required are listed below.

- 1 Remuneration information sheet .
- 2 Certificate of insurance conditions.
- 3 Declaration in case of adapted work as a salaried employee.
- 4 Declaration of authorised work in a sheltered workshop under Joint Committee 327.
- 5 Declaration of unpaid work during a period during which the employee is unable to work.
- 6 Certificate confirming that a maternity allowance has been granted to a female employee who has had to be removed from the workplace.
- 7 Monthly declaration of income following the introduction of a maternity protection measure.
- 8 Certificate confirming remuneration for breast-feeding breaks.
- 9 Certificate confirming an employee's holidays.
- 10 Certificate confirming an employee's return to work.
- 11 Certificate confirming the return to work of a female employee alternating between working days and postnatal leave.
- 12 Certificate to be completed when a female employee has taken all their postnatal leave.

Reporting a cyber incident to the NIHDI

Most of these declarations must be made electronically by a set deadline. However, some declarations are still made using paper forms.

In the event of a cyber incident that makes it impossible for an employer to complete the required form (electronically and/or on paper) in time, said employer must report this incident to the NSSO (<https://www.onss.be/contactez-nous>), which will in turn inform the National Intermutual Board, the six insurance bodies and the NIHDI's Administrative Oversight Team as soon as possible.

The affected company must complete the following steps:

- Fill in the NSSO contact form (available in Dutch, French and German): <https://www.onss.be/contactez-nous>;
- The report must be made by a legal representative of the company;
- Select *Reporting a cyber incident* as the subject;
- Select *Company* as the profile;
- Complete the following fields: first name, surname, email address, company number, company name;
- Provide the telephone number of the person or team within your company that the authority can contact about this report. Additional contact details can be entered in the *Message* field.

- In the *Message* field, please:
 - Provide a description of the situation related to the cyber incident and the consequences of the incident;
 - Specify which obligations regarding the NIHDI (see above) are affected and the persons concerned;
 - If possible, give the estimated duration of the incident;
 - Provide a description of the situation related to the cyber incident and its consequences.

Please note: you must attach a copy of the incident report from the federal police.

It is also worth noting that although declarations must typically be made electronically, the employer may use paper forms in a case of force majeure (if electronic transmission is no longer possible).

Once the incident is over, the employer must inform the NSSO via the same contact form. The NSSO will then notify the relevant bodies regarding payments.

Point of contact:



www.onss.be/contactez-nous

The incident is reported via the NSSO, which in turn informs the National Intermutual Board, the six insurance institutions and the NIHDI's Administrative Oversight Team.

4.2.6 NEO

The National Employment Office (NEO) has also introduced measures allowing companies that are victims of cyber attacks to fulfil their obligations.

Companies are subject to the following legal obligations concerning the NEO.

1 Companies must report the following:

- Anticipated periods of temporary unemployment due to a lack of work for economic reasons.
Deadline: no later than a certain number of days before the actual date of the period during which compensation will be paid for staff laid off temporarily at short notice (typically seven days but this varies from sector to sector).
- The first actual day of temporary unemployment due to bad weather or lack of work for economic reasons.
Deadline: the first actual day of temporary unemployment.
- Temporary unemployment due to technical issues.
Deadline: the first actual day of temporary unemployment.

2 Companies must register the following:

- The numbers of temporary unemployment control forms in an electronic validation book.
- Deadline:** by the time the forms in question must be issued at the latest.

3 Companies must submit the following:

- Electronic declarations on social risks.
- Deadline:** no mandatory deadline, except for form C4, which must be submitted by the last working day.

Reporting a cyber incident to the NEO

Any cyber incidents must be reported when a company contacts the NEO to fulfil one of its obligations.

The NEO is offering to ease its procedures to take into account the difficulties faced by affected companies, namely by introducing the following changes:

- 1 As a rule, notifications involving temporary unemployment must be made electronically. However, in the event of technical issues this may be done by registered letter.
- 2 The registration of control forms can also be done in a paper validation book, or the employer can contact the NEO to communicate the necessary data directly for a short period of time.
- 3 Social risk declarations, with the exception of form C4, must be made electronically. However, these are not subject to a deadline per se. Paper declarations should be used only in very unusual situations.

Point of contact:



The closest unemployment office to the affected company's location shall serve as the point of contact for said company





05

SYSTEM
RESTORATION

A cyber attack can have very different consequences for the affected company's activities (e.g. unavailability of digital services and tools, impact of the attack on partners). As such, crisis management teams must contain any incidents and restart the organisation's operations in a controlled manner.

Impact management can take several weeks, so it is vital that companies have a strong crisis organisation in place from the outset.

5.1 INCIDENT MITIGATION AND BUSINESS CONTINUITY

Affected companies take mitigation measures to prevent the situation from getting worse or, at the very least, to promptly alleviate the impact on company operations and services.

Containing a cyber security incident means limiting the damage and stopping the attacker. You need to find a way to minimise the risk to your organisation while continuing to do business. You need to prevent the incident from spreading to other systems, devices and networks within your organisation and beyond.

At the start of this phase, your company will have to make an important strategic decision: should systems be taken offline immediately to allow for the fastest possible recovery, or should you take the time to gather evidence against the cyber criminal attacking the systems?

In some cases, an (immediate) return to normal operations will simply be impossible. Containment should aim to do everything possible to restore normal operations,

i.e. to recover a usable system by preserving access for authorised users and blocking the attacker.

Once the scope of the attack has been determined, it is a matter of protecting IT systems against further attacks. These new measures may lead to a significant change in practices, particularly with regard to the administration and use of digital services and tools.

Depending on the severity of the cyber incident, affected companies use **business continuity** plans to ensure they can maintain critical operations based on a predefined prioritisation process. As such, to ensure business continuity, a company may decide to take emergency measures to facilitate the processing of critical transactions while efforts to restore the system are under way, or to use an alternative service provider if the primary provider is unable to recover from the incident within a reasonable time frame.

The strategy for managing a cyber incident, backed up by business continuity measures, must also provide for operational solutions enabling the organisation to **continue operating without digital tools over a potentially very lengthy period**.

The end of a cyber security incident does not mean that the affected company is immediately operational once again, since **the reconstruction and reconsolidation of all systems may take several months**. The end of the crisis is instead deemed to be when the organisation's essential activities can be resumed as usual.

Finally, when the crisis is over, it is important to **restore confidence** both within the company, among employees, and externally, among customers, suppliers and all stakeholders.

USEFUL POINTS OF CONTACT



www.cert.be/en/report-incident



www.cybersecuritycoalition.be/tools/

.AGORIA

www.agoria.be/agoriacconnect-trouvez-votre-specialiste-en-cybersecurite



www.febelfin.be/en/themes/fraud-security



www.ccb.belgium.be/fr



www.safeonweb.be/en

Safeonweb.be quickly and accurately informs and advises Belgian citizens on cyber security, online security and critical digital threats.

Have you received a suspicious message? Forward it to suspect@safeonweb.be and then delete it. Do you have a question about cyber security? Or maybe a suggestion? Do you want to give your testimony as a victim? Send your question to info@safeonweb.be. A team of cyber experts will be happy to help.

LA FEB

+50.000

small, medium and large businesses



75%

of employment in the private sector

2/3

of value added



80%

of exports

3 Regions

Pointing the way for the Belgian business community



BUSINESSEUROPE



The FEB is the Belgian member of BusinessEurope

Coordination and final edit

Nathalie Ragheno

Editorial Secretariat

Anne Michiels, Charlotte Jonné

Translation

FEB Translation Department

Publication Officer

Stefan Maes

Layout by

Landmarks

Illustrations by

Shutterstock

Printed by

Graphius

Content Officer

Stefan Maes,
Rue Ravenstein 4, BE-1000 Brussels

Publication date:

December 2022

Deze publicatie is ook beschikbaar in het Nederlands.
Cette publication est également disponible en français.

www.feb.be > Publications

Legal registration D/2022/0140/10

ISBN 9789075495768





The FEB – the voice of business in Belgium – has 40 member federations, which in turn represent more than 50,000 small, medium and large companies. All told, they account for 75% of employment in the private sector, 80% of Belgium's exports and two thirds of its added value. As the country's only multi-industry umbrella organisation for employers, VBO FEB represents companies from all three regions of Belgium.

Our [latest publications](#) are available on our website



WWW.FEB.BE/EN/

