

Emergency Response to Hackers

What should you do in the event of a cyber attack?

If you've had a fire, you call the fire brigade. If you've had a break-in, you call the police. But what do you do if your IT systems have been hit by a cyber attack?

Still too few businesses are preparing properly for such an eventuality. Even though it is many times more likely to happen than a fire. What is the result? Damages running into the tens of thousands, reputational damage, and the loss of valuable data.

So you should always be prepared for a 'digital fire'.



Preparation

There are several things you should actually have under control at all times, even though they might seem obscure.



Safe back-up system

Everybody knows it is sensible to back up your data on a regular basis. And yet we don't always manage to do it consistently. Our advice: work with your ICT service provider to ensure that as a minimum the following three points are in order.

- Perform back-ups frequently.
- Store the back-up in both a digital and a physical location.
- Test your back-up regularly.

Good logging

If you want to be able to act rapidly in the event of a digital attack, it is essential to have good log files. Make sure there are always log files available for the key components in your network. And make sure they can't become infected with the virus that hackers put into your system.

Crisis protocol

In a crisis situation, there usually isn't time for unhurried consideration and action. So it is a good idea to create a crisis protocol. This usually consists of two parts:

- Part 1 focuses on the running of the organisation in a crisis situation, and is also known as the Business Continuity Plan (BCP).
- Part 2 focuses on internal and external communications.

Important information also available on paper

Hacking can result in digitally stored contact details no longer being available, and losing access to the internet or company network to look them up. In some cases, one or more communication channels stop working. Therefore, you should keep important information from your crisis protocol available on paper. This should certainly include:

- individuals that are involved in the crisis team;
- contact details of all employees;
- contact details of public authorities;
- contact details of customers (sometimes you are part of a chain);
- contact details of suppliers (you may be part of a chain);
- contact details of your ICT partner or security experts;
- the information available on the dark web about your company.

In the event of a data breach, you must have the contact details of the following authorities to hand:

- **AVG (www.gegevensbeschermingsautoriteit.be) regarding GDPR.**
This is where you report a data breach or infringement.
- **CERT (www.cert.be)**
- **Local Police**
To submit a report.

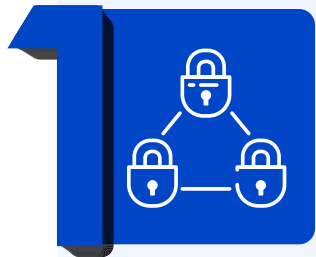
Insurance

There are policies that cover you against part or all of the damage that a cyber attack can cause for your organisation and third parties. It is worthwhile to research whether an insurance policy - and which one - makes sense for you, taking into account the functioning and risks of your organisation.

After taking out an insurance policy, always keep the contact details of your point of contact there on paper.

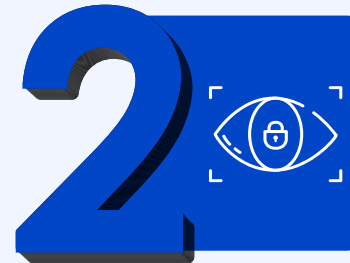
What if you fall victim to an attack?

If your ICT systems have been attacked, it is best to follow a standard procedure. Discuss the steps summarised below together with an ICT specialist with experience in cyber attacks and also a communications specialist. These individuals can be either internal or external to the company.



LIMIT SPREAD

The systems in which the virus has been found must be disconnected from the company network as soon as possible. You should preferably also disconnect the exempted systems to protect them from becoming infected. Never switch off the computer because this makes the investigations more difficult.



ANALYSE INFECTION AND IMPACT

Investigate which virus it is, how it entered and how far (internally and potentially externally) it has spread. This forms the basis for a first draft plan for the recovery options. Always prioritise the critical devices in your network, in order to be up and running again quickly.



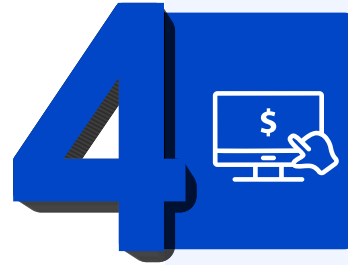
ANALYSE THE BACK-UP

When reconnecting the back-up, you need to bear in mind the following aspects:

- **Quality**
Is the back-up complete and does it contain all the essential information?
- **Age**
How old is the back-up? How much information do you permanently lose by reconnecting?
- **Security**
Has the back-up been infected with the virus?
- **Time**
How long will it take for the systems to be running again?

Reconnect or start from scratch?

After this analysis, it is time for a major decision: reconnect the back-up or install everything from scratch? In the crisis protocol you should include who will take this decision at what stage and research in advance a supplier that is able to rapidly supply new (or refurbished) hardware to your location.



TO PAY OR NOT TO PAY?

If reconnecting a back-up is not an option, it will be time to make an important decision: to pay or not to pay 'ransom money' for the hacked information? This decision involves several important considerations:

- How certain is it that you will get your data back after paying them?
- Who will decide whether to pay?
- What is the maximum amount you are willing to pay?
- Who will conduct the negotiations with the hackers?
- For anonymity purposes, payment is often requested in a digital currency (e.g. Bitcoin). How do you buy these currencies and how do you pay with them?



INTERNAL AND EXTERNAL COMMUNICATIONS

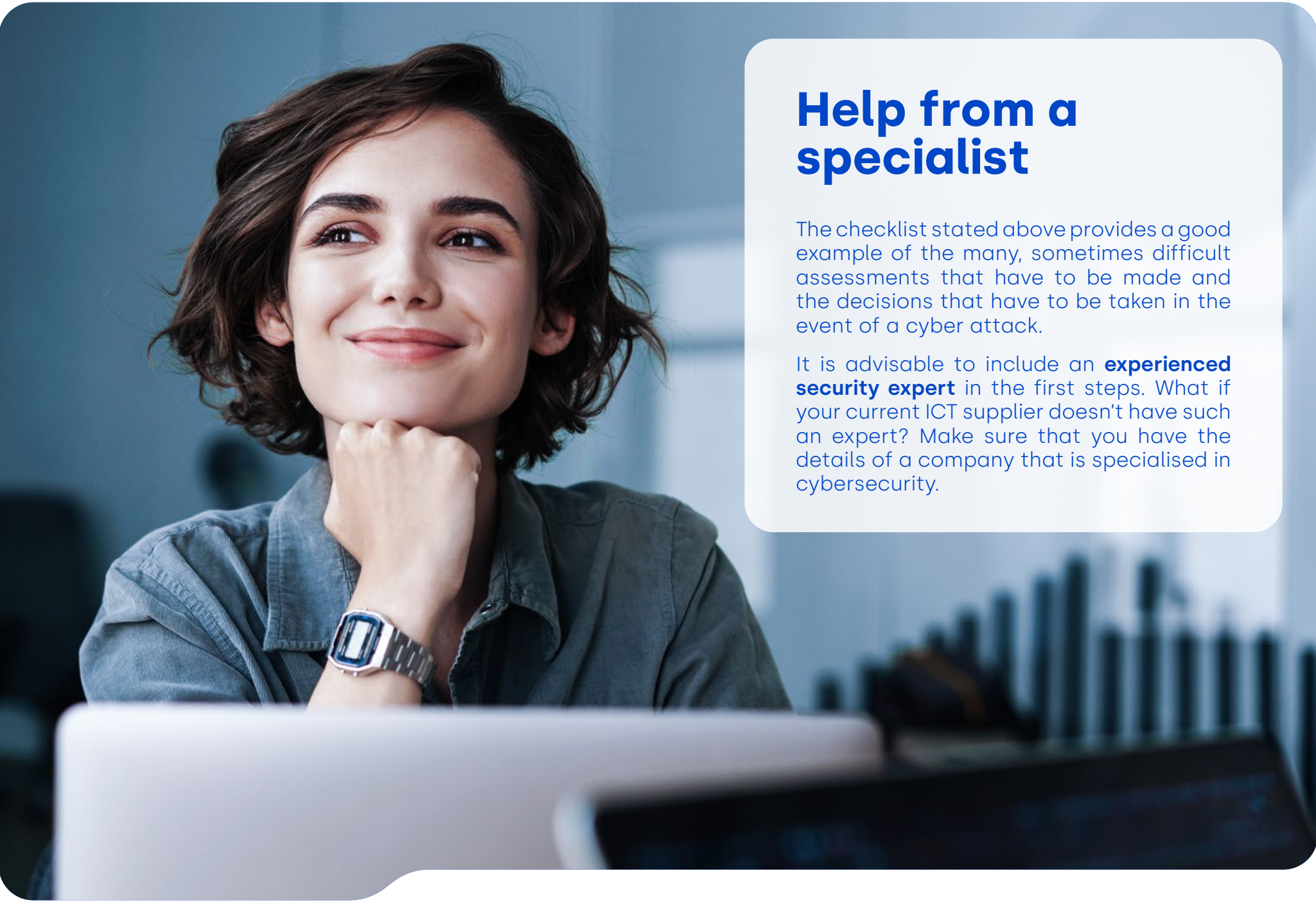
Internal and external communications about such a drastic event as a hack must be carefully considered. It is a good idea to plan it beforehand in the crisis protocol. This should include answers to questions such as:

- How and when do we notify our employees?
- How do we do that for employees that are working at home?
- When do we notify the relevant external parties (suppliers and customers)?
- Are there any other internal and external stakeholders that need to be notified before we go to the press?
- How do we avoid the press receiving information before we have communicated anything to the outside world ourselves?
- What information are we going to send to the press and when should we do it?

Customers, suppliers & government

If your business data has been hacked, an external organisation has gained access to information that may also concern people and organisations outside your company.

This has implications for the General Data Protection Regulation (GDPR). Compile a list of businesses, organisations and people who need to be notified that information about them may possibly have been leaked and what information it is. You should also make contact with the public authorities listed above within 72 hours.



Help from a specialist

The checklist stated above provides a good example of the many, sometimes difficult assessments that have to be made and the decisions that have to be taken in the event of a cyber attack.

It is advisable to include an **experienced security expert** in the first steps. What if your current ICT supplier doesn't have such an expert? Make sure that you have the details of a company that is specialised in cybersecurity.

Save yourself some stress and money?

It is a cliché, but prevention is always better than cure. How can we make the likelihood of a cyber attack on your organisation as small as possible?

Let's get around the table and look together at what would be most appropriate. Is it an awareness training for your staff? A security audit? Or maybe it's monitoring?

Would you like to save yourself some stress and money? Feel free to drop us a line and we can look together at what we could do for your organisation.



Secutec BV (HQ)

Boomsesteenweg 41/11
2630 Aartselaar
Belgium

+32 (0)3 877 82 93
info@secutec.com

Secutec Nederland BV

Breda Business Park - Lijndonk 4
4825 BG Breda
The Netherlands

+32 (0)3 877 82 93
info@secutec.com

Secutec GmbH

Gewerbestrasse West 14
4921 Hohenzell
Austria

+43(0) 664 301 05 68
office-dach@secutec.com

Secutec Canada

4000-1 Place Ville Marie
H3B4M4 Montréal
Canada

+1 438 728 84 32
info@secutec.com

Australia & New Zealand Region

Sonny Bal
+61 449 932 977
sonny.bal@secutec.com