CHEOPS REPORT

Are you **‘always on’?**

Available **round the clock**

Everyone expects you to be ‘always on’: your customers, suppliers, employees – and not forgetting yourself, of course. The most important processes in your company depend on IT systems and must never be allowed to drop out. At least they mustn’t if you value your reputation and customer base. Working from nine to five is a thing of the past, so you have to make sure that your business systems are available round the clock. ‘Always on’, that is. This guide shows you how to prevent that dark day when you are ‘always off’. We examine the risks that you run and why and we also present you with a series of practical measures for improving and safeguarding the continuity of your business systems and operations.

Downtime is not an option

THE STAKES ARE HIGH

Do you know what the risks are that you run when your business systems leave you in the lurch? For a midsized company, every hour that you are not operating can quickly cost you thousands – even tens of thousands of euros. There's the loss of production, potential loss of customers and additional costs and communication, not to mention possible compensation. And most companies have never even calculated the cost of that risk.

In addition to the financial impact and a possible loss of valuable data, an interruption to your productivity can also cause damage to your reputation and competitive position. It can result in the market value of large organisations taking a nosedive, or serious legal consequences.

And what happens if your company can't continue doing business because the important data you have lost cannot be recovered? So it is logical that no one should underestimate the importance of business continuity.

IT AS A CENTRAL PIVOT

It's hard to imagine your business processes functioning without technology – and the tech we use is becoming more and more complex all of the time. Every day, increasing amounts of data circulates automatically round your company and outside it. Your staff and customers all want access to that information, where and when it suits them.

More than ever a well-designed and secure IT infrastructure is essential for being thought of as a reliable business partner. But the strict regulations governing privacy and confidentiality don't make things any easier.

The impact of downtime and loss of data is far greater than you think.

LIMIT THE RISKS

Business continuity is much more than just getting started again quickly after an emergency has occurred. And your IT department is not the only area of the company responsible for making it happen. For that reason, we recommend you take an integrated approach. These days, although having 100 per cent uninterrupted operations may sound like utopia, you can dramatically reduce the biggest risks by taking a targeted approach. This document tells you how.

What affects ‘always on’?

The chance of you having an IT problem that disrupts your business has never been greater than it is now. The number of applications and volume of data is growing rapidly and more and more is happening online and in real-time. If you want to be ‘always on’, your strategy needs to take account of a number of important trends in IT:

1. ALL IT APPLICATIONS ARE INTERCONNECTED

Originally, organisations tended to keep their business processes and the IT applications that go with them separate from one another. These days, companies integrate their applications and departments as much as possible in order to increase efficiency. When an application drops out in one department, this can have a major impact on the essential processes in another. Also, the maintenance of some applications may be outsourced, while others are handled in-house. As a result, the technological setup supporting all of these business processes can be difficult to untangle.

2. YOUR BUSINESS DATA IS EVERYWHERE

As a result of the arrival of cloud computing, social networks, bring your own device (BYOD – i.e. employees who also use their own laptop, tablet or smartphone for work) and the Internet of Things (all possible devices, detectors and sensors that send data through to your IT applications), everything and everyone is connected with each other. We are mobile in the way we work and find it normal to be online everywhere and at all times. Business and personal things run alongside each other, often on the same devices. Business data and the machines we use for our job are no longer kept within the physical confines of your business network and hence are difficult to protect and keep secure.

Business and personal things run alongside each other. Your data is everywhere.

3. TOO LITTLE REALISATION OF THE RISKS

A solid approach for keeping your IT available begins with fully understanding the possible risks. That’s where things tend to go wrong. For instance, too many companies wait before switching to newer, better protected versions of applications and operating systems, even when the manufacturer stops providing technical support for older versions. There is also a lack of realisation that too little is being invested in the specialist management that IT

in general and IT security in particular requires. As a result, vulnerabilities that might have been avoided suddenly come into being.

4. REGULATIONS ARE BECOMING STRICTER

The increase in data protection risk is prompting governments to take measures designed to protect people's privacy better. In the European Union, an important milestone in this area is the advent of the General Data Protection Regulation (or GDPR). These new regulations require companies, from 2018, to introduce a new and stronger framework for the management and protection of personal data in the EU. They include things such as access to and the transferability of personal data, the right to be 'forgotten' or to be notified if there is a possibility that your personal data has been leaked. The new regulations also foresee significant penalties for offenders.

5. THE PHYSICAL RISKS ARE INCREASING

Finally, economic and political factors – such as the plan to switch off power when there are electricity shortages – can also result in downtime. We are having to cope more frequently with exceptional weather, including cold snaps and heat waves, storms and floods. All of which means a greater risk of downtime.

Legislation is becoming much stricter. In Europe, the advent of GDPR is a milestone.

Think strategically about IT and business continuity

It should be clear that business continuity, IT and the way they are protected need to be approached strategically. Restricting risks as much as possible is one major reason. Another reason, just as important, is that the technological choices and strategy you implement today can create a massive competitive edge for you. If you are lacking the expertise or manpower, the best thing you can do is bring in a specialist partner. A partner who gets away from bits and bytes and who is capable of working with you to bridge the gap between IT and your business.

What are **the real risks?**

We have already talked about trends. But do you know what the biggest threats are for the continuity of your IT systems? Maybe you'd think first of fire or a natural disaster… But research tells us that interruptions to systems and downtime caused by those sorts of 'obvious' problems actually rank last in the top 5 most frequently occurring risks. There are all sorts of factors that can undermine your business continuity. We have placed them in the order in which they occur most frequently. The top 3 play musical chairs with each other, depending on the source:

1. IT SYSTEMS THEMSELVES

Reason number one, which occurs with abundant frequency, is the failure of IT systems caused by the poor functioning of hardware, software or inconsistent data. And all too often that is the result of bad management. Managing your IT infrastructure and systems on a continuous and in-depth basis is the absolute fundamental requirement if you want to be 'always on'. Remember, you want to prevent at all times that a server crash or an essential software program going wrong brings your company grinding to a halt.

2. UNWANTED INTRUDERS

Rising rapidly up the list of threats are malware (especially ransomware) and other activities carried out by cybercriminals, such as stealing data and your identity. Having solid defences against these intruders is an absolute priority, because new types of threat are cropping up all the time (see box below). And unwanted intrusions are not always online: conventional break-ins and theft of your equipment also occur on a daily basis.

3. ELECTRICITY

Would you have thought that power outages are among the biggest causes of disruptions to business continuity? Many companies omit to build in emergency power supplies and test them regularly. Modern datacentres provide redundant power by using powerful emergency generator systems, offering a safe alternative for your local infrastructure.

Criminals strike online and offline.

4. YOU AND YOUR COLLEAGUES

You may already be aware that your staff can cause damage inadvertently, for example by being careless with passwords. We also include the loss of devices, usually by being inattentive.

Less often – but not all that rare – is deliberate sabotage or theft, caused for instance by people who are leaving the company, who are unhappy with their job, or who simply want to do harm. Human errors in the IT department usually have greater consequences than a mistake by an ordinary computer user. Incorrect installations or configurations can always happen, but you need to be prepared for the possible consequences.

5. FORCE MAJEURE

Force majeure, or a disaster, is a less common cause of a disruption. But a fire, flood or storm can have very serious consequences. Even strikes or exceptional traffic conditions can hamper access to your IT systems.

Keep the chain intact

A professional IT security policy **does not end with the elimination of just one specific risk** or single point of failure (a link that compromises the whole chain when it breaks). In a digital world where data is king, it comes down to keeping **all of the links in the IT infrastructure intact** at all times.

Your employees constitute a major risk – often inadvertently.

Everyone is a **target**

Today, cybercrime has become one of the major risks for the continuity of both large and small companies. Here is a brief description of the main threats and terms:

ransomware: software whose only purpose is to take your business data hostage by locking it away unilaterally and then offering the key – the private key – for sale as a ransom to the rightful owner of the data.

phishing attack: a cyber-attack, often by e-mail, aimed at getting hold of the personal data of computer users. In doing so, cybercriminals pose as a reliable source, such as a bank.

ddos-attack (distributed denial or service): an attack on an IT infrastructure with the sole aim of overloading the system so that the usual data provided is no longer available (such as the sudden crash of an online system for selling tickets to an event).

social engineering: a technique used to try and get hold of the personal data of computer users through social contact by creating false confidence, or by posing as a person of trust.

zero-hour attack: an attack that uses recent malware or viruses against which antivirus software companies have not yet issued protection. Usually, minor adjustments are made to existing malware in order to circumvent scans.

advanced persistent threat: a targeted, long-term attack, usually by a group of cybercriminals, with the aim of obtaining as much data as possible and causing maximum damage within a single organisation or environment.

Cyber threats, such as ransomware, hold your business hostage. Today, everyone can be a target.

Essential measures

Your policy needs to have an answer for each and every one of the risks summarised above. But what is the best way to arm yourself against these threats in practical terms? Each company has different needs. The nature and risks of the company and the business-critical applications play a role here, as do the processes themselves and the importance of the data.
There are two common denominators that apply for all companies. The first is that they need to avoid problems by protecting their network, data and applications. The second is that they also need to take measures to get things back under control as quickly as possible when incidents occur so that they can restrict the damage and get the systems back up and running quickly and in full.

PREVENTING PROBLEMS

The old adage 'prevention is better than cure' certainly applies to IT problems that may disrupt your business continuity. You should not disregard these four rules of thumb:

1. **Have your IT managed proactively by experts**
   You can bring as much technology as you like in-house, but if you do not manage it professionally, it is just a waste of time. So make sure you have the required expertise in the first place. Proper security is a job for specialists. Setting up a network, then configuring and managing it, not only requires technical knowledge, but also round-the-clock attention and time.

   If that isn't the case, then you need to switch as quickly as possible (and permanently) from an IT management model involving break-fix and putting out fires. Prevent IT problems by monitoring proactively and automating maintenance tasks. That way you don't have to keep chasing your tail. And if you have the courage, admit that you do not have all of the expertise and tools you need in-house to protect and manage your IT professionally. The stakes are far too high.

Have your IT managed proactively by experts

2. **Shield your network. Set up a secure network.**
   That may sound like logic itself, but reality teaches us otherwise. Opt for a layered structure with segments and then monitor data traffic between each segment. Your sensitive data must not come into direct contact with the Internet.

- A firewall is the standard guard for your network. Ideally, you will have several firewalls, again in a layered structure. These scan all incoming data and block traffic and actions that are not permitted. Modern firewalls combine various functions into a

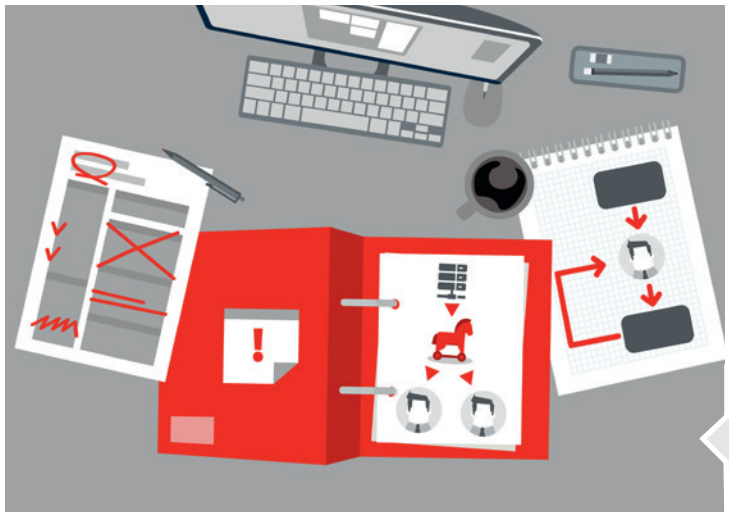
single device, such as an antivirus check or a traffic inspection system based on user identity and specific applications.

- Cybercriminals are increasingly using the backdoor to penetrate wireless networks. So make it a top priority to configure and protect your wireless networks, access points and other wireless systems appropriately.

- Don't give malware the chance to cause damage to your network. Use antivirus software, antispyware, centrally managed personal firewalls and intrusion prevention on your systems and the devices used by end-users. Even more important: keep this protection automated and up to date, and make sure you implement a strict policy.

- Use processes, software and encryption to monitor sensitive data and to avoid it leaking away or falling into the wrong hands. This applies particularly to data kept on mobile devices.

- Finally, control and manage digital and physical access to your network. Check which users have access to it and those who try to gain access. Use central user authentication and establish an active password policy. Additional measures using certificates, tokens or biometric scanning offer additional security.



- It also goes without saying that access to business premises, departments and physical areas (such as your datacentre or server room) must be strictly regulated and monitored.

Introduce proper procedures and apply them carefully.

3. Protect your applications

Define which items of software your employees are allowed to use on your network. Any other software that finds its way to your network must be checked to avoid unwanted applications being used without permission.

To stay ahead of misuse, you need to remain vigilant and keep your systems properly up to date. Carry out regular audits and analyses that will expose these weak spots. By using all available updates and patches – immediately and preferably automatically – you can avoid leaks occurring through applications and software, including self-written programs. Keep gathering information about new threats so that you can prepare to counter them.

Finally, keep user rights under control. Limit and monitor access to users who could make adjustments to systems.

4. Set up procedures and apply them

Your end-users are usually not aware of how important their role is in the security chain. So give them guidelines about the responsible use of e-mail, software and the Internet, as well as personal data versus business data. And check to see that they

are adhering to these guidelines. Simply providing one-off training or documentation is not enough. To give them regular reminders of the risks, you can use samples and practical tests.

It's best not to rely on the standard settings of your IT components. Use a consistent configuration process, focused on your organisation. Network components such as firewalls, routers and switches need to be set securely and uniformly, tailored for your needs. This also applies, of course, to your mobile devices, laptops, servers and PCs.

Carry out regular tests to check how effective your IT security is. Simulate a cyber-attack on your organisation, or a breakdown or hardware defect, or an intrusion or theft. Also take a look at how effective your existing processes and guidelines are. To catalogue any weak spots in your IT, conducting a security audit is a good start.

RESOLVE PROBLEMS QUICKLY

So, despite all of your preparations, have you still been the victim of an IT incident or downtime? If you have, you need to take immediate action to get your business back up and running quickly. You should set up a plan in advance, detailing who needs to do what, when and how. This should range from analysing and resolving incidents, to notifying users, the relevant authorities and your legal department. Managing your response to incidents is part of your business continuity plan. Here are some of the important parts of your approach:

1. **Keep your data secure at all times**
   In the first instance, you require a backup-and-restore plan so that you can keep your business data secure at all times. As part of the plan, you need to take account of the best location for your backups, management and monitoring, as well as the necessary technology. This type of plan is always geared to the needs of your business and contains all of the procedures and responsibilities.

   Backups in the cloud can provide an affordable solution, because you only pay for the storage space that you actually use with your cloud provider. So, no more investing in equipment and maintenance.

Use the cloud to keep your data safe and restore all of your systems quickly.

   Your backups must be rigorously managed. You certainly cannot run the risk that that your backups are incomplete or might fail. Backups need to be carried out automatically and checked regularly using restore tests. Best forget forever the tape stored in the cupboard in your office.

2. **Immediate restart**
   If your organisation has to get back to work quickly after an IT dropout, you need a disaster recovery plan, or DRP. Keeping your data safe is one thing. But if your systems are down, you can't use them. As with a backup-and-restore plan, two areas are essential in your DRP. On the one hand there is the time by which your data and systems have to be

available again after crashing (the recovery time objective, or RTO). Then there is the maximum quantity of data you can afford to lose (the recovery point objective, or RPO).

If a computer crash, even for a short time, is an absolute doomsday scenario for your business, then you need a fully duplicated IT environment. The problem is, not every company can afford the fallback of a second, redundant location.

Disaster Recovery as a Service (DRaaS) provides a cost-effective solution for this that goes further than just backup in the cloud. Not just your data, but also your entire IT environment, including physical or virtual servers, are available via the cloud for a fast restart when needed. You must also set out in the contract with your service-provider the period by which your business activities have to be back up and running after an IT incident.

3. **Respond in a controlled and resolute way**
   Operationally, you need to respond appropriately and in a controlled manner to incidents, based on your recovery plan. Your first priority, of course, is to bring the situation under control as quickly as possible. By checking the network traffic and logs carefully, analysing them and making connections, you will be able to highlight suspicious or criminal activity and respond to it accordingly. Documenting incidents accurately can also be decisive if there are any court proceedings.

   Your legal department won't be solving any IT problems as such, of course, but it can play an important role in dealing with them, such as obtaining compensation, deciding whether to file a report or adjusting your contracts. Should you have been without power for half an hour, for instance, or should you go to the police after an attack?

‘Always on’ starts with a professional approach

Downtime can weigh heavily for your organisation. You can estimate the effects in advance using the ‘risk times impact’ formula: how big is your security risk and how great would the impact be after an incident? But the question remains: how much risk are you prepared to run?

If you are a company that aims to be ‘always on’, a professional and proactive approach is required. **That doesn’t just mean using the right technology, but also especially having that technology managed round the clock and proactively by experts.**

As a result, more and more organisations are working with Internet applications and storing their data and systems off-site, because they realise that cloud computing can enhance their IT security significantly. Reliable local cloud partners offer watertight contracts and invest constantly in the latest security technology. These are investments that companies do not want to – or are unable to – make themselves.

Keeping your IT available and secure is a complex matter and it’s easy to lose control. This guide contains the answers to a number of basic questions. As a next step, you can have a risk analysis or IT audit carried out. The results will give you a firm base for optimising your existing policy or, if necessary, to thoroughly review it.

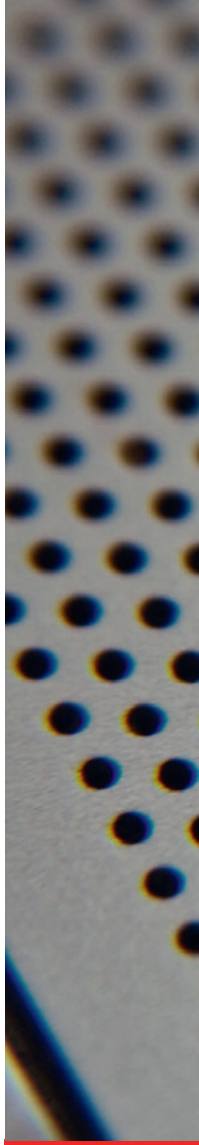
Checklist: have I got everything under control?

Have you had a good look at your IT security policy recently? Use the checklist below to form an idea of how things stand right now and the need for any improvement.

- How current is your plan for protecting your business data?
- What guarantees do you have after a crash that your IT will be ready to operate again quickly? And how long will it take?
- When was the last time you tested the scenario?
- Are you sure about the quality and consistency of your backups?
- Have you examined the weak links in your IT security?
- Do you manage your IT security constantly and do you have the right people and tools to do so?
- Does your security policy take mobile devices into account (including the personal devices of employees and visitors)?
- Do you have a plan if you are the victim of cybercrime? And what happens if you have a power outage?
- When was the last time anyone went on an IT security training course?
- How many people know your total IT infrastructure and are able to manage it?
- Does your security meet your needs and comply with the regulations – and can you demonstrate it through an audit by an independent party?

ANY QUESTIONS ABOUT HOW TO INCREASE YOUR BUSINESS CONTINUITY?

You can contact us via **cheops@cheops.be** to discuss which approach best suits your organisation. We will help you to implement IT as a strategic tool that will make a measurable contribution to your company objectives. With our range of *managed* and *cloud services*, as well as an experienced team of IT experts and unique tools, we deliver more business continuity, profitability and productivity for our customers.



cheops

Prins Boudewijnlaan 49
B-2650 Edegem
Belgium

T +32 3 880 23 00
E cheops@cheops.be
www.cheops.be