cegeka

Reduce cybersecurity risks

Detect and response best practices

On average, it takes 280 days to bring a data breach under control. Some companies are not even aware that cybercriminals have broken into their systems.

How can you cut down this number? And how do you minimize the operational and financial impact of a cyberattack and threats like ransomware?

This e-book provides you with some guidelines for reducing your cybersecurity risks and a roadmap for building a cybersecurity toolkit in a cost-effective way.

Today, every single one of us could be a potential target for cybercriminals. But the tools required to protect us are also available to us all.

Table of contents

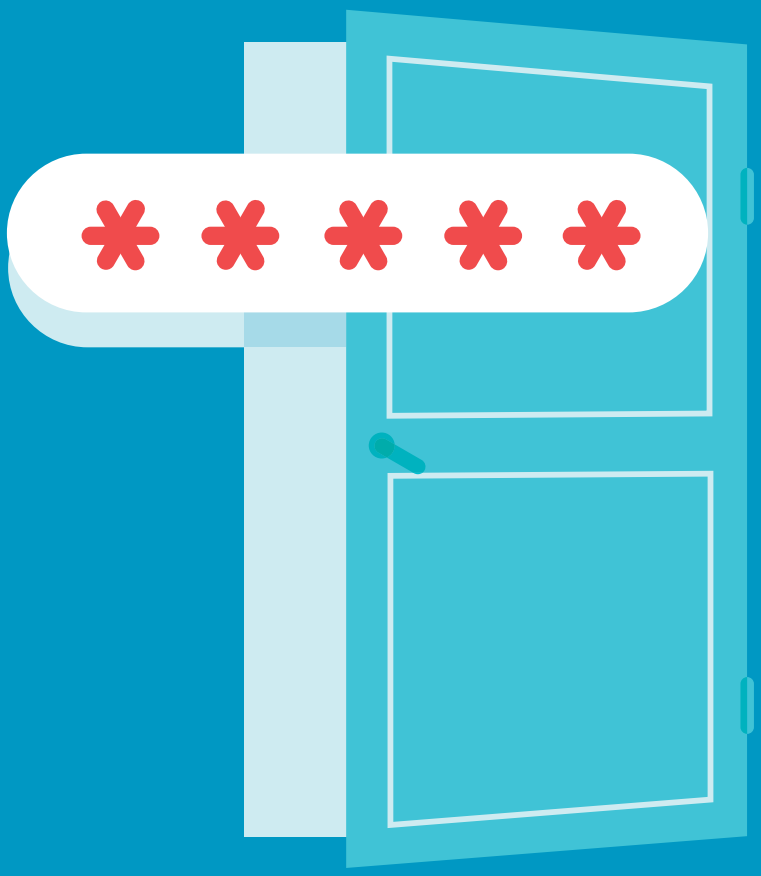
1. Protect yourself against cybercriminals – a step-by-step roadmap to cyber-resilience
   p. 04
   -

2. Eliminate cybersecurity threats – build your cost-effective security toolkit
   p. 06
   -

3. IT security that grows with you – start with the basics, add as you grow
   p. 09
   -

4. Managed Detection & Response: becoming cyber-resilient in a cost-effective way
   p. 11
   -

5. Conclusion
   p. 14
   -



1

Start by adopting the right cybersecurity approach

Reducing cybersecurity risks in five steps

In its Cybersecurity Framework, the American National Institute of Standards and Technology (NIST) provides **guidelines and best practice** for organizations to help curb their cybersecurity risks. Cegeka's cybersecurity approach is based on this framework. We have broken down the actions you can take as an organization into five phases:

- **Assess:** Create an inventory of your important assets, reassess the business context and gain insight into your risks.
- **Prevent:** Protect your assets with the necessary procedures and tools.
- **Detect:** Detect security incidents as soon as possible.
- **Respond:** Respond as soon as you have detected an intrusion to minimize its impact.
- **Recover:** Streamline and accelerate recovery from a security incident with the appropriate recovery procedures.

Unfortunately, many companies focus mainly on the second phase of the security framework: **prevent**. They simply install security software to protect their data and IT systems. But this is not enough: the other four phases are just as important.

NIST Cybersecurity Framework

Read more about
the NIST Cybersecurity Framework at
www.nist.gov/cyberframework

2

Insight first, protection second

Know what you need to protect

You may be tempted to jump straight to the second phase of your cybersecurity approach, to prevent. But in order to protect your IT systems in the most cost-effective way, it is important that you first identify which assets you need to protect and exactly what the risks are. All your security efforts should start with an **assessment**.

In other words, what are your company's **key assets**? Is there data you cannot afford to lose under any circumstances? And do you have data that you definitely do not want to see sold, either publicly or on the dark web?

What are your company's key assets?

Make a list of all the important data your company holds that you definitely need to protect. Here are a few examples:

- Personnel list
- Pay slips
- Customer list
- Customer details
- Bank account numbers
- Passwords
- Quotes

Imagine what the impact of loss or disclosure of this data would be on your business.

Know your enemy

To assess the risks correctly, it is important to know your enemy: the cybercriminals who are targeting your data or infrastructure. Today, one of the most frequently used weapons is **ransomware**.

Cybercriminals use ransomware to encrypt your data, rendering it inaccessible and effectively bringing your whole business to a standstill. This can cause a huge loss of revenue. The cybercriminals then demand a **ransom to make your data accessible again**.

Extortion

Even if you have backed up your data and are able to restore it and rebuild your entire IT infrastructure so that cybercriminals can no longer get in, you will never be safe again.

Because if cybercriminals have hacked into your systems, they have also stolen your data. They could use this to extort money from you by threatening to publish the data, which could seriously damage your business. To prove that they have access to your data, they may show you some of it, or perhaps leak a portion of it to the public.

Three fundamental risks to your business

There are three essential types of risk you want to protect your business from:

Operational risk

If your IT systems are down, your company can no longer process orders, deliver products or services or send out invoice reminders. This will make you lose business.

Financial risk

The financial impact of these attacks is not just limited to loss of revenue. You would be expected to pay the cybercriminals a ransom to prevent them from making your data public. Repairing your IT systems would also come at a cost, as would trying to restore your day-to-day operations and catching up on workloads. Customers and suppliers may sue you or claim compensation if their sensitive information is leaked, and you may also be fined. There may be legal fees to pay on top of all this. And what happens if your quotes or confidential R&D documents are published and your competitors can see them?

Reputational risk

Do not underestimate the damage to your reputation if your company is targeted by cybercriminals. Will your customers still buy products or services from you if you have been hacked? You can be sure that, if their own data has been made public, they will think twice about buying from you. If your customers lose confidence in you, they will take their business elsewhere, and regaining their trust or attracting new customers will require a lot of time and money.

Cost-benefit analysis

Let's do the math: if you are suddenly faced with all three of these fundamental risks – operational, financial and reputational – how would this scenario affect your business, both immediately and in the long term? How much would it cost to become operational again? And then, in comparison, how much would it cost to protect your business from those risks in the first place?

3

Detect and respond

Alarm system

After prevention comes **detection**. If, in the event, your protective measures did not work, would you actually know if there had been an intrusion?

Compare this to an alarm system for physical break-ins. Without an alarm system, you have no way of knowing when burglars are trying to steal your stuff, unless they are breaking down your door. And by then, it is too late.

Most companies have a physical alarm system up and running on their premises. So why not an IT alarm? After all, your IT systems are the heart of your business, even if you are not an IT company.

Don't wait for a break-in before installing an alarm system

Many people – and even businesses – only install an alarm system after there has been a break-in in their neighbourhood. This tends to happen in the digital world, too: people often think that they will not be targeted by a cyberattack. But **everyone is a potential target** for cybercriminals, both large and small businesses. So don't wait until you become a victim of ransomware – be prepared.

Respond

Firstly, there is no point in installing an alarm system with cameras on your premises if nobody is actually watching the footage.

In the same way, a cyber incident detection system is useless if there is no system in place to respond to it. Because after detection, you need to **respond**. It is vitally important to set up a security operations centre – an SOC. The analysts in your "control room" should monitor your IT operations alarm system around the clock and must be able to react immediately to any potential breaches.

Our security analysts have experience with all kinds of incidents, so they are perfectly equipped to help you decide what action to take in the event of a breach.

A well-equipped SOC should also be underpinned by a system that responds automatically to detected threats.

280

days of insecurity

On average, it takes 280 days to get a data breach back under control[1]. That is 207 days to detect the intrusion, and another 73 to resolve it. With a detection system in place, you can reduce this number of days and thus the impact on your business.

1. Source: 2020 Cost of a Data Breach Report by the Ponemon Institute and IBM Security

4

Managed Detection & Response: your flexible security toolbox

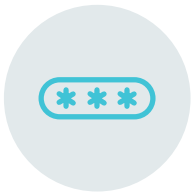
Managed Detection & Response

In the world of IT, your alarm system is called MDR: Managed Detection & Response. It is the digital equivalent of a physical emergency operations control room and the service it provides is made up of the following components:

- The analysts at the **Security Operations Centre (SOC)** monitor your organization for possible cybersecurity breaches.
- A **Security Information & Event Management (SIEM)** system collects logs from a variety of sources and provides real-time analysis and notification of suspicious events.
- The **Network Detection & Response (NDR)** element analyses network traffic, determines the risk level, detects anomalies and, through integration with other systems, can launch a partially automatic response. Our SOC analysts will evaluate the reports from the NDR and react accordingly, where necessary.
- **Endpoint Detection & Response (EDR)** monitors the use of endpoints, i.e. computers or mobile devices and detects abnormal behaviour. It can also launch a partially automatic response. To put EDR into effect, you need to install endpoint protection (EPP) on the endpoint devices. This allows the SOC analysts to connect directly to these devices and to retrieve information and intervene if required.

The automatic responses and reactions of the SOC analysts **minimize any damage caused by an intrusion**. Everyone benefits from an MDR.

Tailor-made alarm system



MDR systems exist in many different shapes and sizes, from simple to complex. To ensure your MDR deployment is **cost-effective**, it is important to choose a system that is tailored to your business.

The most important factor here is that you pay sufficient attention to the “assessment” phase when planning your cybersecurity.

If you let your SIEM collect all your logs in bulk, you will be flooded with notifications – and that means you will not notice the important ones.

However, if you know what the main assets of your business are that you want to protect, you can focus on that data and those particular systems. This allows you to:

- Limit the logs collected by the SIEM to only the **important systems**
- Install EPP on business-critical **endpoints**
- Examine the **network traffic to and from critical servers** and industrial systems where endpoint protection may not be possible with NDR.

This way the SOC can focus on the threats that are relevant to your business.

Start with EDR

If you do not yet have a SIEM, EDR is the first step to protecting your organization from cybercriminals. This technology is the most cost-effective and it also allows you to respond quickly to threats from the outset.

If you already have an SIEM, the next most cost-effective step is to supplement it with EDR. This increases threat visibility and addresses the growing threat of endpoint system breaches. It also allows you to respond more quickly to threats, reducing the operational impact.

Start with the basics add as you grow

With MDR, you can start with the basics and gradually expand your toolbox as you gain experience and develop your security strategy. Depending on where you are starting from, there are two possible paths to take:

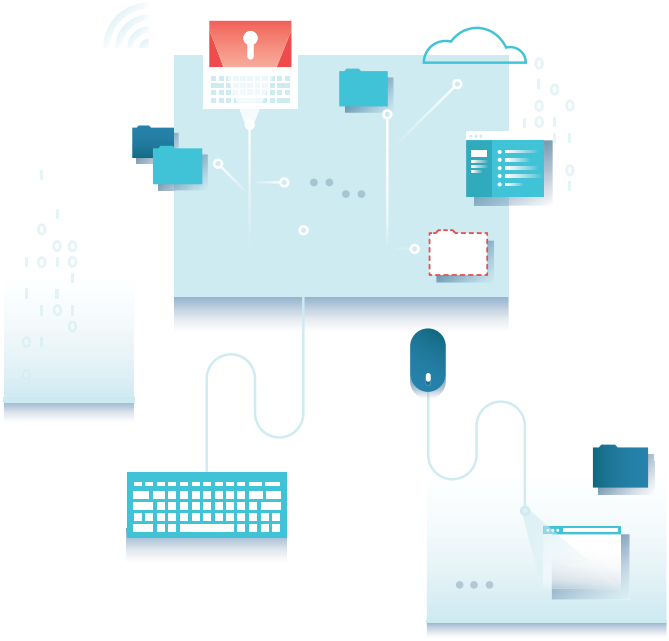
- **You can start with an SOC and SIEM:** firstly, you supplement this with EDR on the endpoints and afterwards you can extend it with NDR for the network traffic.
- **You can start with an SOC and EDR:** this way you expand visibility with SIEM and then add the network perspective with NDR.

NDR offers greater visibility into any threats that exist on your network. It is a powerful addition to your MDR.

Managed EDR

By outsourcing your EDR to experts, you will save money and benefit from the scale and expertise of the provider.

Even if you already have an endpoint security system up and running, it is still worth looking into managed EDR solutions. It can often be cheaper to exchange your own EPP for managed EDR, which will include EPP endpoint security. Reallocating your budget this way would allow you to free up resources that could be reinvested in your security strategy.



5

Conclusion

Conclusion

The roadmap to reduce your cybersecurity risks starts with identifying your organization's key assets and defining the risks posed by cybercriminals. You can then do a cost-benefit analysis to protect your business from those risks.

Because protective measures alone are not enough, you also need to know when an intrusion occurs and be able to react accordingly. Remember, on average, it takes 280 days to bring a data breach under control. If you can reduce this time, you can minimize the operational and financial impact.

This is possible with Managed Detection & Response (MDR). Once you have taken the time to identify your company's key assets, MDR can then help you to focus on the greatest threats to your business, in a quick and cost-effective manner. Start with the basics and gradually expand your security toolbox as you develop and refine your security approach.

The result? You will be able to eliminate cybersecurity threats as quickly as possible and will greatly limit the financial and operational impact on your organization.

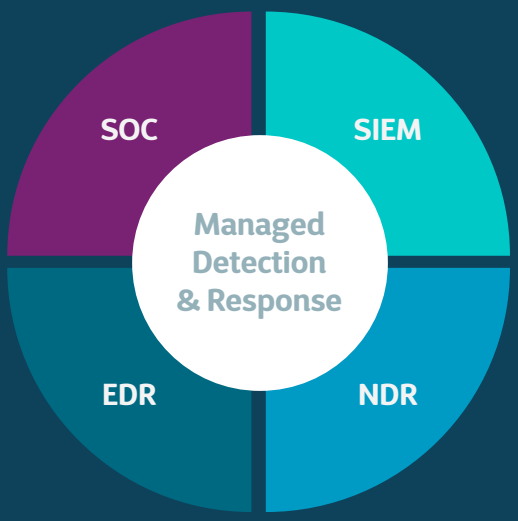
Managed Detection & Response by Cegeka

Cegeka offers a modular MDR portfolio, with a combination tailored to every need, every organization and every budget.

With the advanced Threat & Brand Intelligence provided by Cegeka MDR, you will gain access to an important source of information that will help you quickly and accurately track down security threats in your environment.

Cegeka's modular approach also means that you can take advantage of a future-oriented service can grow with your budget and stay in line with the implementation of your security plan.

Thanks to the as-a-service approach, you only pay for what you actually use and keep the costs under control.



WWW.CEGEKA.COM