NORTHWAVE
Intelligent Security Operations

NORTHWAVE
YOUR DIGITAL DEFENCE

INTRODUCTION

The playing field in the world of cybersecurity is an uneven one. Attacking is easier than defending: the attacker only has to exploit a single mistake to gain access to your environment while, as a defender, you have to be vigilant about everything all at once.

Yet the situation is not hopeless. The majority of attackers only know a limited number of tricks. Just like a burglar who walks the streets to see which houses are interesting and accessible, the average cybercriminal scans the net for interesting organisations that are not resistant to his standard attack technique. You can protect yourself against such attackers.

Some attackers are more targeted in their approach and use a wider range of techniques. They make a greater effort in exchange for a higher yield. But as we have seen in 'Your most important digital threats', standard patterns are also used in these attacks. And again, you can protect yourself against them.

Such protection does not consist of a single measure. It is an interplay of several actions and measures where each:

- reduces the **likelihood** of a successful attack; or
- reduces the **impact** of a successful attack.

The likelihood and impact do not have to be reduced to zero. You may, for example, choose to accept certain risks because it would otherwise be too expensive to defend against them.

BOTTOM-UP AND TOP-DOWN

This document takes you through two approaches for getting and keeping your protection up to scratch.

The bottom-up approach starts in daily practice by fixing what needs fixing. Bottom-up quickly delivers better protection.	The top-down approach starts with the big picture and proceeds on the basis of risk management and a theoretical framework. Top-down gives you a handle on the situation and long-term protection.

There is no need to choose one approach over the other, as both are necessary and can be started up in parallel perfectly well. The bottom-up measures are a subset of the top-down approach.

In the bottom-up section, we describe a set of relatively 'simple' measures that we think everyone should take. Practice shows that more than 80% of successful attacks could have been repelled with the aid of these measures.

In the top-down section, we describe how you can get and remain 'in control'. Not through a patchwork of measures, but through a set of structured, coordinated measures that suit your company's risk profile and risk appetite at any given time.

BOTTOM-UP

In the bottom-up approach, you work directly and pragmatically with relatively easy-to-implement measures. Below, you will find eight examples of the kinds of measures that fit in well with the attacks profiled in the Northwave document 'Your most important digital threats'.

BOTTOM-UP MEASURES

STRONG AUTHENTICATION

Use passphrases and turn on MFA. MFA stands for multifactor authentication—signing in with more than just a password. In many of today's systems, a second factor, such as a token, is easy to turn on. Is MFA turned on for all users? Have your employees been educated about secure passwords?

UPDATE

Installing updates ensures that attackers can no longer exploit known vulnerabilities in the old version of your software. When was the last time you checked all your systems and installed updates everywhere? Do you have a process for this?

BACKUP

A good backup system, including at least one offline copy in a separate location, increases resilience against data loss. Have you tested your backup system by restoring from the backup at least once? Does that fully work?

INCIDENT RESPONSE PLAN

An incident response plan provides guidance the moment an attack is discovered. The first version needn't be more than one A4 page with instructions and a dedicated hotline. Do you have a manual of what to do in the event of an incident? Do your employees know where it is?

PAYMENT PROCEDURE

These include simple rules, such as if a creditor sends an invoice with a new account number, perform a telephone check. These kinds of rules increase your resilience against BEC fraud. Do you carry out an additional check when payment information changes?

ENDPOINT PROTECTION

Antivirus software stops known malware and thus reduces the chance of a successful attack. Does every system—both servers and clients—have antivirus software running?

EMAIL SECURITY

Use security tools to block phishing and malicious attachments as much as possible. In addition, check your email security to make it more difficult for attackers to send emails on behalf of your organisation. Are SPF, DKIM and DMARC properly configured?

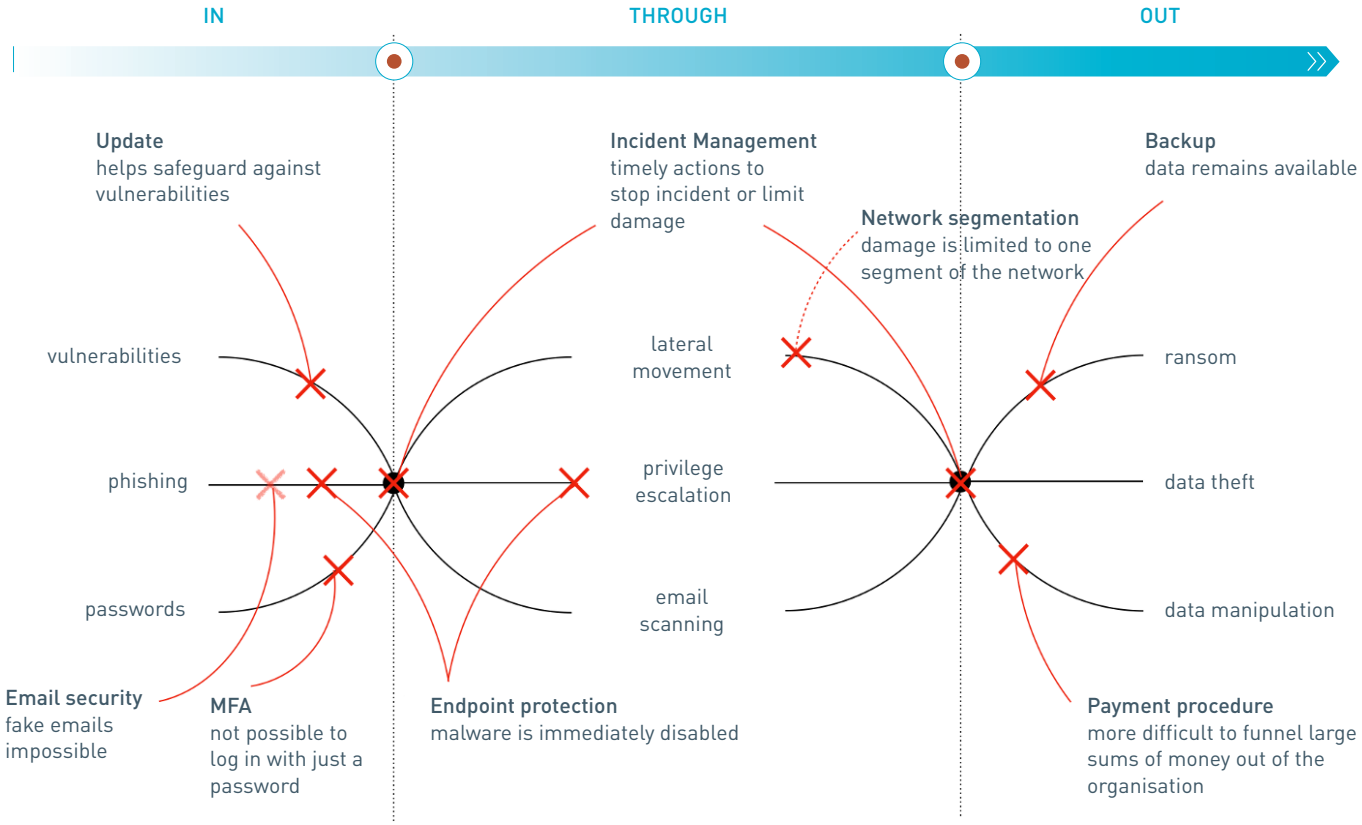
NETWORK SEGMENTATION

Separate parts of the network that do not need to be connected. Doing so makes it more difficult for attackers to attack the entire environment once they have entered it. Is your network divided into segments? For example, do you have a separate network for system administration work?

However, do not start implementing these measures blindly. It pays to first examine what your risks are and which risks you want to accept or mitigate. After that, draw up a plan, and only then get started. In short, you do this to ensure your bottom-up approach dovetails with your top-down approach.

IN, THROUGH AND OUT

We have worked out three examples of successful cyberattacks in the Northwave document 'Your most important digital threats'. The above measures offer protection at various places in that chain of IN, THROUGH and OUT by making the attack impossible, stopping it or limiting the damage done. The diagram below shows where the measures interrupt the attack chain. None of the measures offer complete protection, but taken together, they significantly increase your security level.



BOTTOM-UP IS NOT ENOUGH

These simple measures are a good starting point, and we think everyone should take them. Unfortunately, however, they are not enough:

You also need to take specific measures in addition to these generic ones. Your organisation is **unique**. Therefore, your risks are unique, and require specific measures.

Simple measures are insufficient. You also need to take some **more complicated** measures to reduce your risk.

Attack techniques change over time, so the protection offered by these measures decreases over **time**. You have to keep fine-tuning your measures in a cyclical process.

You have not got a **handle** on your risks. You do not know whether you have taken the most appropriate measures and to what extent you have covered which risks. You have no system for maintaining the measures.

TOP-DOWN

The bottom-up measures cover quite a significant part of your cyber risk. How much exactly? Have you not measured it? Then you have no idea. Nor do you know whether you have correctly implemented the measures according to your business risk profile or which measures are still missing. A top-down approach provides these insights so that you can get a handle on your information security risks.

If you want to take a systematic approach to your security, it is good to start with the following questions:

1. **Who am I?** (We call this the context definition: What does my organisation look like? What are my businesses goals, processes, systems, data, stakeholders, etc.?)
2. **Where do I stand?** (What are my core assets, my vulnerabilities, the threats and thus my risks?)
3. **What do I want?** (What risks am I willing to accept, and what risks am I not?)

With the answers to these questions in hand, you can set up a process to take measures[1] which are:

- done in a continuous cycle;
- risk-based;
- generic and specific;
- existing and new; and
- appropriate to the organisation.

In that cycle, you will naturally want to check and monitor continuously in order to improve your measures where necessary and manage your risks. You now have a *Plan-Do-Check-Act cycle*[2] to raise your security to the right level.

This is what is called security management, and it must be embedded in the existing organisation and fully committed to by management. A Security & Privacy office that is in control at all times and supported by standards such as ISO 27001.

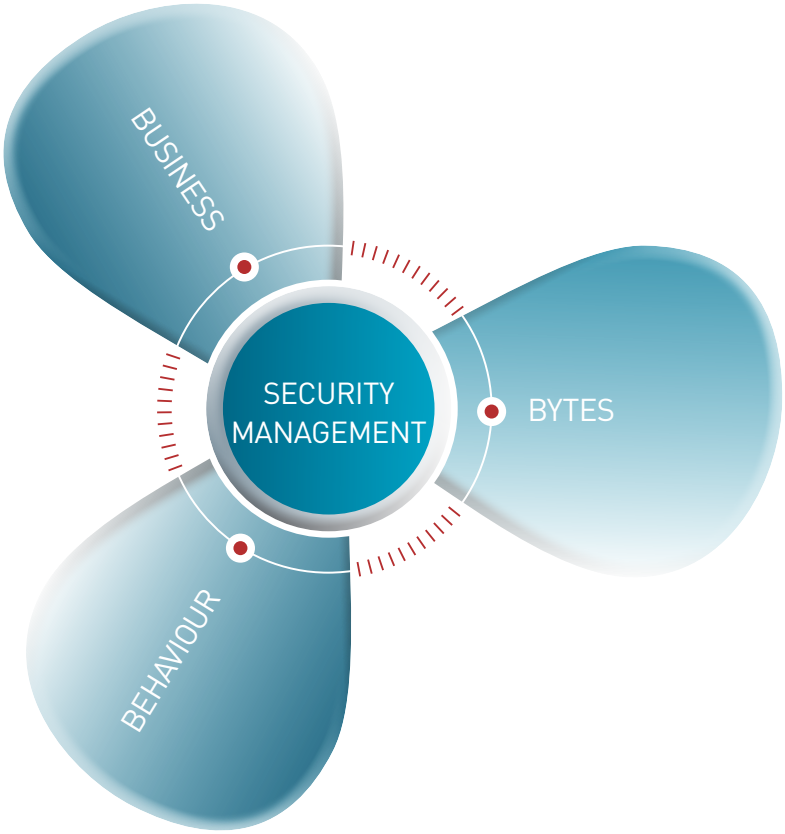
SHIP'S PROPELLER

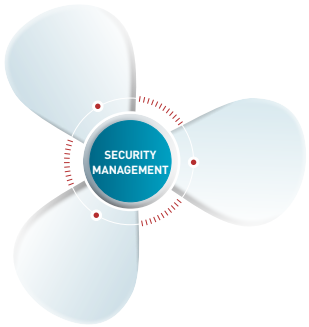
At Northwave, we use a ship's propeller to model the continuous movement of your cybersecurity: the Plan-Do-Check-Act cycle that keeps repeating itself and driving your security forward.

The shaft of the ship's propeller is your security management. This lynchpin connects the blades of the propeller—the three domains that are important when it comes to ensuring your cybersecurity. These are processes, technology and people. At Northwave, we call these **Business**, **Bytes** and **Behaviour**. They form the deliverables of your cybersecurity approach.

We have just looked at the axis of the propeller. In the rest of this section, we will provide you with a high-level overview of the propeller's blades, which will give you enough insight into the key points of security management to get started.

1. These measures can be divided into three categories. We will come back to this later.
2. See https://en.wikipedia.org/wiki/Quality_circle for an introduction and reference to relevant articles.





SECURITY MANAGEMENT

WHAT IS IT?

A continuous process in which changes in insights, your business and threats impact your business risks and security measures. Security management provides a well-informed answer to the questions of what to do, what not to do, and why.

WHY? HOW WILL IT BENEFIT ME?

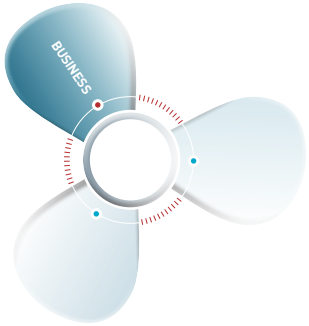
It allows you to take well-informed measures which fit your business risk profile and objectives. You get and maintain a handle on your information security. Through a cyclical process, you raise your security standard to an appropriate level for your organisation. You only invest in measures that are actually necessary and effective at a given time.

WHAT DO I NEED TO DO?

1. You start the cycle by getting clear on the following: What do I have, who am I, and what do I want? This is your foundation.
2. You carry out a continuous Plan-Do-Check-Act cycle.
3. This requires continuous actions, measurements (checks, audits), reports and adjustments.
4. You embed security management in the existing organisation.

BUSINESS, BYTES AND BEHAVIOUR

Together, the three blades of the ship's propeller form what we call your Intelligent Security Operations. They cannot be taken separately; on the contrary, they reinforce each other.
The blades are connected by the propeller's axis: security management. Each blade is a cybersecurity domain. Cybersecurity can only be achieved when all three domains have been implemented and function as a whole.



BUSINESS

WHAT IS IT?

The BUSINESS side of cybersecurity is concerned with **Plans, Policies and Procedures:** clear and functional (visible) products which are implemented and maintained. (The decisions fall under Security Management, the measures under BUSINESS)

WHY? HOW WILL IT BENEFIT ME?

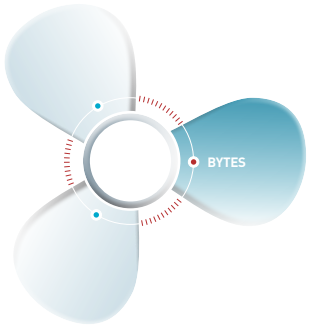
Your information security fits seamlessly into the organisation's vision, strategy and plans. You have thought about **what** you want to do and **why**. You have:

- the right information security guidelines to support your business;
- a blueprint of requirements for all aspects of information security that suit the business; and
- standards and guidelines that define a safe way of working.

WHAT DO I NEED TO DO?

You translate your vision, strategy, risk appetite and business plans into an information security policy.

1. **Plans:** a security roadmap that is up-to-date at all times.
2. **Policies:** the policies that make your plans possible. Here, you should consider things such as clear roles and responsibilities or the use of personal devices, for example.
3. **Procedures:** the interpretation of these choices, such as having a defined process for handling incidents.



BYTES

WHAT IS IT?

BYTES increases your organisation's resilience by linking technology and expertise. Technology encompasses both IT solutions and threat information (intel). Using the right tools in the right way and interpreting the results correctly requires specialist expertise.

WHY? HOW WILL IT BENEFIT ME?

You have the appropriate technologies to manage your risk. In other words, you can:

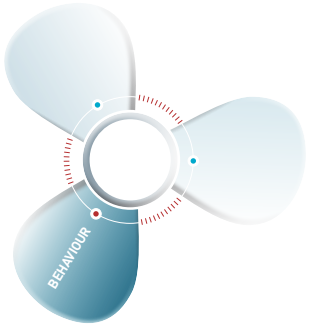
- **Prevent:** The vast majority of attacks will not affect you;
- **Detect:** Attacks that do reach you are detected at an early stage; and
- **Respond:** Security incidents are handled effectively and efficiently.

This three-way split is not limited to BYTES but also takes place in the other two blades.

WHAT DO I NEED TO DO?

Many measures from the bottom-up category fall under the 'Prevent' heading. This heading often gets the most attention, but to move forward, you must be able to take the following actions:

1. **Monitor:** Your environment must be monitored 24/7 based on your risk analysis and the current attack landscape. This is done by a SOC (Security Operations Centre). The SOC also takes immediate action when abnormalities are detected.
2. **Practice:** You do not want to wait for a real attack to test your security. A Red Team assessment will provide you with insight into points of attention so you can further secure your environment.
3. **Respond:** You want to be able to act when things really threaten to go wrong. A CERT (Computer Emergency Response Team) has the knowledge and resources to deal with security incidents. In addition, CERTs worldwide are in touch with each other and immediately share new threats.



BEHAVIOUR

WHAT IS IT?

BEHAVIOUR focuses on the human side of cybersecurity: the behaviour of your employees and the culture within your organisation. This is because security is ultimately about people. You want to achieve a cyber-safe culture within your organisation, one in which employees sound the alarm early on without fear of being called out for it.

WHY? HOW WILL IT BENEFIT ME?

Your employees and organisational culture actively contribute to increased cyber resilience.

- The importance and value of your employees for your security are clear.
- The security risks resulting from employee behaviour are reduced.
- Your employees form an effective additional layer of defence against cyberattacks.

WHAT DO I NEED TO DO?

BEHAVIOUR does not stop with a one-time awareness training but is a continuous process of behavioural and cultural improvement in which you optimally equip your employees to take active responsibility. This translates to:

1. **Awareness and understanding**—Your employees know what behaviour is expected of them and understand what that means.
2. **Ability and willingness**—Your employees are able and motivated to demonstrate the desired behaviour.
3. **Do and keep doing**—Your employees carry out the desired behaviour; cyber-safe behaviour has become part of the organisational culture.

SPECIALISTS

Many top-down category measures require the use of specialists. Not all organisations have these individuals in house—nor do they need to. A number of security companies, including Northwave, of course, offer support in this area. And more than that. Northwave has been brought in in response to many attacks, and we monitor and prevent attacks on our clients. The attack information we extract from our activities is directly used to improve the protection of all our clients.

Specialists are there to assist you, but you should bear in mind that cybersecurity is ultimately always customised and must be tailored to your specific situation, so you will remain actively involved no matter what.

EXAMPLES

Attackers can and will act in different ways. If one method of attack does not work, they will often switch to another. If that does not work either, the average attacker will turn their attention to another victim. You can thwart the attacker in the IN, THROUGH and OUT phases of their attack.

EXAMPLE 1

Attacker Ivan has obtained login credentials from your organisation. He logs into your network using the correct credentials of one of your employees, Maria.

- You have set up MFA (multifactor authentication), and a token is sent to Maria's phone.
- Maria has been trained, so she does not authorise the login and reports the attack to the hotline.

× **Attack stopped.**

Ivan does not give up. He tries to login simultaneously on a number of employee accounts and uses social engineering to trick them into accepting the login.

- Your organisation monitors login attempts. Ivan logs in from an unknown IP address in Russia—in your model, this triggers a red flag.
- Your employees are trained and report the attack en masse to the hotline.
- You have an up-to-date procedure for this kind of attack. It now comes into effect.

× **You have more time to respond and do so quickly and appropriately. Attack repelled.**

EXAMPLE 2

Attacker Eva has successfully logged into Henk's account; Henk is the head of the finance department. Eva attempts to further penetrate the network using privilege escalation and lateral movement. To do this, she tries to install malware.

- Your endpoint protection recognises Eva's malware and disables it.

× **Attack stopped.**

Eva tries to use Henk's account to obtain as much system access and data as possible.

- Your Identity & Access management guarantees that Henk cannot access data and systems that he does not need for his work, so Eva cannot either.

× **Attack repelled.**

Eva uses new, as-yet-unknown malware and gains sufficient rights to disable endpoint protection. She starts looking for other systems in the network.

- You have segmented your network. Large areas, including your production facility, are simply inaccessible.
- Your detection system flags Eva's attempts as suspicious.
- Your protocol for intrusion comes into effect.

× **The attack has been delayed, made more difficult and detected in time and can now be repelled.**

EXAMPLE 3

Attacker Boris has successfully hacked one of your organisation's suppliers. From the supplier's email environment, he sends a fake invoice with a different bank account number.

- Your payment procedure indicates that an external check must be performed in the event of changes.
- Henk from Finance understands the risks, knows the procedure and calls your supplier.
- Your CERT monitors the outside world and recently issued a warning that this kind of attack is becoming popular. Your financial employees are therefore paying extra attention.

× **The payment is not made, and the supplier is warned.**

× **Your email security ensures that such an attack can never originate from your organisation.**

IN CONCLUSION

A JOURNEY

Cybersecurity is a journey, not a destination. Any organisation, even the best-secured ones, can be hit by a cyberattack. But you can considerably reduce the chance of a successful attack by refining your security in a continuous process with the help of Business, Bytes and Behaviour. And if an attack does take place, you will notice that your company is much more resilient. The time between attack and discovery is shorter, the procedures to deal with the attack have already been worked out and the right people can be called in immediately.

Complete security is an illusion, but with Security Management, Business, Bytes and Behaviour, you can get close enough. And stay there.

Every organisation is unique. Therefore, beyond simple, generic measures, cybersecurity always involves a tailor-made approach. Northwave can support you with many generic and specific measures.

But no matter what, you will still have to act on it yourself.