



# Never Waste a Good Crisis: The Six Success Factors of Cyber Resilience

Date: **September 23, 2024**

Author: **Pascal Renckens, Luca Ferentinos, Alex Wielart**

# Table of contents



<b>Executive summary</b>	<b>1</b>
<b>1. Introduction</b>	<b>2</b>
<b>2. What is cyber resilience?</b>	<b>4</b>
<b>3. What threats do you face?</b>	<b>6</b>
3.1 Ransomware	6
3.2 Business email compromise (BEC)	6
3.3 Insider threat	7
3.4 Supply chain compromise	7
<b>4. The six success factors of cyber resilience</b>	<b>8</b>
4.1 Leadership and clear governance	8
4.1.1 Crisis leaders	8
4.1.2 Governance structure	9
4.2 Effective cyber crisis communication	9
4.2.1 Not communicating is (almost) impossible	9
4.2.2 Crisis communication is an integral part of crisis management	9
4.3 Strong relationships and partnerships	10
4.3.1 IT suppliers	10
4.3.2 Customers and stakeholders	11
4.4 Mental strength within crisis teams	11
4.4.1 Coping with stress: planning and task division	11
4.4.2 Coping with stress: pay attention to mental health	12
4.4.3 Training behaviour	13
4.5 Continuous learning and improvement	14
4.5.1 Maturity scan	14
4.5.2 Implemented plans	14
4.5.3 Cyber resilience trainings and regular exercises	14
4.6 Adaptability	15
4.6.1 Adaptability in your basic insights and setup for resilience	15
4.6.2 Adaptability during a crisis	16
<b>5. Conclusion</b>	<b>17</b>

# Executive summary

Cyber resilience is no longer an option but a necessity. Organisations must fortify their defences to withstand and recover from cyber threats. In this context, our unique insights and industry best practices unveil six critical success factors for cyber-resilient organisations, intricately aligned with the evolving cyber-threat landscape.

To begin with, we needed to analyse the definition of resilience. Northwave, originally founded in the Netherlands, draws upon the Dutch language's dual concept of resilience, encompassing *weerbaarheid* and *veerkracht*. *Weerbaarheid* focuses on the ability to withstand challenges and difficulties, which we at Northwave strive towards for and with our clients, based on an integrated approach consisting of three domains: business, bytes, and behaviour. *Veerkracht* focuses on the ability to endure and overcome difficult situations, which is the primary focus of this white paper. In essence, cyber resilience is an organisation's ability to face and cope with adversity, adapt to change, recover, learn, and grow from cybersecurity incidents and crises.

We advocate the use of NIST CSF 2.0 to enable organisations in monitoring and managing the end-to-end incident cycle, from governance to recovery. Each of the six core functions—Govern, Identify, Protect, Detect, Respond, and Recover—is integral to understanding and acting within the incident lifecycle. Yet, as highlighted in our definition of cyber resilience (*veerkracht*), our focus is on Respond and Recover. The NIST 2.0 framework can be understood as a reader's guide for realising our goal of cyber resilience.

Based on our unique observations and industry best practices, we have established six success factors for cyber-resilient organisations:

1. **Leadership and governance:** Effective leadership and a clear governance structure are vital during crises. Experienced leaders can quickly respond, and a well-established governance framework allows for efficient delegation and crisis management.
2. **Cyber crisis communication:** Proactive and transparent communication during cyber crises is essential. Organisations should promptly share bad news to maintain trust, manage expectations, and


reduce the risk of misinformation. Collaboration with crisis management teams is crucial to tailoring communication to stakeholders' specific needs.

3. **Building trustworthy relationships:** Cultivating trustworthy relationships with IT suppliers, customers, and stakeholders is a long-term effort. These relationships not only help organisations weather crises but also enhance adaptability in a constantly changing landscape.
4. **Mental well-being:** Acknowledging and addressing stress, anxiety, and hopelessness in the crisis team is crucial. Prioritising mental well-being equips teams with effective coping mechanisms. Behavioural training and attention to mental health ultimately speed up recovery and prevent prolonged negative impacts.
5. **Continuous learning and improvement:** Creating a culture of continuous learning and improvement involves assessing the organisation's maturity level and implementing plans for regular training and exercises. This approach enhances employee knowledge and tests their capabilities, strengthening the organisation's cyber resilience.
6. **Adaptability:** Recognising and effectively responding to changing circumstances and unforeseen challenges, even if it means deviating from existing plans, is essential for survival. Embracing adaptability is not only a valuable trait but a necessity in today's dynamic environment.

Taking these factors into consideration will enhance your organisation's resilience capability and crisis management capabilities, ultimately better positioning you to navigate the intricate landscape of cyber threats and challenges.



# 1. Introduction



In today's digital landscape, it is necessary for organisations and businesses to enhance their cyber resilience. The value of cyber resilience lies in the ability to withstand and recover from sophisticated cyber threats. A cyber-resilient organisation can safeguard its critical assets and sensitive data while also ensuring uninterrupted operations and retaining customer trust and brand reputation. The reality is that it is no longer a question of whether your organisation will encounter a cyberattack, but rather when and to what extent you are prepared to effectively counter it. What is disconcerting is that over half of senior security and risk leaders, as revealed by a comprehensive study, confessed that their organisation was not prepared for a ransomware attack or any other cyber incident<sup>1</sup>. Only one-third expressed confidence in their workforce's preparedness to execute essential recovery tasks post-cyber incident, underscoring the importance of proactive readiness.

Cyberattacks show no signs of slowing down and will likely be compounded by rapid advancements in artificial intelligence and heightened geopolitical tensions<sup>2</sup>. Notably, despite a temporary dip in 2022, ransomware attacks surged to unprecedented heights in the first half of 2023<sup>3</sup>. An additional alarming trend is that supply chain attacks are predicted to impact a staggering 45% of organisations by 2025, triple the amount of 2021<sup>4</sup>.

Proactive preparation against crises involves two interconnected aspects: meticulous planning and rigorous drilling. Imagine the devastating consequences of firefighters running into a burning building after having merely studied the fire brigade protocols but never experiencing fire drills. The same principle applies to tackling a cyber crisis: improvisation is not a viable strategy. Effective crisis preparedness involves ensuring that up-to-date plans are comprehended by all relevant stakeholders. A well-crafted plan functions as a strategic instrument, empowering organisations to navigate challenges with minimal disruption and secure their interests. Yet, as the saying goes, 'no plan survives first contact', reinforcing the need for thorough stress-testing of the plans via simulated exercises. An organisation that has effectively planned and trained through simulations of incident response and crisis management is far likelier to withstand an actual cyberattack<sup>5</sup>.

1 Osterman Research (2023). Cyber Workforce Resilience Trend Report.

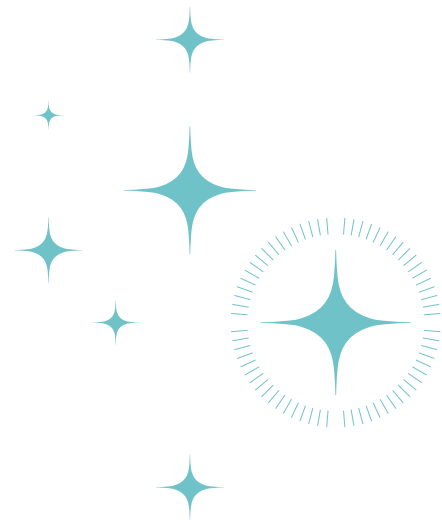
2 SoSafe (2023). CyberCrime Trends 2023.

3 SonicWall (2023). 2023 SonicWall cyber threat report.

4 Gartner (2022). Top Security and Risk Management Trends for 2022.

5 Pearson et al. (2021). Cyberattacks are inevitable. Is your company prepared?





Elevating cyber resilience requires substantial investments, not only monetary, but primarily time and energy. Nonetheless, the dividends are considerable: a well-prepared and cyber-resilient organisation can significantly reduce its response and recovery time following a crisis. In addition to preserving crucial resources, crises offer a platform for incident responders and crisis managers to demonstrate their adeptness in navigating difficult circumstances. Effective management has proven to provide stakeholders with confidence in their organisation's resilience abilities, effectively contributing to and enhancing shareholder value<sup>6</sup>.

## Never waste a good crisis

Combined with our unique observations and industry best practices, the six success factors for cyber-resilient organisations are intricately connected to the cyber-threat landscape, prompting a call to action. Through the NIST CSF 2.0, readers can contextualise the six factors and are guided towards cyber resilience strategies focused on people, processes, and technology. Section 2 delves into the concept of cyber resilience, arguing for an integrated approach. Section 3 provides an outline of the cyber-threat landscape. Section 4 establishes the primary thesis of the paper: an examination of what the six success factors are, and Section 5 concludes the paper.

---

<sup>6</sup> McAllister (2017). Crisis preparedness and its impact on shareholder value.



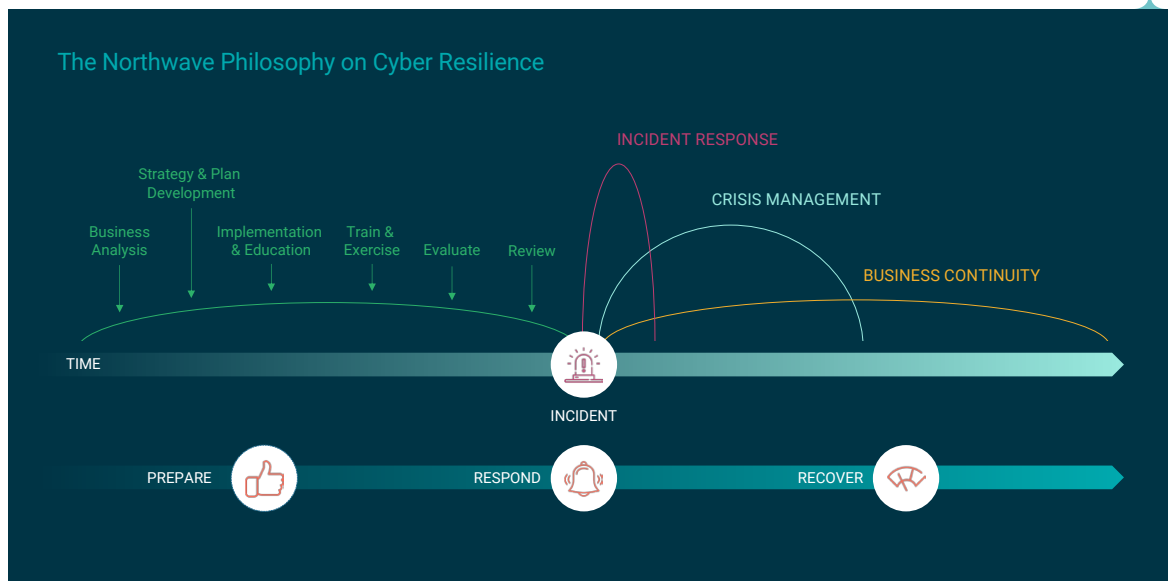
## 2. What is cyber resilience?



In many European languages, the translation of resilience can have different meanings. Northwave is originally a Dutch company, and in Dutch, resilience encompasses both *weerbaarheid* and *veerkracht*. *Weerbaarheid* focuses on the ability to withstand challenges and difficulties. At Northwave, we focus every day on our clients' ability to withstand cyber security threats with an integrated approach based on three areas of expertise: business, bytes, and behaviour. *Veerkracht* focuses on the ability to endure and overcome difficult situations, which is the primary focus of this white paper.

The field of cyber resilience has rapidly grown out of a necessity to react to successful cyberattacks. Northwave's definition of the *veerkracht* meaning of cyber resilience is an organisation's 'ability to face and cope with adversity, adapt to change, recover, learn, and grow from cybersecurity incidents and crises'. This is authenticated by the literature, which tends to focus on four phases: prepare, absorb, recover, and adapt<sup>7</sup>. ISO 22361:2022<sup>8</sup>, a standard dedicated to security and resilience in crisis management, aligns with these principles, emphasising the importance of preparedness, effective response, and continuous improvement in the face of cyber threats. The prevent phase falls outside the scope of cyber resilience, as it is implied that the most undesirable situations have already occurred.

According to Northwave's philosophy, cyber resilience is best practiced through an integrated approach that combines three fields—incident response, crisis management, and business continuity management—into a cohesive framework (illustrated in Figure 1). By combining these three fields, you adopt a holistic view of your risks and their interconnectedness, in turn gaining better understanding of your business processes and the defences for the full spectrum of cyber threats, from minor incidents to a major crisis.



**Figure 1: Three streams during cyber incidents**

The value of the integrated approach arises in the interdependencies of the three streams. **Incident response** addresses source control from a technical and operational perspective, while **crisis management** focuses on effect management and strategic decision-making during escalated incidents. **Business continuity management** aids in recovery and returning to normal operations. Adopting this unified framework for cyber resilience helps organisations minimise blind spots and ensures coordinated functioning amongst security teams, leading to efficient responses and streamlined actions

7 Ali et al., (2023). Innovation for Resilience: A Focused Study on Workforce, Climate, Supply Chain, and Cyber Resilience.

8 International Organization for Standardization. (2022). ISO 22361:2022, Security and resilience - Crisis management - Guidelines.



## 3. What threats do you face?



You need to thoroughly understand the cyber threats you face to proactively prepare and counter them. A previous Northwave white paper, [Your Most Important Digital Threats](#), identified the three most common threats organisations face today: ransomware, business email compromise, and insider. Based on the incidents we handle, our exchanges with intelligence partners, and public information sources, we reaffirm that the three threats are threats which warrant more attention, and we have further assessed that supply chain compromise does as well.

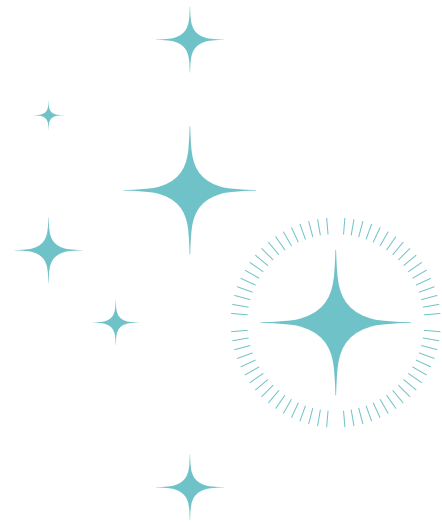
### 3.1 Ransomware

Ransomware remains a very pressing threat. Ransomware is malicious software that encrypts a user's systems or files; after encryption, the decryption key is offered in exchange for payment. It often involves extracting the victim's data and deleting the backups while threatening to publish the data. Ransomware attacks have a significant impact on the continuity of business operations. Therefore, the financial consequences often extend far beyond the payment of ransom. Previous Northwave research has shown that besides the aforementioned serious impact on business continuity, ransomware can have a lasting psychological impact as well, including distress symptoms so severe that they require psychological help<sup>9</sup>.

### 3.2 Business email compromise (BEC)

BEC, also widely known as CEO fraud, is a form of fraud in which the threat actor manipulates the email traffic between two parties to execute fraudulent transactions. Threat actors either gain access to a mailbox in the target organisation or spoof the identity of a trusted figure in the organisation. The methods they use involve social engineering tactics such as phishing or spear phishing to impersonate a person the victim knows, deploying remote-access software to log in to a victim's machine, or registering a domain name with a strong resemblance to the victim's domain name. The threat actors attempt to manipulate a transaction to redirect the money, which results in a considerable financial impact and significant reputational damage for organisations.





### 3.3 Insider threat

Insider threat refers to individuals that are part of the employee base with legitimate access to or advanced knowledge of the organisation's functioning and harm the organisation. The harm could be the result of a third-party compromise (i.e. on the supplier/vendor side), negligence, or malicious intent. Most cases involve either a lack of awareness or negligence. Malicious insider threat is relatively rare, but can materialise in cases of intellectual property theft, fraud, or even espionage. What makes insider threats typically difficult to defend against is that the person is already inside. Their motives can range from resentment to anger to financial gain.

### 3.4 Supply chain compromise

Supply chain compromise is an attack vector utilised by threat actors by victimising suppliers or third-party service providers of the target organisation, rather than attacking the target directly. They are used since they exploit the trust and dependencies of the less secure parties, typically involved in the production, distribution, or maintenance of software and hardware.

Gaining insight into the threat landscape is an advantageous initial action. Considering its evolving nature, organisations are compelled to adapt. The six success factors outlined below assist in strategically minimising the impact of these cyber threats.

---

9 Northwave (2022). After the crisis comes the blow - The mental impact of ransomware attack.



## 4. The six success factors of cyber resilience



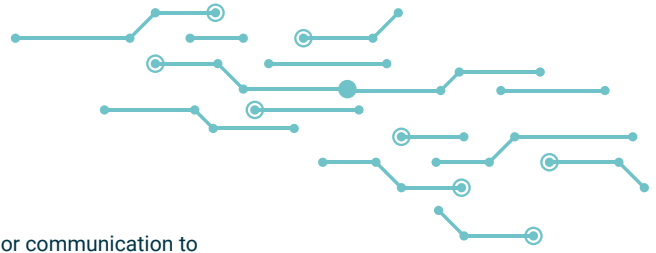
The six factors are (1) strong leadership and clear governance, (2) effective crisis communication, (3) strong relationships and partnerships, (4) mental strength, (5) a commitment to continuous learning and improvement, and (6) adaptability. The NIST 2.0 CSF can be adopted as a reader's guide, with **Respond** and **Recover** being the most relevant core functions; this is because our definition of cyber resilience assumes that an incident has occurred and preventative measures have been bypassed. Nevertheless, significant overlap exists among the other core NIST functions of Govern, Identify, Protect, and Detect and the six success factors. Each function reinforces the others and contributes to improving cyber resilience in organisations.

### 4.1 Leadership and clear governance

#### 4.1.1 Crisis leaders

Effective leadership, facilitated by a clear governance structure, is the backbone of an organisation's resilience when navigating a crisis. While overall leadership responsibilities rest with the board, in the context of resilience, effective leadership refers to incident responders and crisis managers who are entrusted with the responsibility of identifying the issue, minimising its repercussions, and restoring operational continuity within the organisation. Effective crisis leaders offer clear direction, make decisive choices, and coordinate with each other (incident responders, crisis managers, and business continuity managers) to ensure alignment with organisational goals. Ultimately, they guide organisations through challenging times and make them stronger on the other side. Logically, we notice that the most effective crisis leaders have been tried and tested, therefore experience is perhaps the most valuable quality they offer.

For instance, imagine a manufacturing organisation facing a ransomware attack. If their OT systems controlling machinery, assembly lines, or any other critical industrial processes are impacted, the manufacturing operations could grind to a halt. In the beginning, incident responders detect an incident. Once the incident is recognised as severe, incident responders escalate and communicate their findings to the crisis managers. The incident responders contain the ransomware's spread, initiate eradication measures, and gather information. Simultaneously, the crisis managers assess the broader impact of the OT being impacted and make critical decisions. An example concerns the ransom payment



and negotiations with the threat actor, whether to involve law enforcement, or communication to stakeholders such as business partners or the media. All the while, the teams coordinate with the right business managers to ensure business continuity. Experienced incident responders and crisis managers recognise how best to approach the crisis based on their instinct and habits.

#### 4.1.2 Governance structure

No crisis is resolved without a dedicated team; a characteristic of good leaders is recognising the value of their team and being able to delegate. Known as the gold-silver-bronze (GSB) command structure, a crisis organisation normally consists of three levels, each with distinct roles and responsibilities. The gold team focuses on the strategy and sets the intent. The silver team focuses on tactical aspects by formulating the plans necessary to achieve the strategy intent. They consider practical implications and instruct the bronze team, who carry out the operational response that is outlined in the incident response, crisis management, disaster recovery, or business continuity plan. More specifically, the GSB structure can be effectively prioritised by using a permanent core team and a flexible team. The core team consist of members who are always present when an incident or crisis has been determined, and the flexible team consists of members who are added to the core team depending on the subject expertise needed. It is important to be aware of different events in which flexible members could be involved and that the GSB structure can differ greatly depending on the needs and structure of each organisation.

## 4.2 Effective cyber crisis communication

Organisations that communicate effectively during times of change or crisis are better equipped to manage uncertainty and keep their stakeholders informed. Clear communication helps maintain trust, manage expectations, and facilitate collaboration. To execute effective crisis communication, we say you need to keep at least the following two principles in mind:

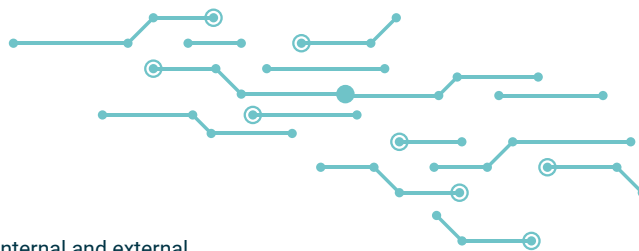
### 4.2.1 Not communicating is (almost) impossible

In today's highly connected world, where information flows rapidly through various channels, not communicating during a crisis is nearly impossible. Silence or a lack of official communication leaves a void that is often filled by speculation, rumours, and misinformation. This can lead to increased anxiety, loss of trust, and further damage to the organisation's reputation. In the absence of official communication, stakeholders may turn to social media, news outlets, or other unofficial sources for information, which can result in the spread of inaccurate or misleading information. By proactively engaging in crisis communication—stealing thunder—organisations can regain control over the narrative, correct misinformation, and provide accurate and reliable updates directly to stakeholders.

Therefore, organisations should always take transparency as the starting point; however, the timing of transparency is of the utmost importance. Sometimes, there are good reasons to not (yet) be transparent. Reasons for this can be varied; consider, for instance, the day of the week, a recent stock market listing, the influence of (geo)political dynamics, or legal perspectives. Deciding to not (yet) proactively communicate is a risk which should be considered carefully and requires a good strategy.

### 4.2.2 Crisis communication is an integral part of crisis management

Crisis communication should be thoughtful and well-planned. It requires careful consideration of the messaging, timing, and the channels used to communicate, as well as alignment with the organisation's overall crisis management strategy. Therefore, during a cyber crisis, collaboration between the crisis management team (CMT) and crisis communication team (CCT) is vital to ensure an effective response. As previously described, the CMT is responsible for effective management strategies, while the CCT



is responsible for ensuring clear, accurate, and timely communication with internal and external stakeholders. They develop and disseminate key messages that address the crisis, provide updates on the organisation's response efforts, and address stakeholder concerns. The team also manages media relations, coordinates communication channels, and helps maintain the organisation's reputation and stakeholder trust throughout the crisis.

When we help organisations that are dealing with a cyber crisis, we see that crisis communication and reputation management are distinct yet interconnected disciplines. While crisis communication focuses on managing communication during a crisis to address immediate concerns and mitigate the impact on reputation, reputation management takes a broader and more proactive approach to build and maintain a positive image of the organisation over the long term. Both disciplines are essential in effectively managing an organisation's reputation in different contexts and timeframes. However, it is important to note that ethical crisis communication should be put first, since this will benefit the organisation's interests and reputation in the end.

For an effective cyber crisis strategy, it is vital to listen to your important stakeholders. What do your employees, customers, suppliers and maybe even the media need to know? What do they require from you? How can they be properly informed? This input should underpin your cyber crisis communication strategy.

### 4.3 Strong relationships and partnerships

Resilient organisations build and maintain strong relationships with their stakeholders, which include their employees, (IT) suppliers, and customers. They foster and contribute to a sense of community. These relationships encourage collaboration, trust, and support that can carry organisations through challenging times. Resilient organisations not only acknowledge their own role within a larger ecosystem that includes supply chain partners, but they also understand that the continuous delivery of their products and services relies on the collaborative efforts of all stakeholders.

#### 4.3.1 IT suppliers

At Northwave we have seen incidents and crises where good relationships, founded on trust with IT suppliers, were crucial to getting back in business as fast as possible. Therefore, it is essential to determine responsibility and accountability policies with suppliers and to check these directives regularly for compliance. Too often, organisations fully rely on the IT supplier knowing what to do when a cyber crisis arises. However, large cyber crises are often a first for both parties. Therefore, the trust organisations place in their IT supplier can also be their vulnerability. As previously discussed, supply chains and IT suppliers are increasingly used to exploit the trust and dependencies between the less secure parties involved in the production, distribution, or maintenance of software and hardware.

Building a strong relationship with IT suppliers starts with being aware of and recognising an organisation's own dependencies on these suppliers. Executing a business impact analysis (BIA) reveals whether certain suppliers are a single point of failure for a business's vulnerable process. However, IT suppliers should not be viewed as a threat. Once these insights are available, opportunities can become clearer. The partnership between an organisation and their IT partner is only strengthened by collaborating on securing common environments.

With those insights, there are multiple best practices to minimise the impact of those dependencies through the establishment of strong partnerships before a crisis occurs. They create a foundation for effective collaboration during challenging times:



1. Establish a clear point of contact on both sides, including backups for after office hours and during holiday periods.
2. Set clear service-level agreements (SLAs) with your IT suppliers, based on your business continuity requirements, which document what services the IT suppliers will provide against what service level standards.
3. Train and drill multiple threat scenarios and let your IT suppliers participate in the exercises. You will need their support most during the crisis, therefore you should both drill these scenarios up front.
4. Execute a disaster recovery test where you test the recovery and backup procedures together with an IT supplier that the business is dependent on. You will stumble upon unexpected errors, which will provide insights into how long restore procedures could take. We have witnessed IT suppliers making claims that they could restore within four hours, whereas it actually took five days. This insight up front can prevent spoiled relationships with IT suppliers during an actual crisis. Moreover, if executed well, it creates a feeling of mutual control.

#### 4.3.2 Customers and stakeholders

Of course, this also works the other way around. Cyber crises can erode your reputation and customers' trust and confidence in your organisation. Having strong pre-existing relationships can help mitigate this impact. Customers and stakeholders who trust the organisation are more loyal and more likely to believe that the company is taking the incident seriously and working diligently to resolve the issue. Additionally, established relationships with customers allow for quicker recognition of their needs and enable a more personalised approach to addressing those needs.

### 4.4 Mental strength within crisis teams

When your organisation is under attack, your people are under immense stress for a prolonged period<sup>10</sup>. To be able to defend yourself effectively, it is necessary to invest in their mental strength. This not only ensures faster recovery but also prevents fallout, which otherwise only further delays the business recovery process. This can only be achieved through preparation.

The following variables (this is a not an exhaustive list) contribute to developing mental strength within crisis teams: coping mechanisms, trained behaviour, and physiology.

#### 4.4.1 Coping with stress: planning and task division

Research on how best to deal with stress shows a multitude of effective strategies. These strategies or actions that people take to deal with the stress of an unusual situation are called coping strategies<sup>11</sup>. Often, we distinguish between two types of coping<sup>12</sup>: problem-focused and emotion-focused. **Problem-focused coping** focuses on removing the source that causes stress, and **emotion-focused coping** is about thinking and reflecting on where the feelings and thoughts are coming from and then coping with them constructively. Both types of coping are effective and can be stimulated from the outside.

To enhance problem-focused coping, it is necessary to unite across a shared crisis agenda. Indeed, when asked what could have helped to resolve a ransomware attack more quickly and with less negative consequences for mental health, both CERT team members and affected companies indicate that clear planning and task division is crucial<sup>13</sup>. Experience has taught us that one of the most effective ways to come to such a shared planning and task division is the OODA loop, which was initially developed by military strategist and United States Air Force Colonel John Boyd:

<sup>10</sup> Northwave (2022). (n9).

<sup>11</sup> APA Dictionary of Psychology. Coping.

<sup>12</sup> Lazarus, R. S., & Folkman, S. (1984). Stress, appraisal, and coping.

<sup>13</sup> Northwave (2022). (n9)

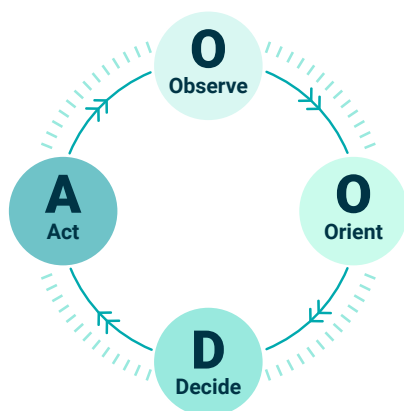






Figure 2: OODA-loop

OODA Loop: Decision-making method	
	<b>Observe</b>
<b>Time management:</b> set end time of crisis meeting	
<b>Scaling up:</b> which teams are active in addition to this team (governance)?	
<b>What is the cause:</b> what information is available about the incident?	
	<b>Orient</b>
<b>Separate facts from assumptions:</b> what do we know (facts) and what do we think (assumptions)?	
<b>Setting goals:</b> process goals and end goals	
	<b>Decide</b>
<b>Create scenarios:</b> determine current and potential impact	
<b>Assertiveness:</b> discuss possible options and choose the best option	
	<b>Act</b>
<b>Prioritize:</b> what needs to be done first?	
<b>Take action:</b> who is going to execute which action and when?	
<b>Repeat:</b> decide when and how the next meeting will take place	

#### 4.4.2 Coping with stress: pay attention to mental health

Besides problem-focused coping, emotion-focused coping can be a positive way to deal with negative thoughts and stress, especially since cyber crises do not get resolved within a short period of time. In fact, dealing with a crisis can take months or even years. Consequently, the negative impact of such a crisis on mental health can also occur over a prolonged period. In fact, up to a year after a ransomware incident, one in seven members of the crisis team will have symptoms of trauma that are so severe that they require professional help<sup>14</sup>. It is therefore unsurprising that crisis teams who have dealt with ransomware attacks not only indicate a need for planning and task division, but also a need for concrete tips and tricks to help themselves and their colleagues to prevent severe mental impact. Here, we describe some effective methods for encouraging healthy coping, based on our experience:

- **Monitor mental health regularly:** the stress symptoms you observe are often just the tip of the iceberg. By assessing the current state of mind of your crisis team, for instance at the beginning of each start-up meeting, you can keep an eye on people who may require additional help.
- **Encourage social support:** social support is one of the most effective ways to encourage emotional coping. It can thus be helpful to advise your people to actively seek social support, both from their colleagues and in their private life.
- **Encourage physical activity:** physical activity improves mood, gives people energy, and helps get rid of stress. Advise your employees to take time to go for a run or have a meeting outside while walking where possible.





- **Facilitate healthy eating:** when stressed, we often crave unhealthy foods such as pizza or chips. These may provide temporary comfort, but they ultimately contribute to more negative effects on mental health. By simply providing healthy foods and drinks rather than sugary or fatty food and drinks, you will help your employees recover faster.
- **Encourage fun:** humour is also widely used in very extreme situations. For example, you can compare your own negative thoughts and feelings with something that could have been even worse—to the point of absurdity. Being able to laugh and let go can have a positive effect on mental health.
- **Allow for sufficient rest:** people often approach cyber crises as a sprint; they work very long hours and sleep too little. However, a cyber crisis is a marathon, not a sprint, and to be able to stay healthy, sufficient rest is crucial. It can thus be helpful to agree on a maximum of 12 working hours per day.

#### 4.4.3 Training behaviour

Stress plays an important role in crisis situations. Recognising and learning to regulate these stress phases is essential. Stress occurs when the body is challenged to adapt to a stressor<sup>15</sup>. A stressor triggering a stress response is heavily contingent on previous experiences. While the physiological responses to stress are always the same, the way in which stress is handled differs from person to person and, consequently, from crisis team member to crisis team member. It depends on perception and how one reacts emotionally and cognitively. Visualisation is often used as a technique to reduce and prevent stress because of the powerful way it affects the mind and body.

Visualisation and/or using mental imagery to improve performance has been used for years within both professional sports and the armed forces. Doing and repeating something so often (including in your head) that you literally start dreaming about it at night ensures that it becomes automatic, and when you need it in a crisis situation, it does not require unnecessary thinking capacity. Visualising in the context of a cyber crisis means talking about various scenarios together, for instance during a workshop or a walkthrough session. Visualisation provides a first step in memory, but it is not enough to ensure a successful response to a crisis. To make it a complete drill and make it effective in stressful situations, realistic and unexpected exercises are necessary.

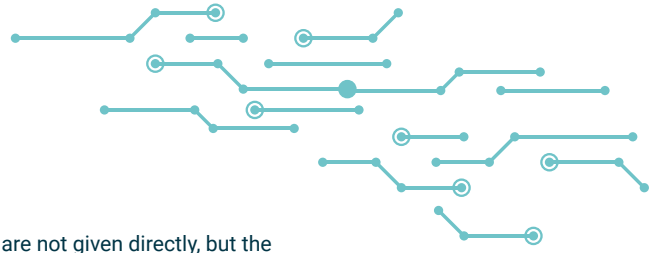
The fight or flight response is the body's natural physiological reaction to stressful events that was first researched by American physiologist Walter Cannon<sup>16</sup>. In the years since his research, physiologists and psychologists have developed and refined Cannon's work, coming to a better understanding of how people react to threats, which are the fight, flight, and freeze reactions. When one freezes, one is unable to move or act in a stressful situation.

To prevent people from freezing, it is important that they can fall back on a well-rehearsed drill. This is achieved by repeatedly training and drilling certain actions or process steps. This can be done in multiple ways. But there is a difference between implicit and explicit learning, which is whether the behaviour is ensured intrinsically or extrinsically. Explicit learning goes from 'watch me as a facilitator explain the steps to follow, then show it using an example and then you can copy that behaviour yourselves'. Implicit learning is more about coaching and redirecting the team, without prescribing everything in advance. First, let the team explore the situation and act from their intrinsic motivation. The goal is that the most important things will be remembered instead of just trying to remember certain steps and being less focused on information coming in from the (external) environment. This is the case, for example, in gold-team exercises: a full day of simulated cyber incident drills in which the IT network and architecture are used for the creation of a customised and realistic scenario. Gold-teaming is a way to learn through practice; guidance is given on the behaviour of individuals in the team

<sup>14</sup> Northwave (2022). (n9)

<sup>15</sup> Selye, H. (1984) *The Stress of Life*.

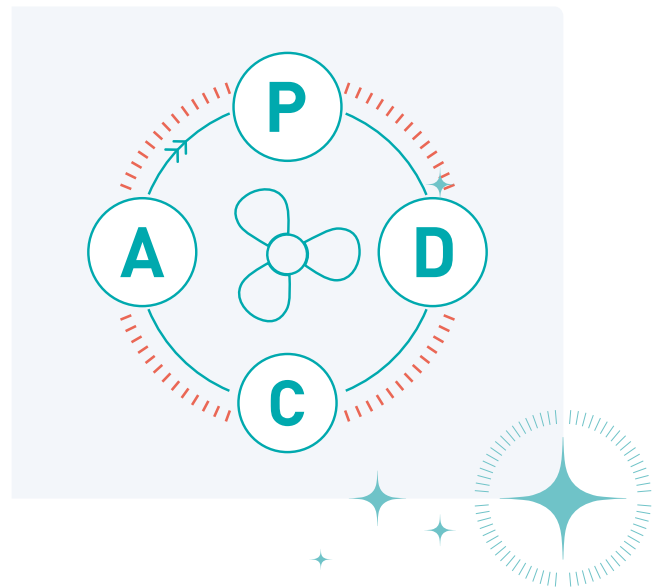
<sup>16</sup> Cannon, W.B. (1929). *Bodily Changes in Pain, Hunger, Fear and Rage*.



during a setback, but without everything being predigested. Here, solutions are not given directly, but the participants themselves must investigate the situation to come to a solution. This sometimes causes friction. But as Seneca once said, 'A gem cannot be polished without friction, nor a man perfected without trials'. Friction within a team stimulates growth. As a result, individuals within the team become comfortable with the uncomfortable.

#### 4.5 Continuous learning and improvement

Resilient organisations foster a culture of continuous learning and improvement to ensure they are evolving effectively. They encourage feedback, analyse lessons learned from past challenges, and apply those insights to improve their processes, systems, and strategies. The learning component, which has continuously been addressed throughout this white paper, focuses on the employees' knowledge and the exercises required to improve and strengthen the organisation's cyber resilience capacity. To increase your organisation's cyber resilience, it is essential to prepare by doing business analyses and developing plans and strategies while also implementing, training, evaluating, and reviewing them. For maintaining and updating plans and procedures, Northwave recommends establishing overarching policies using the Plan-Do-Check-Act (PDCA) cycle. This is business management method is used to control and continue the maintenance of processes. There are a couple of starting points when it comes to establishing organisational learning and improvement, which are explained below.



##### 4.5.1 Maturity scan

Firstly, it is important to gain regular quantitative insight into your current maturity level by conducting a maturity scan or assessment. A maturity assessment contributes to a clear overview of key aspects such as incident response capabilities, crisis management practices, and business continuity. It allows you to benchmark your organisation against industry standards and best practices and offers a roadmap with recommendations for staying ahead of the ever-changing cybersecurity landscape.

##### 4.5.2 Implemented plans

Additionally, ensure that your plans remain easily accessible by thoroughly putting into action your crisis management, incident response, and business continuity plans. While having well-crafted plans is crucial, it is important to acknowledge that unexpected events will inevitably arise. Hence, possessing plans alone holds little value. It is imperative to actively engage in both creating the plans as well as continuously updating those plans based on new threats and internal changes. Alongside that, a plan needs to be implemented within the organisation and its execution strategised. Implementation is done by introducing and explaining the plan to the organisation, actively involving the people who need to use it, and planning training sessions and exercises to practise the plan.

##### 4.5.3 Cyber resilience trainings and regular exercises

To ensure continuous learning and improvement, providing regular training and exercises for the individuals who deal with cyber resilience within the organisation is recommended—training sessions such as role-specific training, crisis decision-making training, and crisis communication training.

<sup>17</sup> Cannon, W.B. (1929). Bodily Changes in Pain, Hunger, Fear and Rage.



Training incident- and crisis-management team members ensures that they gain correct, up-to-date knowledge and skills to execute important tasks and responsibilities during a crisis. In addition to training, conducting regular drills will also help to identify vulnerabilities, test incident response capabilities, and improve cyber resilience. If done on a regular basis, these exercises are a very efficient way of strengthening your organisation's response strategies. For adequate learning and improving, it is important to ensure a drill cycle which carefully builds up in maturity, for example:

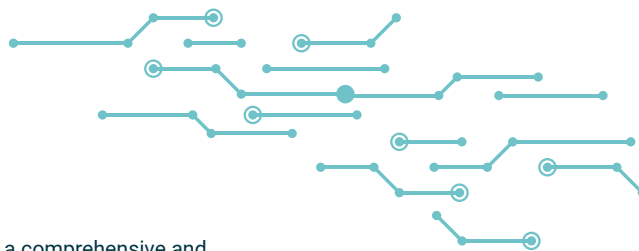
- **Incident or crisis tabletop exercise:** Start by organising a tabletop exercise when setting out to as an incident response or crisis management team. During an incident or crisis tabletop exercise, teams are challenged to communicate, collaborate, and exchange information on a more advanced level. The outside world is simulated by a response team, and individual information is sent to the participants. They ask/answer questions, bring in new information, and serve as your counterpart in logging decisions throughout the exercise. Practice managing the cyber incident and engaging with relevant stakeholders (e.g. IT service providers or vendors) without any risk.
- **Semi-live cyber crisis exercise:** Once teams have drilled separately, start having teams drill together and execute a semi-live exercise. Semi-live exercises may involve multiple teams and locations, with lines of communication to different response teams. In this way, your teams practice with and against each other and therefore face 'real' stakeholders and real emotions. This increases realism and, ultimately, your cyber resilience.
- **Gold-team cyber crisis exercise:** With a mature cyber-resilient organisation, the next step is to execute a gold-teaming exercise. Gold-teaming is a crisis management exercise combined with red-teaming. The crisis scenario is based upon the results of a Red Team. Gold-teaming is an unexpected exercise which picks up where red-teaming leaves off, making it the most complex exercise to deal with.

## 4.6 Adaptability

A key element of Northwave's definition of resilience is being able to adapt to change. For an organisation to thrive in the face of adversity and in challenging circumstances, whether that be a sudden economic downturn, a natural disaster, or a cyberattack, they must showcase their ability to evolve and thrive in the face of change. Just as comprehending your security posture and strategies is crucial, it is equally crucial to know when and how to adapt those strategies in response to a crisis. This underscores the value of drilling multiple threat scenarios and having adaptable plans which enable deviation. It is impossible to plan for every risk; however, there are many measures to mitigate associated risks.

### 4.6.1 Adaptability in your basic insights and setup for resilience

Most gains in terms of adaptability occur during the cold phase. The crucial first step is to prioritise the business processes that have the greatest impact on the organisation's success. To differentiate between critical and non-critical processes, companies should regularly conduct business impact analyses. This type of analysis identifies the most critical processes, assesses their dependencies, and enables the development of tailored recovery strategies during a crisis. By forecasting the threats and their disruptive consequences, business continuity managers are aware of any necessary information that must be gathered in a crisis to customise the recovery strategy.



The second step is to recognise and stay informed on emerging trends. For a comprehensive and relevant business impact analysis, it is advantageous to include timely and updated cyber-threat intelligence. A common organisational pitfall is adopting a reactive approach which does not account for [the most pressing and common cyber threats](#) and their potential consequences to the organisation. To ensure business continuity, organisations must recognise threats and their potential consequences and embrace the idea that the threats demand innovative, unique solutions and recovery strategies. Embracing innovation is easier said than done, since it can be costly and often requires both approval from leadership and a commitment to continuous learning.

For example, in the event of a ransomware attack, backups are essential to returning to business operations. The 3-2-1 backup strategy states that an organisation should have at least three copies of its data on two different devices/media, of which one copy should be stored off-site in case of disaster recovery. Ideally, the quality of the backups is checked routinely. During the forensic recovery, indicators of compromise (IOCs) could assist in identifying malicious activity in the organisation's environment.

#### 4.6.2 Adaptability during a crisis

With the necessary conditions for adaptability addressed in the cold phase, adaptability occurs during the hot phase, the crisis. During the hot phase, the exercise-tested plans should be the central point of reference. However, if it is necessary to adapt the plans (owing to new insights), it is important that resilience leaders trust their own and their teams' expertise and judgment and feel they can innovate if needed. Being able to make informed deviations is not merely a beneficial characteristic but an essential necessity for survival. As one loosely translated expression goes: 'You can prepare for 1000 situations, but then situation 1001 will inevitably occur'. The more time you spend training, the more patterns recognised and the more experience there will be to spot when adaptability is required.

To continue the example of the ransomware attack, it is important to set realistic recovery time objectives for your most vulnerable processes. We have observed that a ransomware attack will disrupt your processes for an average of 23 days<sup>17</sup>. As a result, appropriate workarounds and other methods of working must be prepared and tested. Combining business analyses with threat intelligence enables organisations to adapt to threats and customise their recovery strategies to return to business as usual.



<sup>17</sup> Northwave (2022). (n9).



## 5. Conclusion

Never waste a good crisis. In cyber resilience, we would prefer to never waste a good *simulated* crisis. We can talk and you can read about cyber resilience ad infinitum, but that will not enhance your resilience. Experiencing it in a variety of ways in a safe environment increases awareness, offers new perspectives, and facilitates growth. Taking ownership and seeking that challenge makes your business stronger and more resilient. With an understanding of the cyber threats you face, we can train your cyber resilience capacity and apply the six success factors to be able to conquer all the threats we have identified and reach the stage of being a cyber-resilient organisation:

- **Effective leadership and a clear governance structure** function as the backbone of an organisation during times of crisis. Experienced crisis leaders are empowered to roll up their sleeves and get to work immediately. Assisted by an established governance structure, they can delegate tasks to their teams and respond to crises effectively. After all, no crisis is resolved without a dedicated team. Therefore, characteristics of good leaders include being able to recognise the value of their team and being able to delegate.
- **Effective cyber crisis communication** is now a fundamental responsibility for organisations. It boils down to stealing thunder. If there is bad news, proactively and transparently deliver it to maintain stakeholder trust, manage expectations, and mitigate the risk of misinformation during times of uncertainty. The communication should be crafted in collaboration with the crisis management teams and tailored to meet the specific needs of the stakeholders.
- Building trustworthy **relationships and partnerships** with IT suppliers, customers, and stakeholders does not come easily. Over time, cultivating these relationships contributes to strong and durable capacities that weather crises, but also enhances the overall ability to adapt and thrive in an ever-changing landscape.
- Stress, anxiety, and hopelessness are inevitable when tackling a cyber crisis. Yet being aware of this impact and bolstering the **mental strength of the crisis team** not only leads to faster recovery but also prevents prolonged fallout. By prioritising mental well-being, organisations can equip their teams through effective coping mechanisms, trained behaviour, and attention to mental health.
- A culture of **continuous learning and improvement** involves two steps: firstly, recognising where to focus by understanding your organisation's maturity level, and secondly, implementing plans and regularly training and drilling. These steps develop employee knowledge and test them through exercises with clear roles and responsibilities, fortifying the organisation's capacity for cyber resilience.
- Lastly, **adaptability** as an organisation means that you recognise and respond effectively to changing circumstances and unforeseen challenges, even deviating from existing plans if necessary. Embracing the ability to pivot and make informed deviations from the original course is not just a valuable trait but a survival imperative.

At this point, you have only read a white paper about the six success factors of cyber resilience. Knowledge is an essential first step, but now it is time to act, experience, and learn. The Northwave Resilience Team is ready to help you out in taking those next steps. With a multidisciplinary approach based on business, bytes, and behaviour, your organisation will not be wiped out by a crisis—it will be able to overcome it.

# About Northwave Cyber Security

Founded in 2006, Northwave Cyber Security is the leading Dutch interdisciplinary specialist in cyber security, with offices in Utrecht, Leipzig, and Brussels. With their professional and managed cyber security services, they enable European clients to remain in control while placed under the permanent protection of their confident cyber crew. Their integrated approach towards cyber risk mitigation delivers solid security and aims for cyber awareness and resilience.

---

## Get in touch with us.

**Currently facing a security incident?**

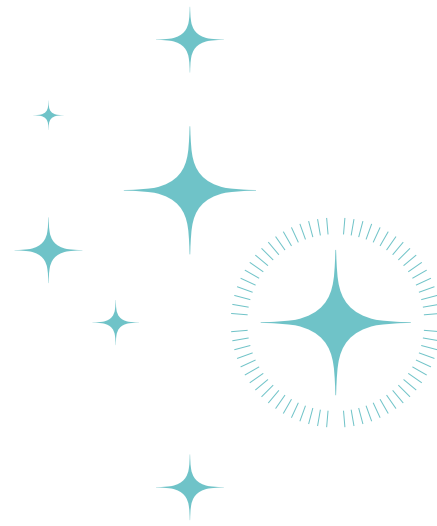
**Call day and night: 00800 1744 000**

## Contact

E: [info@northwave.nl](mailto:info@northwave.nl)

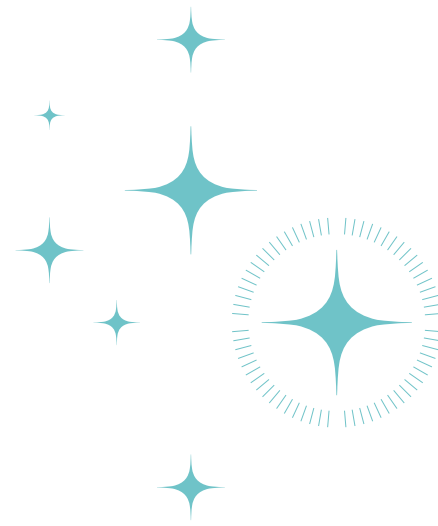
T: +31 (0) 30 303 1240

W: [northwave-cybersecurity.com](https://www.northwave-cybersecurity.com)





# Reference list



1. Osterman Research (2023). Cyber Workforce Resilience Trend Report. Available at <https://www.immersivelabs.com/wp-content/uploads/2023/05/Osterman-Research-Cyber-Workforce-Resilience-Trend-Report-May-2023.pdf>
2. SoSafe (2023). CyberCrime Trends 2023. Available at <https://sosafe-awareness.com/resources/reports/cybercrime-trends-2023/>
3. SonicWall (2023). 2023 SonicWall cyber threat report. Available at <https://www.sonicwall.com/2023-cyber-threat-report/>
4. Gartner (2022). Top Security and Risk Management Trends for 2022. Available at <https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022>
5. Pearson, K., Thorson, B., Madnick, S., & Coden, M. (2021, March 9). Cyberattacks are inevitable. Is your company prepared? Harvard Business Review. Available at <https://hbr.org/2021/03/cyberattacks-are-inevitable-is-your-company-prepared>
6. McAllister (2017). Crisis preparedness and its impact on shareholder value. Continuity Central. Available at <https://www.continuitycentral.com/index.php/news/resilience-news/2238-crisis-preparedness%20and-its-impact-on-shareholder-value>
7. Ali, H., Subah, N., Higman, M., Majkut, J., Harding, E., Ghoorhoo, H., Spaulding, S., Nair, D., & Barkof, S. (2023). Innovation for Resilience: A Focused Study on Workforce, Climate, Supply Chain, and Cyber Resilience. Center for Strategic and International Studies. Available at [https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230323\\_CSIS\\_Innovation\\_Resilience.pdf?VersionId=8Pt7ZAzTR6GIGrFucs35omyv6pjnlsxL](https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230323_CSIS_Innovation_Resilience.pdf?VersionId=8Pt7ZAzTR6GIGrFucs35omyv6pjnlsxL)
8. Northwave B.V. white papers & articles.
9. Northwave (2022). After the crisis comes the blow - The mental impact of ransomware attacks.
10. Northwave (2022). (n9).
11. APA Dictionary of Psychology. Coping.
12. Lazarus, R. S., & Folkman, S. (1984). Stress, appraisal, and coping. Springer Publishing Company.
13. Northwave (2022). (n9)
14. Northwave (2022). (n9)
15. Selye, H. (1984). The stress of life. McGraw-Hill Education.
16. Cannon, W. B. (1929). Bodily changes in pain, hunger, fear, and rage. New York; London:D. Appleton and Company.
17. Northwave (2022). (n9)