Buyers guide

Awareness, behavior and organizational culture

CYBERVEILIG NEDERLAND

Index

Introduction

The human factor plays an important role in increasing the cyber resilience of organisations. Organisation's employees work with digital systems daily and during this perform activities that influence the security of your organisation. It is thus a good idea to develop an organisation culture where this security is implicitly guaranteed.

To develop a cyber secure culture, it is important to work on two aspects:

- Increase awareness and knowledge
- Develop cyber secure behaviour

You can take different measures to work on these aspects. You can also request assistance from a cyber security service provider. It is important that you choose measures and services that are compatible with your organisation and organisation culture. Some measures and services are more effective than others. This is also linked to the maturity of your organisation in the field of a cyber secure culture. Only when the measures are compatible with your culture, it will be easy for employees to integrate them in their own activities, and they would be more likely to act in a cyber secure manner. If there is a proper connection to your culture, employees will be less likely to see measures as an obligation that must be met, they will translate it into the desired cyber secure behaviour and a positive development of the organisational culture. This is also often a growth process that proceeds step by step.

The purpose of this document is to give you insight into the aspects that play a role in the development of a cyber secure organisation culture and the services available on the market to realise this. With this information we hope that you will be able to submit a specified request in the market if you require support in this field. This document defines the various services and shows the current options available in this field. This way you will be able to make a better decision about what suits you, but you can also use this information to easily compare the quotations with each other. We see this document as a supplement to the Cyber security Dictionary published before (see Cyberveilignederland.nl/woordenboek) that formed the point of departure of the definitions.

We mainly wrote this buyers guide awareness, behaviour and organisational culture for security managers such as CISO's, but also for IT-managers, for Learning & Development supervisors, such as HR and communication managers and for buyers of security products and services. Naturally this document will also be useful to other target groups. However, we chose the topics based on the primary target group.

Achieving a cyber secure organisation culture

A lot of psychological research has been done into increasing awareness and knowledge, influencing behaviour, and developing an organisational culture in the field of security. Models and theories have been developed that explain where you can implement interventions in an organisation to positively influence the culture of an organisation.

These models and theories show behaviour aspects that you will want to influence, such as realisation and understanding, knowing, wanting, can, do and continue to do or maintain. The models and theories give direction to the cohesion and the order in how you influence these behavioural aspects. Specifically, the order is very important. For example, certain elements are preconditions before people proceed to a different behaviour.

For example, if an organisation wants employees to destroy confidential documents after use in shredder, it is important that the employee...

- Knows that he/she is required to do so (realisation)
- Understands how the shredder works (knowledge)
- Is facilitated by a paper shredder near the workplace (can, opportunity)
- And will want to make time to shred paper (want, motivation)

As soon as employees are aware and know what they are expected to do, it is important to give insight into what certain desired behaviour does not (yet) occur. Next, interventions can be formulated that will lead to the desired behaviour in a certain organisational context and can become part of the organisation culture, so that the behaviour can also continue to exist for long afterwards.

All of this is combined in the following four steps for awareness, behaviour, and organisation culture:

- Awareness and knowledge development
- Insight into the cause of the lack of desired behaviour
- Perform the suitable interventions for desired behaviour
- Perpetuating the desired behaviour in the organisational culture

Examples of these models and theories are (see attachment for details):

- Exercise Therapy and Behavioural Change (Balm, M.F.K., Purdue University Press, 2002)
- Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads (MacInnis, D. J., Moorman, C., & Jaworski, B. J., Journal of Marketing, 55, 32-53, 1991)
- Attitudes, personality, and behaviour (Ajzen, I., 2nd Ed., Milton-Keynes, England: Open University Press, McGraw-Hill, 2005)
- Persuasive by Design, Behaviour Change Model (R. Renes, S. Hermsen , Draaiboek gedragsverandering, 2017)
- Self-Determination Theory (Deci & Ryan, 1985; 2000)
- Transtheoretisch model (Prochaska & Di Clemente, 1982)
- The CASI-model (see https://www.communicatierijk.nl/vakkennis/casi/documenten/

Maturity in the field of organisation culture development

The maturity level of an organisation is an important aspect regarding the development of an organisation culture where security is considered an integral part. This maturity is apparent from the broad approach that an organisation has in the field of cyber security, in which several components play a role, such as risk management, policy, responsibility, technology, compliance and behaviour.

In the first instance, many organisations usually pay attention to making technology safe and setting up the associated processes, but they focus even less on the employees. However, it is important to grow in maturity across the board (technology, organisation, and people) in the field of cyber security. The steps described in the previous section (awareness and knowledge development, insight into the causes of lack of behaviour, measures aimed at behavioural change, perpetuation in the organisational culture) can serve as a guideline for the successive steps to be taken.

To approach behavioural change in a structured way, it is also possible to use a maturity model to grow step by step to a higher maturity level. Many suppliers currently use a maturity model they have developed themselves that can support this. These models are often developed based on an existing maturity model.

Most of these models have 5 levels of maturity that can be described as follows:

- **Ad hoc**. Awareness activities are deployed on an ad hoc basis. This is often very limited and incident driven.
- **Recorded.** There are various activities in the field of awareness, mainly driven by compliance considerations (for example from an implementation of the ISO 27001 standard).
- **Repeatable.** There is a plan with clear objectives, linked to the cyber risks of an organisation, and structural attention is paid to awareness and knowledge development, sometimes with a few steps aimed at behavioural change.
- **Managed.** There is insight into the desired behaviour in relation to the cyber risks incurred by an organisation. Interventions that change behaviour are managed from this point of view.
- **Optimised**. At this level, we have succeeded in creating a safety culture in which cyber-safe behaviour is self-evident and employees hold each other accountable for the (lack of) desired behaviour.

The table below shows the relationship between the above maturity levels and the 4 steps for awareness, behaviour, and organisational culture. In other words, every maturity level requires different measures related to awareness and behaviour.

MATURITY LEVELS	4 STEPS FOR AWARENESS, BEHAVIOUR AND ORGANISATION CULTURE
1. AD HOC	1. Awareness and knowledge development
2. RECORDED	1. Awareness and knowledge development
3. REPEATABLE	1. Awareness and knowledge development 2. Insight into the cause of the lack of desired behaviour
4. MANAGED	2. Insight into the cause of the lack of desired behaviour 3. Perform the suitable interventions for desired behaviour
5. OPTIMISED	4. Perpetuating the desired behaviour in the organisational culture

Table 1 Relationship between maturity levels and steps for awareness, behaviour, and organisational culture

The application of a maturity model could help an organisation to determine the current situation. A (initial) measurement is often performed for this. An organisation can then determine the desired level based on risk estimates on the one hand and available budget on the other, and when this level should be reached. In the end, that determines the measures that must be taken in succession.

Using a maturity model can be supportive for a CISO to place the necessary measures in the field of awareness and behaviour in the right context and to approach it in a structured way. This context can also help with the motivation of the required investments for the budget holder within the organisation.

Based on the choices in the field of maturity, a course can be put together for a specific period to implement awareness, behaviour and culture development. Ideally, the interventions form a continuous cycle where it can be alternated. This also has to do with the way in which people learn.

A course could, for example, look like this

WEEK	ACTIVITY
1-2	Identify the risks due to human behaviour
3	Workshop commitment management Identifying desired behaviour
4	Kick-off campaign cyber security behaviour for all employees with VR-game
4-6	Awareness e-learning employees
6-8	Behaviour measurements: • Mail phishing test • Check password
8-12	Analysis of current cyber safe behaviour in the organisation
12-37	Intervention program behaviour
CONTINUE	Weekly newsletter cyber security

Table 2 Fictional example of a possible development program

A glossary with services for a cyber safe organisation culture

In the paragraphs below we will explain which services are available in the market in each of these steps. This is not an exhaustive summary, but it gives an image of the current options available. The services are classified in the following categories:

- Measurements about cyber safe behaviour
- Workshops
- Communication campaigns for staff
- Trainings
- Analysis of behaviour and culture
- Behavioural interventions
- Culture program
- Consultancy

Measurements about cyber safe behaviour

Initial assessment

With a zero reading, the current level of the organisation is measured on a certain aspect related to cyber safe behaviour within an organisation. The purpose of the measurement is to determine a starting point for the changes to be made regarding cyber secure behaviour so that the effect can be determined after implementing certain interventions.

Er kan bijvoorbeeld gemeten worden op factoren als:

- Knowledge: what do employees already know about cyber secure behaviour?
- The attitude of the employees: do they feel safe working is important?
- The subjective norm: what does an employee think he or she is expected to do?
- The estimated control: do your employees feel they have adequate knowledge and tools to work cyber safe?
- Etc.

Effect measurements

Ideally a measurement is repeated annually, so that the organisation gains insight into the growth and development of the maturity in the field of awareness and behaviour. A zero reading could be more effective if the company has insight into the threat, risks, and measures that they have to / must take with regard to safe cyber behaviour.

Management dashboards

Because programs aimed at behavioural change often take a longer time, it is wise to regularly inform management about the progress of the program. Based on the baseline measurement and the goals set, a management dashboard can be set up to clearly display the progress.

Workshops

Workshop management insight into problems and commitment. To involve management in the movement towards more cyber secure behaviour, it is important that they also understand why the desired behaviour is required. By paying attention in a workshop to the greatest threats, risks and desired cyber-safe behaviour in the context of their own organisation, the sense of urgency is increased, and support is created for the necessary measures.

Management commitment is an important requirement for a successful development program in the field of awareness and behaviour. A workshop for the management is therefore often scheduled before the start of a program to establish sufficient support for the changes.

A management commitment session could serve various purposes:

- It could offer insight into the problems
- Discuss the use and necessity of management commitment
- Display, record and express the use and necessity of security awareness
- Record and express the rolls and responsibility of management
- Discuss the influence of the example function
- Discuss tasks

Tabletop workshop

A tabletop workshop focuses on a fictitious simulation that tests the organisation's cybersecurity capabilities. In most cases, attention is focused on incident response and crisis management.

During such a workshop, an organisation is confronted with a (sometimes tailor-made), fictitious scenario of a cyber-attack. This way the extent to which the organisation can effectively resist a cyber-attack is tested. It focuses on testing (existing) procedures in the field of crisis management and incident response. Depending on the target group, it is also possible to coordinate the dilemmas with the characteristics of this target group.

Possible dilemmas and learning purposes that are addressed:

- Whether participants have established sufficient procedures to ensure the continuity of the operations of the organisation as much as possible when a cyber crisis occurs.
- Whether participants also adhere to the prescribed procedures during a cyber crisis to guarantee the continuity of the organisation.
- Whether participants comply with their duty of care and reporting towards, for example, the NCSC, the Ministry of Justice & Security, and the responsible supervisors within the sector of the affected organisation.
- Whether participants have adequate internal communication with employees during a cyber crisis.
- Whether participants have adequate communication with partners within the sector during a cyber crisis. This includes partners within the industry with whom we collaborate in the field of production and supply and other organisations within the sector that could be affected by a cyber-attack.
- Whether participants have adequate external communication during a cyber crisis. In this regard think about journalists, politicians, directors, clients, civilians, and companies.

Communication campaigns for staff

Awareness campagnes

There are various forms of awareness campaigns that the organisation can use to focus on the importance of cyber secure behaviour.

For example:

- Newsletters. The power of communication lies in diversity and repetition. A newsletter pays attention to current security topics and can, for example, highlight positive examples from within the organisation.
- Blogs/vlogs. For a development program to be successful, it must align with the culture of the organisation. Blogs and vlogs can also be used for this. Ambassadors from within an organisation can have their say in blogs and relevant security topics can be brought to the attention in vlogs in a contemporary way.
- Posters, stickers, and other visible references. It is important that employees develop the desired behaviour and then continue to do so. Small reminders and nudging could support this. New behaviour will only become automatic if it is performed often and without having to think about it. Stimulating posters, stickers and other visible references can support this.

General presentations by security experts

Learning about certain topics that are relevant for a specific target group can be done in the form of a general presentation by a security expert. It can focus on topics such as the importance of information security or recent security lessons based on market research or threats to a particular department (e.g., finance or HR), or practical lessons for safer working (e.g., passwords).

It is also possible to show by means of a live hacking demo how, for example, passwords can be cracked using specific attack strategies or how an organisation's IT systems can be penetrated. It is important to coordinate the presentation

with the target group's level.
An audience without technical knowledge benefits more from a presentation in understandable language with examples that match their own work environment, while IT experts can benefit from a technical presentation about the first incident response steps in a ransomware attack.

Challenges / fun activities

A fun factor is increasingly being incorporated to make awareness campaigns more attractive to a wider audience. Learning is combined with a pleasant experience to learn the desired behaviour in a positive manner. Examples of these types of activities are:

- VR game. In a virtual world, the game's players are exposed to a variety of exciting challenges, and they must make wise choices.
- Escape room Players must escape from a difficult situation, for example by trying to prevent a fictional cyber-attack from being carried out on them.
- (Pub)quiz. Teams compete for most points regarding knowledge questions about digital security while having some drinks.
- Phishing battle. Teams of employees can take on the role of an attacker and initiate phishing actions themselves towards the other teams to collect as many points as possible. In this way, the participants gain more insight into the approach of an attacker and into desired behaviour to prevent phishing.

Often these types of activities are accompanied by a debriefing that summarizes the lessons learned.

Training

Digital training

Various digital training courses are conceivable to increase the knowledge level of employees in the field of cyber security. Many providers have a large digital library available with digital training courses.

When choosing suitable digital training, you need to take various elements into account:

- Language. It is important that the available languages match the languages that are used most frequently within your organisation.
- Culture. The way in which people learn is related to the area in which they grow up, live and work. Some training is primarily developed from one country or region. Other have a wider variety of content in this field.
- Training format. Some training courses are supplemented with text, others with infographics and animations and others with videos in which actors act out recognisable work situations. It is good to gain insight into the training formats offered and to choose what suits your organisation best.
- Expertise. Every organisation that develops training courses uses its own experts, such as learning experts, psychologists, and game designers, and has its own expertise. It is good to find out what the most important substantive principles are that forms the foundation of the teaching material and which (type of) experts have been deployed in the development of the digital training courses.
- Scope of the information available. The amount of information available varies. It is therefore important to check whether the information available about certain subjects is adequate in the view of the desired learning objectives of your organisation.
- Increasing the information available Some suppliers only have one type of training available (for example animations about basic topics). Other suppliers have a wide variety, ranging from micro learnings and brief introduction videos to in-depth programs. Depending on the desired learning outcome, a specific layout of the content will be suitable.
- Renewal. It is good to check how often the content offered is updated. The digital security domain changes all the time and it is important that new insights are included in the training in time. It is also important that the offering remains suitable with your organisation's look.
- Sector-specific content. Some suppliers have content available that focuses on specific sectors.

Live training

Apart from digital training, live trainings can also be presented in the framework of awareness and behaviour. These are training courses presented by trainers, sometimes on site and sometimes remotely (via a digital learning environment).

This often concerns tailor-made training courses. Depending on the specific challenges or risks that an organisation has, certain themes could be highlighted during such training courses Most live training is presented to groups and supplement existing digital training courses. Additional benefits of live training are that the interaction within the group could lead to useful insights and/or new solutions for the organisation

Serious games

Serious games are being used more and more during learning. The main purpose of these games is to educate and to make the learning experience pleasant. Such a game could for example be a board or card game, but it could also be a digital game. The game includes lessons about awareness and safe behaviour. Depending on the content of the game, certain aspects are emphasized.

Analysis of behaviour and culture

Social engineering tests

These types of tests focus on investigating the behaviour displayed by employees when they are confronted with a fictional threat. It investigates in which areas employees are currently vulnerable, so that appropriate measures can be taken based on the results.

Examples of social engineering tests are:

- Phishing. During a phishing test, an employee is seduced to supply confidential information. This could for example be via an e-mail, but also via telephone or chat. Many service providers have digital platforms available for phishing tests via the mail with which you or they can send fictitious e-mails to your employees. In the case of phone or chat phishing, an employee of the service provider is used to pretend to be someone else and try to persuade the employees to share confidential information.
- Mystery guests. When deploying a mystery guest, someone tries to penetrate an organisation without being authorised to do so. This concerns, for example, passing through security unseen and entering areas that should not be accessible to guests.
- Red teaming. In a red teaming test, the red team tries to get as close as possible to the ‘crown jewels’ of an organisation. This often means a combined approach in which, on the one hand, attempts are made to physically enter a building without the correct authorisations and to digitally break into the organisation’s systems. The purpose is to identify the areas in which the organisation is vulnerable for a digital attack.
- Passwords check Unfortunately people still uses passwords that too easy to “guess”. People often do not realise that hackers can crack passwords faster based on common patterns than with the use of a brute force method (in which all possible options for a password are tried. If employees use words in their password that appear in the dictionary or, for example, the company name and then change certain letters into numbers, a password is easy to crack. A password check examines how many passwords can be cracked quickly and which patterns in the passwords often occur, so that advice can be given based on this for improving the passwords used within an organisation.

Conducting research into cyber-safe behaviour in an organisation.
There are roughly two methods to measure the current cyber-secure behaviour of employees in an organisation:

- Qualitative research
- Quantitative research

Qualitative research focuses on descriptions and is used to understand thoughts and experiences of employees. An example of qualitative research is conducting interviews or setting up focus groups. Qualitative research is especially suitable for conducting exploratory research and delving deeper into people’s personal experience. However, the interpretation of qualitative data is subjective, and the data can be influenced by undesirable factors, such as who the interviewer is and the extent to which questions are asked during an interview. Qualitative data is also often limited, because only a small portion of the target group is surveyed. Answers given by this group are not necessarily representative of the entire target group. Nevertheless, qualitative research does give a first impression of what is going on within a target group and, due to the personal approach, important issues can arise that might otherwise remain underexposed.

Quantitative research focuses on numbers and is used to get as objective a picture as possible of a situation. An example of quantitative research is a questionnaire. Quantitative research is less sensitive to subjective interpretation of data, is easy to conduct among a large target group, and is easy to replicate if you want to identify the same subject again. However, quantitative research provides limited information about an individual’s experience, and specialist statistical knowledge is needed to analyse quantitative data. Moreover, when it comes to factors that are difficult to measure, such as knowledge, motivation, and behaviour, this requires specialist knowledge about psychometrics.

A combination of the two research methods, a mixed methods approach, combines the advantages of both methods and is therefore often preferred.

When setting up (qualitative and quantitative) research, it is wise to consider the following questions:

- What do you want to measure? Cyber-safe behaviour consists of several themes. Some providers focus specifically on identifying a single theme, such as phishing. Others look more broadly at, for example, email usage, password management and incident reporting. The more themes that are included in a study, the better the understanding about cyber-secure behaviour in an organisation. It is also important to think about which data is valuable, for example about the actual current behaviour, the level of knowledge about certain topics, what employees find important, etc.
- Who do you want to measure? Who will participate in the study? To get as complete a picture as possible of the behaviour within an organisation, it is wise to include all (groups of) employees in the survey. The more people from a target group participate, the more accurate the picture that the survey provides.
- How do you want to measure? In quantitative research into cyber-safe behaviour of employees, objective data (such as the number of downloads of illegal software) is often limited. Instead, survey questions can be formulated, such as statements and multiple-choice questions. Usually these are so-called self-report items: people indicate how they behave, feel, or think about certain topics. When a provider has sufficient expertise about psychometrics in-house, self-report items are a good alternative to objective data.
- Why do you want to measure? It is important to determine in advance what the research data will be used for. If it is used as a baseline measurement, it is good to discuss this in advance with the provider so that this is considered in the research layout. The research layout mostly determines the usefulness of the data afterwards.

Service providers in this area have experience with all these aspects and can advise on a suitable approach and provide examples of effective measurements that they have performed before.

Behaviour interventions

Behaviour intervention program based on the organisation context

Knowing what you must do does not necessarily meaning that you are doing it. That is why it is important to first understand which factors of behaviour you can control as an organisation. Psychological theory says that behaviour consists of three factors:

- Capacity – does someone have enough knowledge to show the requested behaviour?
- Motivation – does someone want to display the desired behaviour?
- Opportunity – is someone able to display the desired behaviour?

To change behaviour, the interventions that are used must activate employees on these three factors: by learning, motivating, or facilitating. It is important that each intervention is tailored to the specific needs of a target group. To achieve the same desired behaviour, it may be necessary to deploy different interventions for different target groups. For example, if a lack of knowledge is identified as a barrier to the desired behaviour of a certain target group, a lecture can be used that emphasizes knowledge transfer. When it comes to a lack of motivation, the approach of the same lecture may be motivation, or a completely different intervention that motivates employees. Or you can opt for an intervention that basically forces the behaviour so that employees no longer have a choice.

Examples of possible interventions that based on the organisation context are:

- Social engineering
- Roadshow
- Reading
- Ambassadors
- Serious Game
- Educational session
- Hack Demo
- InterVision groups
- Event with a competitive element
- Escape room

Culture programs

Analysis of safety in relation to the existing organisation culture

Before working on a safe organisational culture, it is necessary to gain insight into the current organisational culture and identity of the organisation. This includes important underlying standards and values, the (example) behaviour and the vision of employees and management.

Insight into this can be obtained by means of a survey throughout the organisation, interviews with employees, field research (observing behaviour in practice) and/or desk research.

Intervention program for culture change

Based on an analysis of the current culture, it is important to determine what the desired culture is and what is needed to achieve it. This could be formulated in an intervention program for culture change. Elements that could be included in this are:

- Repetition of important messages, so that the need for cyber-safe behaviour is more firmly established.
- Promoting target behaviour by addressing social influence. Target behaviour is, for example, an employee addressing visitors without guidance or badge, locking a screen when leaving a workplace or addressing colleagues about visibly undesirable behaviour. A cyber safe culture is enhanced by stimulating social influence.
- Using informal/formal leadership in communicating and propagating the importance of a cyber-secure organisational culture.
- Working on visibility and accessibility of security within the organisation. Think for example about the visibility of the cyber security team, the way the help desk communicates about this topic, involvement of management, etc.

Activities to secure the safety culture

Various activities are conceivable for perpetuating the culture. Apart from the importance of repeating the message, this could also mean:

- Communication training for target groups that are actively and reactively involved with cyber security (IT helpdesk, communication, management, HR department) and how to make this part of daily work.
- Campaigns for promoting a safe reporting culture
- Communication about desired target behaviour (e.g., infographics, short videos with explanations, articles on intranet, newsletters) and addressing colleagues.
- Technical support of target behaviour (e.g.: report phishing button, password manager).
- Security ambassador training/education that offers permanent support.
- Have the CEO/director pay constant attention to the subject in communications, sometimes more implicitly, other times explicitly.

Consultancy

Advice about organisation-specific problems

Depending on the specific context of an organisation, there could be questions that require a tailor-made approach. In that case, service providers can provide advice applying the service provider's knowledge in the context of an organisation.

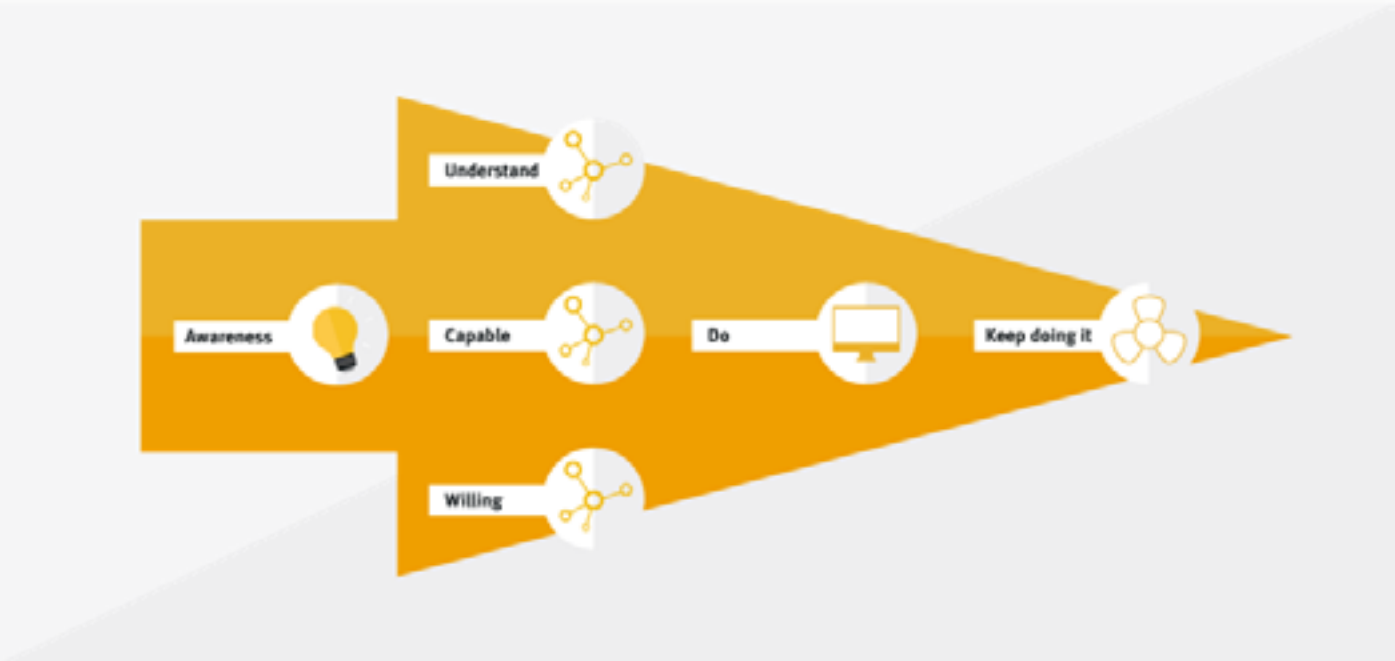
Appendix

The Balm model

Reference:

- **Exercise Therapy and Behavioural Change (Balm, M.F.K., Purdue University Press, 2002)**

The Balm model explains how people achieve cyber-safe behaviour. It starts with awareness: “Why is cyber security important to our organisation?”. Employees must then understand what this means for their own behaviour (‘what knowledge, skills do I need?). The organisation must facilitate cyber-safe behaviour, also technically. And ultimately, people must also want to exhibit cyber-safe behaviour themselves, in which leadership and exemplary behaviour of important and visible players, such as management, for example, play a major role. If these four preconditions are met, people will also move towards cyber-safe behaviour. Subsequently, the organisation must also maintain this behaviour in order to guarantee a cyber-safe culture in the long term.



The Behaviour Theyory of MacInnis, Moorman en Jaworski

Reference:

- Exercise Therapy and Behavioural Change (Balm, M.F.K., Purdue University Press, 2002)
- Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads (MacInnis, D. J., Moorman, C., & Jaworski, B. J., Journal of Marketing, 55, 32-53, 1991)

The behavioural theory of MacInnis, Moorman & Jaworski (1991) states that behaviour can be seen as the result of three factors: motivation, capacity, and opportunity. In other words: does someone want to do it, is he able to do it and does he get the chance to do it?

- Capacity The extent to which a person can display certain behaviour, given his or her characteristics, skills, knowledge and instruments.
- Motivation Does a person want to display the behaviour; what goal does a person find important?
- Opportunity The extent to which the circumstances promote or hinder the behaviour. For example, physical conditions, social conditions, and technology.

If all three these factors are adequately present, behaviour will take place. If one of these factors is (partially) missing, the chance of behaviour is much smaller. Dividing behaviour into these three components increases insight into the measures an organisation can take to achieve certain desired behaviour. The insight that behaviour consists of multiple components makes it clear why awareness programs often do not lead to the desired result. Awareness concerns knowledge and capacity. The fact that behaviour does not occur due to a lack of knowledge is thus an assumption. It may just as well lack motivation or opportunity to exhibit the behaviour. It is therefore relevant to investigate, prior to devising or implementing an intervention, why certain behaviour does not occur or occurs minimally.

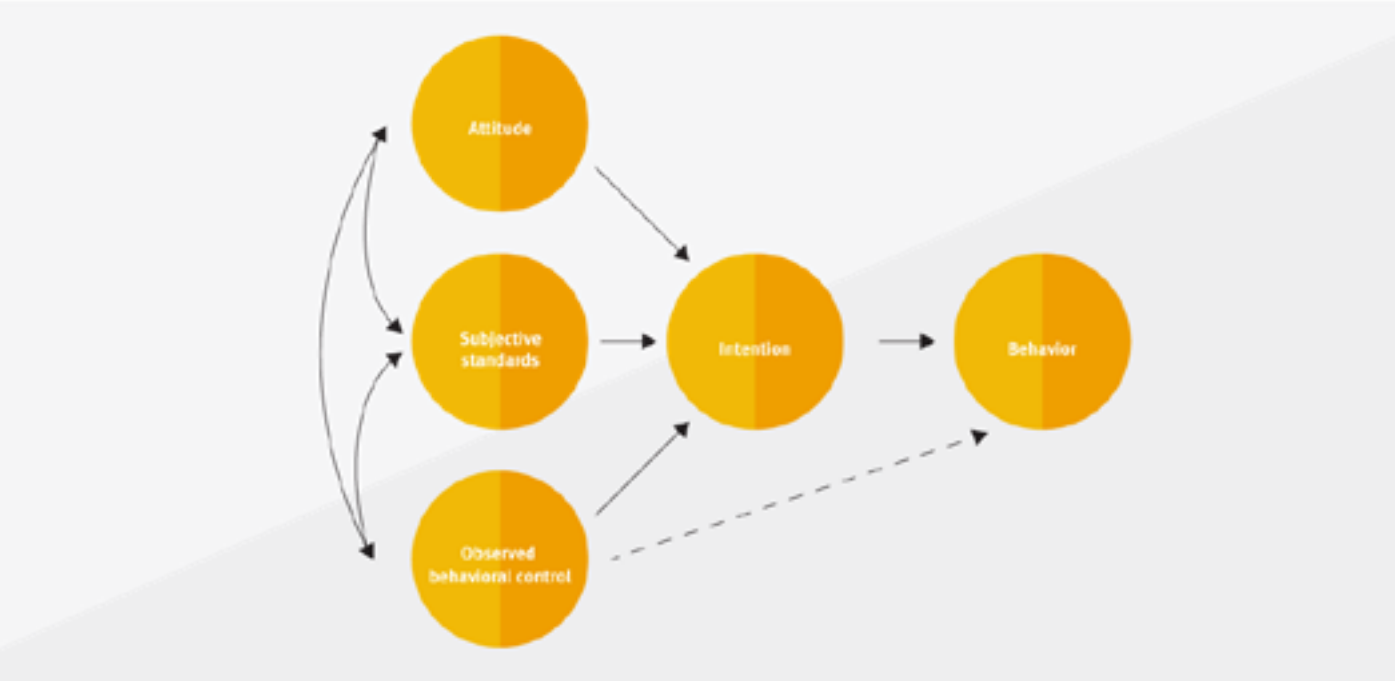
Theory of Ajzen

Reference:

- Attitudes, personality, and behavior (Ajzen, I., 2nd Ed., Milton-Keynes, England: Open University Press, McGraw-Hill, 2005)

Ajzen's theory (theory of planned behaviour) states that conscious behaviour arises directly from the intention to perform the behaviour. According to Ajzen, the intention is determined by three elements:

- Attitude. The attitude concerns a person's feeling about the behaviour. When the person has a positive attitude toward the behaviour, the person is more likely to consciously engage in the behaviour.
- Subjective norm. The subjective norm is about what the person thinks others – in his immediate environment – think of the behaviour (to be performed) and how they judge it. When the person thinks that other will consider the behaviour to be normal or good, the person is more likely to consciously engage in the behaviour.
- Perceived behavioural control. The perceived behavioural control concerns the extent to which the person believes that the behaviour is easy to perform. This concerns both one's own skills and the environmental factors that promote or hinder the behaviour. When the person believes that behaviour is easy to perform, the person is more likely to perform the behaviour consciously.



Persuasive by Design Behaviour Change Model

Reference:

- Persuasive by Design, Behaviour Change Model (R. Renes, S. Hermsen , Draaiboek gedragsverandering, 2017)

How do you ensure that your campaign has the intended behaviour-changing effect? Behaviour is complex and covers various aspects. By asking questions during the design process and providing ideas for intervention strategies in your design, the behavioural lenses help you focus sharply on the behaviour of your target audience. The various 'lenses' provide insight into, among other things, how you can influence automatic facets of behaviour, how your target group views the target behaviour and what the motivation of the target group is.

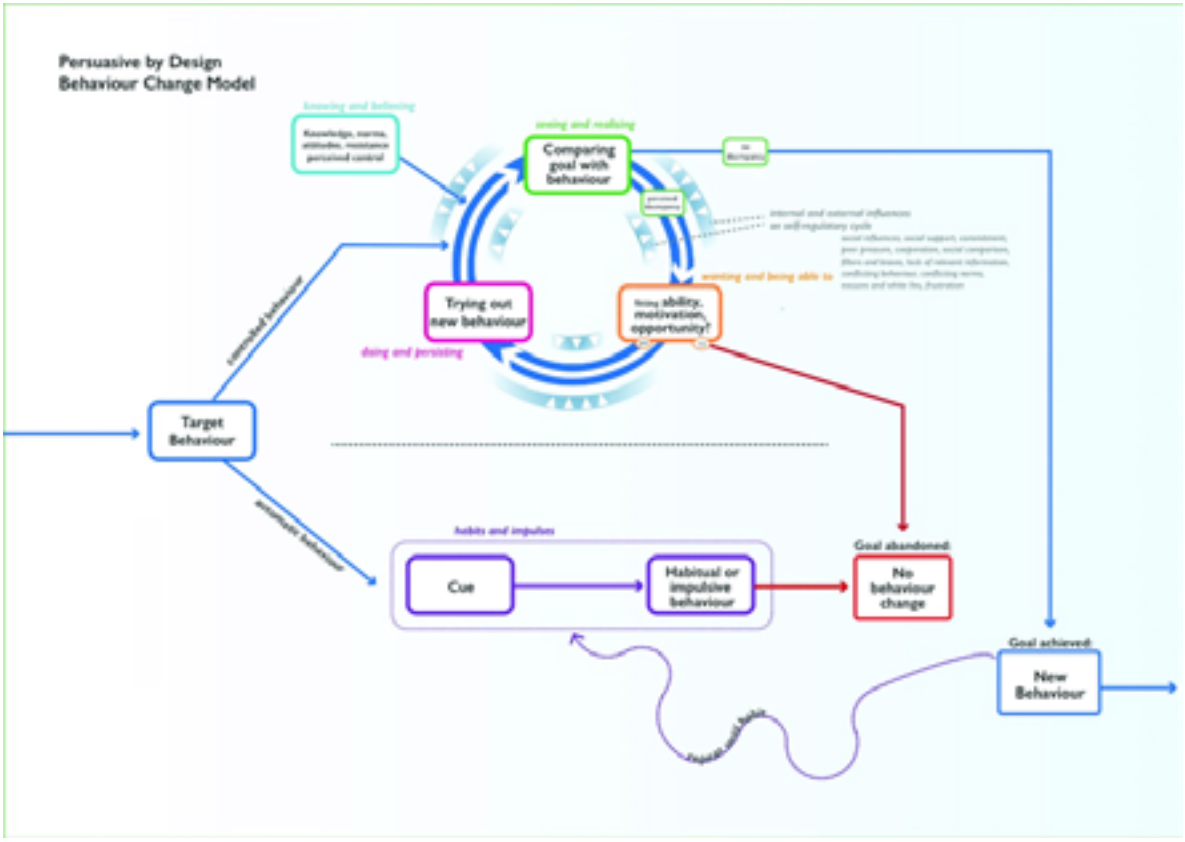
- Lens 1: Habits and impulses. A large majority of our behaviour is automatic. We do not think about it. It can consist of reflex impulses, but also more or less deeply engrained habits. Use this lens to see whether the target behaviour of your target group has automatic aspects and how you can influence it.

- Lens 2: Knowing and finding. The desired behaviour does not always correspond with the will and the options of the target group. Use this lens to see what knowledge the target group has of the target behaviour. Investigate what the target group thinks of the target behaviour, for example whether they feel resistance to it.

- Lens 3: Observe and understand. Target groups are not always good at observing their own behaviour. Use this lens to see whether your target group is well able to perceive the difference between its own behaviour and the target behaviour. Also investigate if they need help with this.

- Lens 4: Want to and can. Behavioural change is only really possible if there is sufficient motivation, and the right skills are available. Use this lens to see whether the target group is sufficiently motivated to change the behaviour, whether they have the right skills to do so and whether they are given the opportunity to perform the new behaviour.

- Lens 5: Do and continue to do. To arrive at new behaviour, it is necessary to try out the desired behaviour in feasible steps and to continue to apply it. Use this lens to see how easy and attractive it is to try out, repeat and maintain the new behaviour.

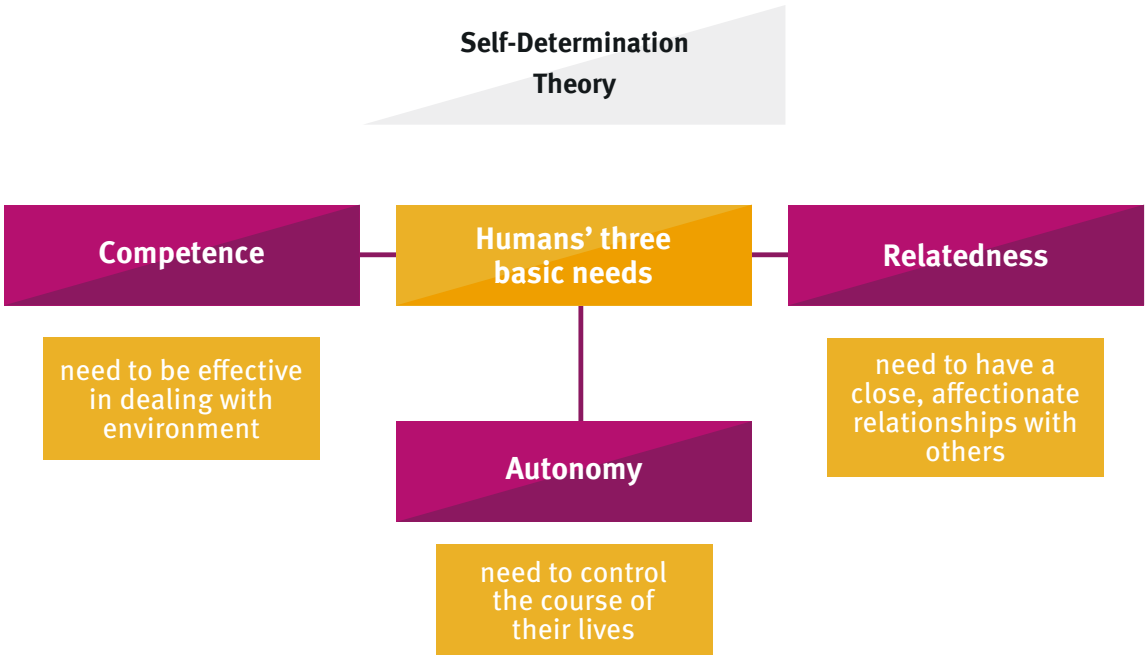


Self-Determination Theory

Reference:

- Self-Determination Theory (Deci & Ryan, 1985; 2000)

This theory states that three innate and universal psychological needs can increase intrinsic motivation, which makes people want to grow and change. If the three basic psychological needs of autonomy, competence and relationship are addressed, this will have a positive effect on intrinsic motivation.

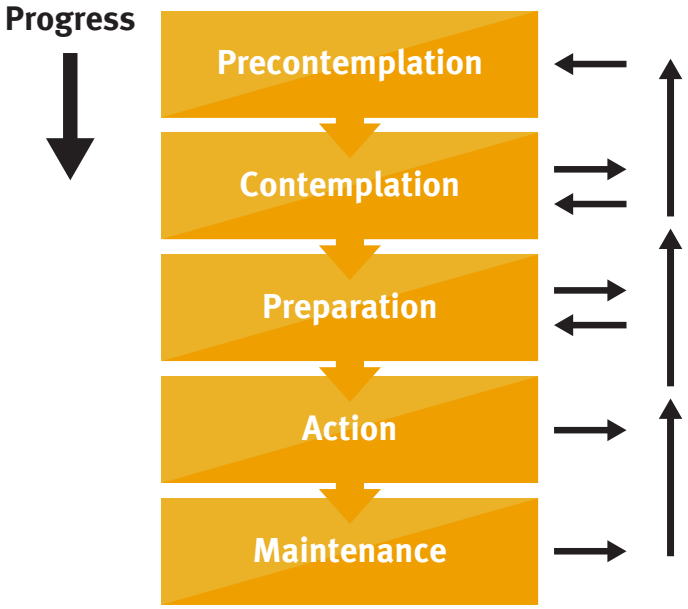


Transtheoretisch model

Reference:
- Transtheoretisch model (Prochaska & Di Clemente, 1982)

The transtheoretical model, also known as the circle of behavioural change, provides insight into which steps are taken in a change process. The change process is shown in a circle of six steps. The theory states that behavioural change is not a linear process (with a clear start and end point), but a circular process. During each phase, the person may revert to a previous phase or old behaviour.

The six steps in a row are:
- Precontemplation: on this level there is no intention to change (yet). The person is often not aware of the problem.
- Contemplation: here the person is aware that there is a problem. The motivation to do something about it is there, but the person has not yet taken any action.
- Decision-making (preparation): at this level, the person makes real plans to do something about the behaviour.
- Action: here the person takes action to change the behaviour.
- Persistence or consolidation: at this level, the person tries to perpetuate the change achieved and not fall back into old habits. The new behaviour must find a place in life and be integrated with other activities.
- Fall back: in most cases, the person is unable to fully retain the achieved situation from the first attempt. Fall backs are regular and the process starts over.



The Communication Activation Strategy Instrument

Reference:

- Het CASI-model (zie https://www.communicatierijk.nl/vakkennis/casi/documenten/publicaties/2019/03/08/handleiding-casi, 2020)

The Communication Activation Strategy Instrument (CASI) model was developed by the Public and Communication Service of the Ministry of General Affairs and is used by ministries, among others, to develop effective interventions for behavioural change. CASI is a step-by-step method for applying insights from recent scientific research to the practice of behavioural change.

The main underlying principle of CASI is that you start with a clear analysis before coming up with a solution or intervention. In this analysis you determine what the desired behaviour is, who the target group is and what the current situation looks like.

You then deepen your analysis by investigating which factors influence the desired behaviour, the so-called 'behaviour determinants'. Behavioural determinants are factors that make the desired behaviour easier or more difficult. These can be factors in the (digital) environment (such as the user interface), factors in the social environment (such as norms and exemplary behaviour), factors relating to knowledge and skills, but also psychological factors (such as resistance or risk perception).

Based on this analysis, you select the most promising strategies to stimulate the desired behaviour in your target group, given your target group and associated behavioural determinants.

In addition to this step-by-step method, CASI offers a check list of ten concrete, evidence-based tips for behaviour change:

- Keep it simple
- Make it personally relevant to people
- Create something people want to see
- Let people see good behaviour
- Show people and situations that are recognisable
- Give your target group concrete instructions
- Prevent resistance
- Use the social environment of your target group
- Communicate where the behaviour takes place
- Keep it up for a long time and repeat.

CYBERVEILIG NEDERLAND

Contact
E-mail: info@cyberveilignederland.nl
Telephone: 088 - 118 25 10