Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Beyond e-learning

Guiding principles for achieving cyber-secure behaviour in your organisation

Introduction

Our aim in this publication is to offer you guiding principles to help you promote cyber-secure behaviour among the employees in your organisation. Knowledge about cyber attacks is an important part of achieving this aim, but it is not enough. Improving cyber-secure behaviour in your organisation calls for more than an awareness campaign or a mandatory e-learning module. Do you recognise this in your workplace? And are you keen to make improvements that are effective? This guide will help you reach that goal.

Target group

This publication on promoting behaviour that supports information secure behaviour is for the CISOs of organisations covered by the Cybersecurity Act (NIS2 Directive), who know they need to do more than launch awareness-raising campaigns to achieve this goal, and who are keen to find out more about the strategies employed by cyber-resilient organisations. In addition, this publication is relevant for the directors and managers of organisations who want to develop an integrated approach to cyber-secure behaviour.

This publication was created with contributions from

ASML, DWG, Digital Trust Center, Eneco, Secura, SURF and Leiden University.

We also received welcome input from Avans University of Applied Sciences and Saxion University of Applied Sciences.

Contents

Background

Using the principles we offer you in this publication, you can build your own programme for cyber-secure behaviour. This is essential because cyber-secure behaviour is a key component of your cyber resilience. The risk of accidents can never be ruled out. Stress and fatigue are often to blame, but lack of support from the organisation and technological measures also play their part. Unsafe behaviour is rarely deliberate; more often than not, it is a side effect of action taken to save time or simplify working processes. Unsafe behaviour can have serious consequences for the information security at all kinds of organisations. For example, leaving a laptop unattended can result in a data leak or using your own devices on the company network can increase the attack surface. Attackers are aware of these weaknesses and exploit them using a range of manipulation and deception techniques.

So how do you promote safe behaviour? There is no one-size-fits-all solution. What works for you will depend, among other things, on the type of organisation, the products or services you provide, and how the world around your organisation operates. In other words, what works for you may not necessarily work for another organisation. And what generates resistance within your organisation may not be an issue somewhere else.

We know from research and practical experience that awareness and knowledge acquisition alone do not necessarily result in safe behaviour.[1] However, this does not mean there is no sensible action you can take. From discussions with a range of organisations, NCSC has distilled a number of guiding principles that apply to almost every organisation. Applying the principles in this publication equips you with the building blocks for an effective behavioural programme. It enables you to work on a customised programme that contributes to cyber resilience throughout your organisation.

This publication offers tools for establishing cyber-secure behaviour in your organisation that is both effective and structural. In doing so it supports the goal envisaged by the Cybersecurity Act (NIS2 Directive).

In this publication, we feature six guiding principles; each principle is divided into a further set of recommendations. Through a number of case studies, we show you how to apply these guiding principles in practice. The cases are all based on real-life situations.

What is secure behaviour?

Cyber-secure behaviour involves recognising, avoiding, countering, reporting and minimising risks to information security.

Secure behaviour is an interplay between knowledge, social norms, organisational-cultural aspects and strategic, tactical and operational support within the organisation.

Cyber-secure behaviour is part of your organisation's integral security, which encompasses physical security, social security and information security. Each of these aspects influences the other and they can therefore not be seen as separate. Given the scope of this publication, we will limit ourselves to the subject of cyber-secure behaviour.

1. A measured approach

An organisation may undertake all kinds of activities to promote safe behaviour but unless it measures their effect, it will never know whether or not they actually make a difference. A measured approach is therefore essential. What does this mean in practice?

Start by setting a baseline

Only when you know what challenges your organisation currently faces can you identify opportunities for improvement in cyber-secure behaviour. Starting a behavioural campaign without a baseline value is a bad idea. For example, ask yourself whether awareness is the challenge facing your organisation or whether the challenge lies elsewhere. It is important to note that measurement does not

[1] See, for example, research on the effectiveness of e-learning: Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, 103585.

always have to be quantitative. Dialogue with employees, managers and process owners can also offer a clear insight into where you stand. One pitfall definitely worth avoiding: using phishing tests to measure secure behaviour. Even with the best of intentions, phishing tests are more likely to measure how good the phishing email is than the secure behaviour of your employees.

Understand the underlying problem

Once you have a clear understanding of the organisation's challenges in terms of cyber-secure behaviour, you can see which problem needs to be solved. Is unsafe behaviour a motivational problem? A knowledge problem? Is it the byproduct of a heavy workload? Or is there an underlying technical problem? We often see organisations coming up with a solution ('We need e-learning!') before they are clear about which problem they need to solve.

Achieve clarity before you bring in a supplier

Wait until you are clear about what problem the organisation wants to solve before you consider bringing in a supplier. Decide what you can do yourself and what you need to outsource. Be thorough when you ask a potential supplier to explain the solution they are offering: is it really the solution to your problem? Not only that: also ask them to clarify in advance how they plan to measure the effects and experiences they are promising. Be wary of suppliers who are not willing to play a role in measurement or who hide behind previous measurements carried out at other organisations.

Assess and measure your interventions

Whatever form your programme takes, you want to know the results. Your organisation is eager for that information too. So it's important to measure, even after the intervention. This helps you understand the effectiveness of your approach, discover areas of resistance and make adjustments where necessary.

2. Let your risks be your basis

Behavioural programmes are more successful when they are risk-driven. In other words, your behavioural programme is closely linked to your risk management. What does this mean in practice?

Risk analysis as a starting point

Risk analysis shines a light on what is keeping managers and directors at your organisation up at night. It provides a deeper understanding of the interests to be protected and the possible threats to those interests. You can also use risk analysis to clarify your level of resilience to cyber threats.[2] This type of analysis also highlights the risks associated with unsafe behaviour, from the boardroom to entry-level employees. Identify these risks and take them as a starting point for your behavioural programme. But remember: investing in safe behaviour is not the first step in mitigating risks. Start by taking a closer look at your policy and your technology and then think about the contribution that investing in safe behaviour can make.

Take risk appetite into account

Some cybersecurity risks are more relevant to your organisation than others. One important factor to consider is the risk appetite of your board or management team. Think carefully about which risks you want to include in your behavioural programme. It is sometimes better to mitigate risks by taking technical or organisational measures. Motivating your staff to come up with unique, unbreakable passwords is good, but it's better to invest in a validated password manager and multifactor authentication which employees are required to use. Be realistic about what you can and cannot solve through behaviour (take a closer look at the lessons to be learned from behavioural science, see also Section 4). In addition, remember that behaviour doesn't always have to be about prevention. Information security incidents or cyber risks that are difficult to address using preventive behaviour may well be tackled in other ways. These might include responding to incidents, timely reporting or disconnecting systems.

Persevere and grow flexibility

Promoting safe behaviour is a long-term commitment. Complying with standards or frameworks can be a good starting point, but your behavioural programme

[2] NCSC-NL has published several guides on risk analysis. You can find them on our NIS2 theme page.

will be more effective if it is risk-driven. This makes your behavioural programme more flexible; risks are not static, they evolve through time.

Case study: Focus on risk

A major organisation in the Netherlands wants to launch a behavioural programme. Their previous attempt at awareness training failed to deliver the desired results. Analysis showed that employees did not pay much attention to the online learning environment and the majority thought the topics were too general. The CISO decided to take a different approach. The board had previously carried out a comprehensive risk analysis covering about twenty scenarios that could seriously harm the organisation. The CISO, in consultation with the board and managers from various departments, came to the conclusion that not all risks can be addressed through behaviour. However, behaviour seemed relevant to five of these scenarios, three of which they identified as urgent: attention to unauthorised access, secure transmission of confidential data and handling customer data in CRM software. The CISO and her team come up with input for the new behavioural programme in collaboration with managers from the various departments. They focus primarily on these three scenarios and consulted a behavioural scientist to help them develop interventions. One idea is to organise face-to-face interactive sessions to discuss the risk of unauthorised access and practise the desired behaviour. This idea was put forward by one of the team leaders. The session proved to be effective, though it also became clear that it needs to be repeated at regular intervals.

3. The entire organisation needs be on board

Cyber-secure behaviour involves everyone. There was a time when we automatically looked to the IT department if anything happened in this area, but we now know that creating a cyber-resilient organisation is a collective responsibility. What does this mean in practice?

The board initiates the dialogue

The board of directors needs to actively convey the importance of creating a cyber-resilient organisation. You need to explain that this is not simply the responsibility of the IT department, but that awareness and the right behaviour needs to be in place across the organisation. When the dialogue about cybersecurity is initiated at boardroom level, the organisation cannot ignore its importance.

As a manager, open the discussion on cyber-secure behaviour

It is not just the CISO and the board of directors who need to work to make cyber-secure behaviour a reality, but everyone in the organisation. With this in mind, talk in your team about what safe behaviour entails. Make it concrete and specific: what is the current situation in your team and where do your employees need support? Make agreements with each other: what targets will your team work towards?

Help build a learning organisation

Preventing cyber incidents is a noble goal, yet they can still happen to the best of us. When they do, it's always a shock but if you don't learn from these incidents as an organisation, in a worst case scenario they will not only cost you a lot of money but all that trouble will also have been for nothing. Turning an incident into a learning opportunity can lead to a different way of working or a technical solution, for example, which in turn will prevent the same incident from happening in the future. Avoid penalising employees who report a cybersecurity incident. If you come down hard on them, it makes them less likely to report which in turn increases the risk of incidents not being detected on time. So be sure to create a culture where learning is the norm and there is room for constructive dialogue. Emphasise the positive side of incidents. Of course, that's not the same as cheering them on. What matters is that we shake off the taboo attached to causing incidents, and reward reporting instead. A secure workplace is the number one priority.

Lead by example

As a director, have you ever fallen for a whaling attack? If so, set a good example by being open about what happened. Tell your fellow directors and explain what the organisation can learn from such an incident. After

all, you want employees to report all incidents, right? In addition, lock your laptop when you leave the room, store data carriers securely, and make sure that the security rules (verified password manager, multifactor authentication) apply to you as well as everyone else.

Make safe behaviour part of staff development interviews

Make cybersecurity a recurring topic in your staff development interviews. This is another chance to show that you want to be a learning organisation. Bring up the topic, for example, in a conversation about working to improve cybersecurity as opposed to productivity and chasing short-term goals. It's an approach that enables management to gauge whether employees are sufficiently facilitated to act in ways that boost safety.

4. Let behavioural science work for you

Behaviour is complex. We are not the rational beings we think we are. The field of cyber resilience in particular has benefitted from the latest insights from behavioural science in recent years. Make use of the knowledge that is already available. What does this mean in practice?

Apply insights from behavioural science

Most CISOs are not specialists in human behaviour. This is an area in which you probably need to enlist expertise: expertise that combines knowledge/research from sociology, anthropology and psychology into findings that can shape the cyber-secure behaviour you are aiming to achieve in your organisation.

Check whether products and their experts make use of behavioural science

Behavioural science offers valuable insights into how to promote safe behaviour. It is essential that the products you purchase and the experts you hire base themselves on the latest knowledge of how the human factor influences cyber-secure behaviour. Ask the suppliers of products designed to promote safe behaviour about the expertise behind their product: what behaviour-based insights have they incorporated? And how can they demonstrate this? For example, have these insights led to any recent changes in the product or service? Is this supplier's knowledge up-to-date, especially in this area?

People are the solution

The people in your organisation are your most important asset. Without them, the work simply doesn't get done. While people are often portrayed as the 'weakest link' in the cybersecurity chain, it makes more sense to see them as the 'final link' in that chain. Cyber resilience is all about the human element.

Case study: Phishing email

Should a director participate in an organisation-wide phishing test? There are still directors who believe they don't need to: after all, a management assistant handles their emails and when they do answer an email personally, they are convinced that they would never fall for a phishing email. A missed opportunity! It implies that clicking on a suspect link is something that could never happen at directorship level, when in fact it can happen to anyone. What matters is how you respond as an organisation and how and what you learn from such an incident. That's so much more important than sending the message that you would never fall for a trick like that. As a director or manager, you are also a role model.

Insights from positive psychology teach us that a shift in your thinking or attitude towards your employees is key in motivating them to behave more securely.[3]

Empower people

A vital starting point in cyber-secure behaviour is therefore exploring ways to empower the people in your organisation. How do you incentivise them to act the way you want them to? Give people the feeling that they are making a difference. They are part of the solution, so make them feel involved.

[3] Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187.

Another insight from positive psychology: use positive case studies that emphasise the importance of the human factor. They appeal to people and are good for motivation. In other words, avoid phrases like '20 per cent of our staff don't lock their laptop'. Accentuate the positive instead: '80 per cent of our colleagues lock their laptop when they leave their workstation for a short time.'

5. Customisation is key

Promoting safe behaviour means different things in different situations. Organisations operate in specific contexts, employ people from different backgrounds and face a variety of challenges and risks. Moreover, keeping a watchful eye on information security and cybersecurity is not the only task in your employees' busy schedules. If you want your behavioural programme to be effective, customisation is absolutely key. What does this mean in practice?

Connect with your employee's point of view

There is no such thing as a 'typical employee'. Employees come in different shapes and sizes. These differences encompass everything from cultural differences to various roles and functions. Moreover, the information security risks within teams vary considerably. A keen awareness of diversity is important, including employees who are neurodivergent. The human brain is not a standard instrument; people's drives and motivations differ. An HR employee encounters an entirely different set of risks from someone who works at the IT service desk. They each have their own information needs due to the specific context in which they work. On the whole, generic campaigns tend to have little impact. Customise your information: make it concrete and specific to the target group you are dealing with. An IT department responsible for managing systems and login portals needs knowledge, skills and understanding of the importance of multi-factor authentication and security-by-design principles. For an HR department, emphasising the safe handling of employees' personal data by facilitating secure email practices may well be a good idea.

Bear this in mind and always consider how the form and content of the behavioural programme suit the employee you are dealing with. Involve your target group in the design and implementation of your programme.

Emphasise skills

Many behavioural programmes focus on imparting knowledge and seek to raise awareness, but knowledge and awareness do not automatically translate into behaviour. Knowledge about information security and recognising cybersecurity risks are important because they tell you something about the need to act securely. But achieving security takes more than that. Ask yourself what skills your employees need to turn that knowledge into action and how they can master these skills. Think about how employees in your organisation can ensure that company confidential information is handled securely. This can range from using a secure platform to exchange files (encryption), and storing confidential documents or laptops in a safe, to reporting a possible leak to the person(s) responsible. Integrate these actions and skills in working arrangements and processes, and use incidents as an opportunity to learn how to do things better.

Case study: Boardroom dilemma session

How can we make cyber resilience come alive at boardroom level? This question prompted the security department of a company in one of the Netherlands' vital sectors to organise a dilemma session for its directors. Instead of addressing the possible consequences of a cyber attack with the aim of increasing knowledge, they decided to take a different approach. The directors were presented with three scenarios, all of which involved consequences for the directors' respective portfolios. Among other things, this resulted in an interactive dialogue on dilemmas, as opposed to a 'one-way session' in which the security department provided information. They took a subject that was often considered abstract and remote and gave it a practical sense of immediacy, with insights into the organisation's crown jewels, critical processes, risk preparedness and possible consequences for the functioning of the organisation as a whole and the directors, both individually and as a team, in the unfortunate event that a cyber attack spirals into a crisis.

Keep things clear and understandable

People's working days are usually busy enough. Information security is by no means the only issue competing for your employees' attention. Focusing on cybersecure behaviour comes in addition to their

regular work. It's important to realise that. Be careful to select the knowledge, information and associated behaviours that are really important for your organisation. Less is more: for example, pick three to five points with a need for behavioural change. Offer support simply, positively and accessibly to make sure that you don't burden employees unnecessarily.

Case study: Diversity in behavioural programmes

An international robotics company employs professionals in Europe, America and Asia. The company attaches great importance to encouraging employees to report information security incidents as soon as possible. One way to lower the reporting threshold was to introduce a simple report button in the email environment. Diversity among cultures was another specific focus of attention. In Europe, there is a strong emphasis on motivating employees by reminding them that they are part of the solution when they report an incident rapidly. In America and Asia, this approach proved to be less effective. In these cultures, it made more sense to prioritise removing fear of reprisals and make clear agreements with management on how incidents should be dealt with.

6. A continuous and integrated process

A behavioural programme is not a one-off initiative. Working on behaviour is an ongoing and integrated programme of change. By involving a range of organisational units, you increase the chances of your programme being effective. What does this mean in practice?

Build on what you've already got

Thinking about how to encourage positive behaviour and discourage negative behaviour is usually nothing new. It can apply to everything from safely operating machinery or equipment to using the stairs or evacuating a building. In most cases, the CISO is not a behavioural expert and cannot possibly have detailed knowledge of every unit in an organisation. It therefore makes sense to build on existing programmes and interventions, and integrate secure working practices for information and IT. Invite input from organisational units where information security and cyber risks call for a specific approach. Take steps to ensure that security and how it relates to behaviour is discussed in an integrated setting, for example by bringing together relevant security staff on a monthly basis and learning from each other.

The power of repetition

Manage this process in such a way that you keep your employees alert, without overloading them. Only offer information and training in a form that is relevant to the employee's experience and point of view. Prevent resistance by honing your approach to suit your target audience. At the same time, it's important to remember that behaviour doesn't change overnight. Practising and testing skills, repeating knowledge input and regularly addressing risks will always be an essential part of steering your employees towards the secure behaviour you want them to demonstrate.

References

In these publications, we refer to the following publications/websites:

Publication	URL
Research on the effectiveness of e-learning	https://www.sciencedirect.com/science/article/pii/S0167404823004959
NIS2 theme page	https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/hoe-kan-uw-organiseren-zich-voorbereiden-op-de-nis2-richtlijn
Moving from a 'human-as-problem" to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169-187.	https://www.sciencedirect.com/science/article/abs/pii/S1071581919300540

Published by
National Cyber Security Centre (NCSC)
PO Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

January 2025