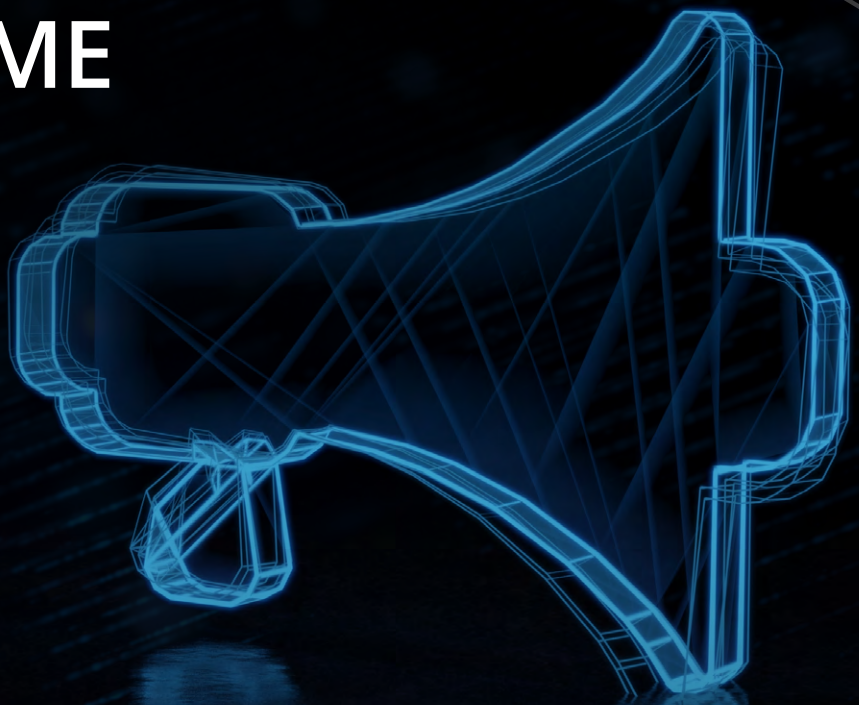
AR-IN-A-BOX

YOUR GUIDE TO DESIGNING A CYBER-AWARENESS PROGRAMME



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

CONTACT

For contacting ENISA please use the following details:
info@enisa.europa.eu

AUTHORS

Alexandros Zacharis, Dimitra Liveri, Georgia Bafoutsou, Marianna Kalenti (ENISA)

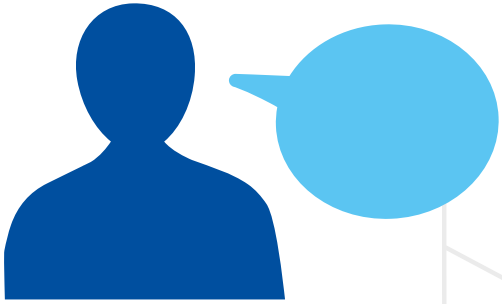
CONTRIBUTORS

Chloe Blondeau, Goran Milencovic, Theodoros Nikolakopoulos (ENISA)

LEGAL NOTICE

COPYRIGHT NOTICE

FOREWORD



This is a step-by-step guide for the design of a cybersecurity-awareness programme in your professional environment. The document presents all the necessary steps and relevant suggestions. However, it is important to note that each organisation should create their own tailor-made programme, by picking and choosing the proposals that suit their needs and recipients the most.

From programme to campaign

Within this document, there will be multiple references to both **programmes** and **campaigns**, which have different definitions in the context of awareness raising and can be defined as follows ([1]).

- **Programme.** A plan encompassing multiple awareness-raising activities over a long period of time (from several months to 1 or even 2 years), following the organisation's strategy for cybersecurity. It can include one or more internal or external campaigns, focused on a common cybersecurity topic or target group.

- **Campaign.** A set of individual and dedicated activities focusing on specific topics, goals or target audiences. A campaign may be stand alone or part of a programme.

1 In this report, the term 'roadmap' is used to refer to the visualisation of an awareness programme over a period of time.

STEP-BY-STEP PRESENTATION AND ANALYSIS

In order to create an **internal** cyber-awareness programme, tailored to your employees' needs, you need to follow the steps below:

- identify objectives;
- secure financial resources;
- ensure human resources (HR);
- split your employees into target groups;
- choose the right tools;
- create a time plan;
- implement the programme;
- evaluate the programme.

1. IDENTIFY OBJECTIVES

The first step in this process is to set the objectives of your cyber-awareness programme. These derive from the overall cybersecurity strategy of your organisation. Programme objectives are set on the basis of the SMART (specific, measurable, achievable, relevant and time-bound) ([2]) methodology, which can assist in creating a trajectory towards specific objectives that are clearly defined and attainable in the short and medium term. Those objectives will, in turn, determine the selection of the specific tools and methods that will be used for each programme.

Overall goals for awareness and learning

Definition of SMART awareness objectives

Selection of specific material, tools, methods

The awareness-raising objectives stem from the risk assessment of the organisation. Every organisation might set different objectives for its own awareness programme, yet some generic ones that are always applicable, and can easily be converted to SMART objectives, are the following.

- **To raise cybersecurity awareness** by showing the pervasiveness of cyber risks, promoting cyber hygiene and providing guidance on good practices for individual users.
- **To promote cybersecurity education and culture** within the organisation. This will help different entities of the organisation to identify the right communicating channels and common language to be used, in order to unite their efforts against exposure to threats.
- **To be prepared for incidents.** This will help the personnel identify the right order of actions to take, based on their role, and help the key actors involved in the event of a cybersecurity incident.

Other generic objectives can be:

- to develop an understanding of emerging cybersecurity threats and landscape;
- to promote cybersecurity culture and hygiene;
- to test policies and procedures (e.g. escalation, backup, incident handling).

2 https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-16_en_0.pdf

2. SECURING FINANCIAL RESOURCES

Prevention is less expensive than recovery when it comes to the damage that cyberattacks can cause. A common misconception is that low budgets devoted to security-awareness programmes are the only reason for the delivery of non-effective programmes. On the contrary, one can build very thorough cyber-awareness programmes with a low budget and limited resources.

Along with this guide, the aim of the AR-in-a-Box framework is to provide the basics for anyone to kick-start an awareness-raising programme from scratch, regardless of the resources available.

Before attempting to secure the budget for your awareness programme, you need to consider your organisation's overall approach to investing in cybersecurity awareness, along with its maturity in the field. Whether you are following a reactive v proactive, a benchmark or a risk-based approach, some part of your budget will be allocated to awareness.

The best approach to securing the budget is to come up with real examples and statistics of the money to be saved or the risks to be avoided (based on the risk assessment) – should the awareness training take place – and present this to the management. Collect data on incidents and breaches from your organisation, or similar ones, to justify the need for an awareness-raising programme.

In addition to the above, here are some rules to follow in order to regulate the budget needed and avoid overspending.

Management

They play the most critical role in the adoption and implementation of any awareness-raising activity. Based on their endorsement and support, the management can play a catalyst role in the viability of an awareness-raising strategy, so make sure they are involved in the design and the objectives-setting phase of the awareness programme from an early stage. Management vision can shift the scope of the strategy, based on their risk appetite. What is more, budget allocation depends on their support.

- Try to identify the must-do topics of your programme and the must-train employees who will minimise the risk for your organisation when trained.
- Reuse or update existing material or resources.
- Select open-source material or create it in-house.
- Exploit synergies in the community where available.

3. ENSURING HUMAN RESOURCES

The following roles have been identified as key for the success of any cybersecurity-awareness endeavour your organisation might pursue. They are all equally important and meet different needs and functions in the various life cycle phases of a cybersecurity-awareness strategy. Combined, they will form the cybersecurity-awareness team (CAT) of your organisation, even if you do not have staff occupying all the roles. The composition of CATs in organisations differ.

Cybersecurity officer

The security officer's insight and steering ability are paramount to the future of the strategy. The security officer is the one to provide input on the objectives and identify the target audiences and most relevant training topics, based on the needs but also the threats to which the organisation is exposed. The cybersecurity officer can assist in the design of a programme or undertake its overall supervision, in order to better control content development and customise it to the organisation's needs.

Public relations and communications

These teams play an important role in disseminating the right message internally and engaging the right target employee groups via the proper channels (innovative ideas reflecting the culture of the organisation might surprise you).

Information and communications technology (ICT)

The heavy weight of ICT maintenance and implementation or practical security always falls on the hands of the ICT department. Therefore, ICT should always be involved in awareness-raising activities to customise the content based on the operation reality of each organisation.

Incident response teams (security operations centres)

These teams are made up of operational experts that have a good overview of the vulnerabilities of the systems in place, but also monitor traffic and handle potential incidents. They can always feed the awareness programme with information and tailor it to the needs of the staff or to the trending threats.

Human resources

HR are responsible for promoting but also engaging the different target audiences to all relevant activities. HR can introduce procedures that make awareness programmes mandatory in various stages of the employees' induction in an organisation.

Data protection office / legal department

The legal department's valuable input in privacy and personal data topics can enhance the learning experience and also cover specialised security topics of the awareness-raising training agenda.

Instructors

These people are responsible for delivering the programme content to the target audience. Instructors can be external entities or employees of the organisation with a specialised background, or even some other member of the CAT who has the skills and charisma to deliver public speaking.

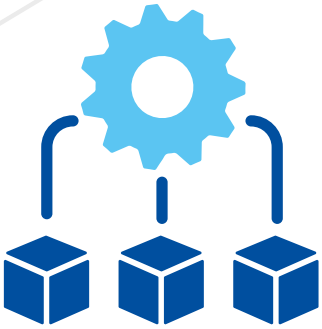
4. CHOOSING EMPLOYEE TARGET GROUPS

Identification and categorisation of employees in target groups is paramount when developing a strategy for cyber awareness and cyber-culture development, as they improve the dissemination of key messages to the appropriate recipients. Below is an **example** of the breakdown of a generic organisation's staff, which can be used as a guide to follow and fine-tune based on your needs.

Table 1. Employee target groups

Audience groups		Clustered audiences
1	Generic employee	Generic employee
2	Contractor	
3	HR	
4	Communications and marketing	
5	Legal	
6	Operations and research and development	C-level, decision-makers, handling budgets
7	Finance and procurement	
8	Managers, officers	
9	Heads of unit, directors	
10 11	Cybersecurity professionals Information technology (ICT) professionals	Professionals / horizontal implementors of cybersecurity measures and users of cybersecurity solutions, working for organisations and/or individuals

NB: The roles as presented above **do not** exist in all types of organisations. In several cases one employee might occupy more than one role (e.g. IT professional and cybersecurity professional).



11 groups of employees are identified as potential receivers of learning products and experiences.
A further analysis of the audience groups can pinpoint additional meaningful clusters based on common characteristics of theirs (**generic employee, chief level (C-level), and ICT and security professionals**, as presented in Table 1 below), and can also provide insights on the approach and methodology for creating awareness.

5. SELECTING THE RIGHT TOOLS

The tools that you will employ in order to deliver your awareness-raising programme must be tailored to meet all its parameters (target audience, resources, objectives, budget), and must:

- raise awareness on the most prominent cybersecurity risks, as derived from the risk assessment (**what** are the most prominent risks of internet use?);
- provide knowledge on how to tackle and respond to such risks (**how** can I navigate the internet safely?);
- influence behavioural change (**why** should I change my digital habits?).

Tools are considered to be the foundation of any activity and may include infographics, tip sheets, posters, videos, presentations, exercises, quizzes and puzzles, etc. (More information and an analysis are provided in "Promotion Channels Analysis" document of AR-in-a-Box

Based on the analysis of the target groups' background, you can divide your target audience into three categories based on their proficiency level (PL) on the topic:

- **aware – proficiency level 1 (PL1),**
- **trained – proficiency level 2 (PL2),**
- **experienced – proficiency level 3 (PL3).**

For the majority of target audiences, the material to be produced and delivered should aim at achieving PL1 awareness. A systematic approach towards devising, delivering and disseminating PL1 awareness material will foster a change in the awareness level of cybersecurity risks, which can lead to eventual influence and/or change of behaviour towards more facilitative, safety-prone digital habits.

Target group PL2 cannot be effectively served by PL1 awareness material only. To ensure this audience group remains skilled and up to date, awareness material should include PL2 or even PL3 products.

PL3 covers experienced staff with a technical background. Specialisation and training are therefore discussed rather than awareness. Trainers that conduct the awareness programme are categorised as PL3.

As such, Table 2 presents proposals for the PL1 and PL2 objectives per audience group and topic categories.

Based on this analysis, decisions can be made about the creation of material and the use of tools and experiences for the following:

- **single topic across relevant employee groups** (e.g. video on malware risks targeting the audience groups);
- **single employee group across topics** (e.g. website campaign on common cybersecurity risks, such as email spams, password attacks, malware, phishing and ransomware);
- **cluster employee group across topics** (e.g. networking event for professionals on latest developments in data breach, malware, ransomware and relevant certifications).

Table 2. Matrix of proficiency level per target audience and topic category

PL drop down per audience group and topic category		Audience groups		
		Generic employee	C-level	ICT and security professionals
Topic categories	Cyberbullying	PL1		
	Online gaming	PL1		
	Online pornography	PL1		
	Safe internet	PL1	PL1	
	Sexting	PL1		
	Fake news	PL1		
	Privacy and data protection	PL1	PL1	
	Financial scams	PL1		
	Mobile banking	PL1		
	Device safety	PL1	PL1	
	Email spam	PL1	PL1	
	Business email compromise fraud	PL1	PL1	
	Password attacks	PL1	PL1	
	Data breach	PL1	PL1	PL2
	Malware	PL1	PL1	PL2
	Phishing	PL1	PL1	
	Ransomware	PL1	PL1	PL2
	Cyber upskilling	PL1		PL2
	Cyberterrorism		PL1	
	Certifications			PL2

6. CREATING A TIME PLAN

First and foremost, a time plan should be tailored to business activities, the workload and the topics of the campaign (i.e. if you want to target the financial department, it is not prudent to launch a cyber-awareness programme during December when the fiscal year is closing). Furthermore, do take into consideration that you need to devote time beforehand, in order to identify the current cybersecurity posture of the organisation (e.g. through a simple, quick survey or quiz). An indicative example of a time plan is presented below.

January	February	March	April
Baseline quiz	Training topic	Videos and dissemination material	Videos and dissemination material
May	**June**	**July**	**August**
Training topic 2	Simulation exercise	HOLIDAYS	HOLIDAYS
September	**October**	**November**	**December**
Back-to-school training	Games/test/quiz	Insights collections	Report to management

As one may notice, you also need to allocate time to regular sanity checks (such as tests, simulation exercises or quizzes) as they provide a better insight on the effectiveness of the programme and the absorption of the information provided so far. It also allows for on-the-fly corrective action to improve the current programme.

7. IMPLEMENTING THE PROGRAMME

Three timestamps are considered relevant for delivering cybersecurity-awareness training to your employees:

1. when they join the organisation as part of the induction process;
2. after an incident, in order to indicate the procedures, roles and responsibilities in place;
3. at regular intervals throughout the year.

Each of these instances offer a different opportunity to build employee knowledge on specific aspects of cybersecurity or to provide them with real-world examples of what to do and not to do. If you can plan ahead, you can develop the right types of courses for the right occasions.

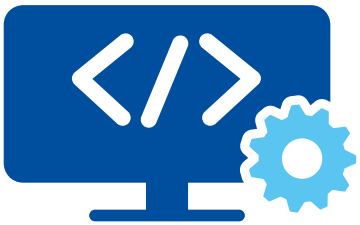
Onboarding

When someone joins an organisation, induction to its cybersecurity culture is important. The new recruit has to go over the people, processes and technology that are most relevant to their job functions when it comes to security. Focus on general policies and role-specific information that will help new employees do their jobs more effectively.

Security maturity requires constant learning.

Training, like many aspects of security, is not a one-off activity. One needs to include it in all aspects of the organisation until it becomes an integral part of organisational culture. When hiring new employees, it is vital that they receive a course as part of their 'welcome package', which will help them perform their tasks while taking cybersecurity aspects into account. Following that, ongoing post-incident and periodic cybersecurity training will help maintain the culture.

Cybersecurity training is an ongoing process that you will need to modify and amend as your organisation grows. This is part of ensuring that your security posture is as mature as it can be, even as your company and the cybersecurity landscape grows and evolves.



Specifically, set up a one-on-one or group session for new employees. This can be delivered via an engaging, interactive presentation, where you go over the key security principles and tools they will be using and those they should be aware of. Following this, you can quiz them to test out their new knowledge.

Post-incident

If a security incident occurs in your organisation, it can be a good time to offer a refresher course. Instead of laying blame, think of this as an opportunity to analyse an actual issue that arose and show how it can be avoided in the future.

What pieces of information did your team not have (or forgot along the way) that would have helped them avoid the situation? How can you better educate them for the future? With this information in hand, set up an all-company meeting where you can review best practices for these types of incidents. Focus on the attack vector and how others in the organisation can avoid falling victim to the same type of attack.

Continuous

The idea here is to set up a curriculum that covers the most common security threats (this will change over time as new ones come to the fore) and keeps cybersecurity top of mind through a regular cadence of education and awareness.

8. EVALUATING THE PROGRAMME

Upon implementation of the programme, you need to assess its effectiveness in order to identify the lessons learned and the changes that may need to be made in the future.

KEY RECOMMENDATIONS

The key factors for a successful awareness-raising programme are summarised below.

Deliver the right message to the right employee group. Identifying key audiences from the group of employees helps ensure messages are received by those who will be most receptive to them. Identifying the target audiences and tailoring the programme to their specific needs and level of knowledge, from the early planning stages of a programme, ensures that the right message reaches the right audience. Messages need to be clearly related to cybersecurity topics that audiences find familiar.

Key message formulation is important for the success of a cyber-awareness programme. Since every cybersecurity topic and audience is unique, each training requires a customised approach. For the development of future awareness-raising and educational training, specific and achievable objectives should be set to act as success indicators. Taking into consideration the geographical and the thematic scope, the employees' group should be reached with messages that respond directly to their cybersecurity fears and particular needs.

Selection of the appropriate tools. The process of selecting the appropriate tools, in order to communicate the correct message(s) to the employees effectively, is key in the cyber-awareness design.

Learning by monitoring and evaluating. The development of measures to assess the impact of the entire programme should be considered from the very start of its design. Regular monitoring and evaluation help to keep track of what is happening and allow the team to take corrective action if necessary.

ANNEX

Example of an awareness-raising programme.

Objective	Indicative implementation timeline
1. Raise awareness on the cyber threat of phishing. • Provide a custom training on the topic, informative material and a hands-on quiz to evaluate progress. • Utilise a phishing simulation campaign to capture before and after results. • 100 % of staff should participate in the activity.	6 months
2. Promote cybersecurity education and culture. • Provide a custom training, a reporting process in the event of an incident and a hands-on table-top exercise to evaluate lessons learned. • 80 % of the staff should participate in the activity.	1 year
3. Improve preparedness in the event of an incident. • 100 % of ICT personnel should participate in the activity. • Provide training and a hands-on technical exercise to evaluate lessons learned. • Test escalation procedures in place and identify gaps.	6 months

Table 3. Suggested programme delivery methods according to proficiency level target

PL1 – aware	PL2 – trained
Webinars / information sessions	Real-time courses (face to face or online)
Intranet/website, portal	e-learning / online courses
Videos, leaflets	Webinars/workshops
Podcasts	Video tutorials
Helplines / hotlines / chat boxes	Training labs
Newsletters	Discussion groups / forums
Awareness kits (posters, background, screensavers, infographics, customised Windows login pages)	Gamification (role playing, escape rooms, mock attacks)
Online games, quizzes	Micro/nano learning
Publications	Diplomas and certifications

Table 4. Suggested delivery methods per target group

Target audience	Channels and delivery methods
Generic employee, contractor HR, communications and marketing, legal, operations and research and development	• Social media websites, portals • Online games and quizzes • Gamification (e.g. role playing, escape rooms, mock attacks) • Awareness kits (posters, background, screensavers, infographics, customised Windows login pages) • Helplines / hotlines / chat boxes • Video tutorials • Discussion groups / forums
Finance and procurement, managers, officers, heads of unit, directors	• Newsletters • Awareness kits (posters, background, screensavers, infographics, customised Windows login pages) • Videos • Webinars/workshops • e-learning / online courses • Publications • Conferences/events
ICT professionals, cybersecurity professionals, cyber knowledgeable	• Real-time courses (face to face or online) • Videos • Webinars/workshops • e-learning / online courses • Training labs • Certifications/diplomas • Publications • Networking events / conferences

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu