AR-IN-A-BOX

YOUR GUIDE TO DESIGNING A CYBER-AWARENESS CAMPAIGN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

CONTACT

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

AUTHORS

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

CONTRIBUTORS

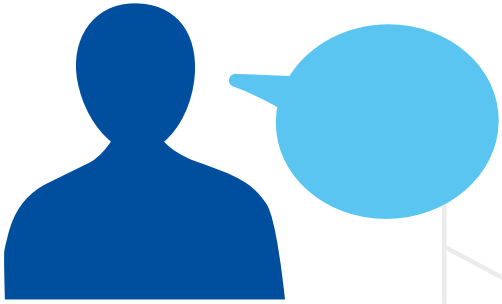
Chloe Blondeau, Goran Milencovic, Theodoros Nikolakopoulos (ENISA)

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue number: TP-09-22-591-EN-N
ISBN: 978-92-9204-592-0
doi:10.2824/842525

FOREWORD



This is a step-by-step guide for the implementation of an **external** cybersecurity-awareness campaign in your professional sector. It provides the tools required to design, implement and evaluate such a campaign, targeting various audiences through different channels.

From programme to campaign

Within this document, there will be several 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 organization's strategy for cybersecurity. It can include one or more internal or external campaigns, focused on a common cybersecurity topic or target audience.

- **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.

GENERAL PRINCIPLES

1. PURSUE BEHAVIOURAL CHANGE AS THE END GOAL

When designing an awareness-raising campaign, decision-making should always be based on the desire to achieve behavioural change, to the extent that it is possible. When selecting awareness-raising activities, determine how they will address or include behavioural change and call to action for the target audience. This principle should steer decisions for the programme, guide choices and help structure contributions from stakeholders.

2. TAKE A RISK-BASED APPROACH TO DEFINE YOUR AWARENESS CAMPAIGNS

A risk-based approach means that defining, executing and monitoring a campaign relies on continuous risk assessment. This includes a pre-assessment of the threat landscape (i.e. emerging threats) and the context in which cybersecurity applies to the target audiences. This ensures that the activities will cover relevant topics and address the risks that pertain to the target audience. In addition, a risk-based approach will help steer the monitoring of key performance indicators (KPIs) and highlight where efforts should be strengthened.

3. KEEP IT SIMPLE AND BE SELECTIVE

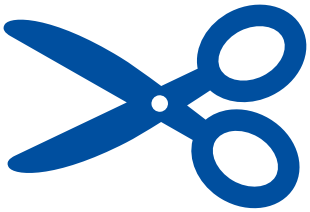
A key success factor of an awareness-raising campaign is to focus on the most important issues that you want to address. What are the top three risks in terms of behaviour or target audiences that your organisation wants to address this year? Where can you make the most impact in line with our overall objective? Instead of taking a complex perspective and striving to do everything, focusing on a selection will help channel efforts, measure impact and generate consistency and publicity.

4. LEVERAGE AND FACILITATE PARTNERS

For any campaign, especially for external campaigns, closely cooperate with and empower partners – whether they be contributing partners or multipliers who can implement campaigns locally. In addition, always take a wider perspective when looking for partners and seek beyond traditional stakeholders to find other communities that can contribute to the effort. Once chosen, assess how to efficiently facilitate them (e.g. by providing templates, setting objectives, running books or proposing a list of activities).

5. TAILOR AWARENESS-RAISING ACTIVITIES TO TARGET AUDIENCES

The tools and activities to be implemented must be tailored to target audience profiles, in order to deliver a core set of relevant and applicable cybersecurity knowledge. Secure behaviour objectives are relatively similar across the entire population, but achieving these objectives requires thinking about how specific groups can best be motivated, taught and empowered. A campaign should drive motivation and interest rather than deploy generalist and one-time activities. Therefore, defining the target audiences and identifying related risks, key behaviour, significant activities and security topics is part of a tailored approach.



6. CONTINUOUSLY MONITOR AND FOLLOW UP ON RESULTS TO MAKE IMPROVEMENTS

Comprehensive monitoring of results through metrics and KPIs helps with knowing what to focus on, thereby steering and leading to improvements in the programme, potentially also through benchmarking. Besides tracking metrics, an important part of this task also focuses on gathering feedback from participants, stakeholders and partners. This information may, for example, be collected through qualitative feedback, scoring questionnaires or informal briefings from partners and multipliers. Finally, as a nice to have, consider the possibility of monitoring the external landscape: unanticipated threats, incidents or other events that might require a change in awareness-raising activities.

7. COMMUNICATE RESULTS AND SUCCESS STORIES ACROSS THE ECOSYSTEM

Increasing visibility and publicity is important because this will generate more traction for (future) awareness-raising activities. Publicly communicating success stories from an awareness-raising campaign can serve this purpose. For this, stakeholders can be asked to contribute local success stories that resulted from their own awareness-raising efforts and activities. This will display concrete results, thereby creating more involvement and interest in future activities.

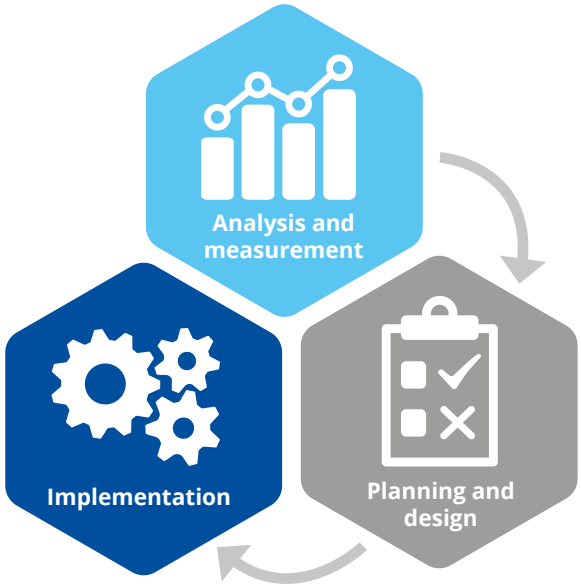
8. USE POSITIVE AND EMPOWERING MESSAGES

A common narrative within cybersecurity-awareness initiatives is that people are the 'weakest link' in an organisation. This negative storyline that blames users should be replaced by a more positive and empowering message.

In addition, with awareness-raising communication, creativity and humour should be considered as ways to lighten the message and prevent a negative narrative from arising, which often tends to be counterproductive. The message you want to share with the audience should be of an empowering nature, as people need to be provided with hope about how to turn a negative situation around with action. This also includes thinking about how the target audience might feel like they have achieved something, and how they may even feel proud and satisfied after participating in cybersecurity-awareness activities. While it is beneficial to make the audience aware of dangers and risks, equally as important is the message that they are all capable of contributing to responses to these threats. This positive and empowering point of view should also be applied to an organisational perspective, where the message should be spread that cybersecurity should be seen as a business enabler and not blocker.

DESIGNING AN AWARENESS-RAISING CAMPAIGN

A campaign design consists of three phases: analysis and measurement, planning and design, and implementation. These phases have a logical order (as illustrated below), but they are not strictly sequential, meaning that some can run in parallel. They rather serve as building blocks with a particular focus. The model described sets out clear delivery stages and encompasses all elements of a successful awareness-raising campaign. This offers flexibility to each organisation to follow their customised approach when it comes to an awareness-raising campaign.



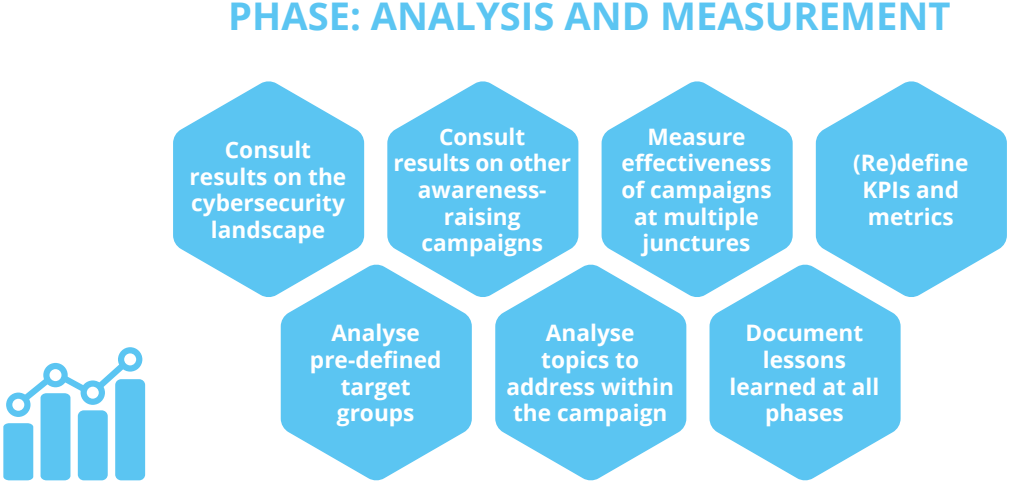
NB: The steps presented are extensive and, depending on the organisation's needs or size, could be merged or some could be omitted.

PHASE 1:
ANALYSIS AND MEASUREMENT

The aim of this phase is twofold. First, this phase is about analysing the landscape in which the campaign will be executed. Among other things, risks will be identified, target audiences and their behaviour will be mapped and security topics will be chosen. From here, the desired goals will be defined, providing input to defining success indicators.

Good practice hints are as follows:

- investigate success stories and push for failures while providing examples;
- assess the level of knowledge and skills of the target group prior to establishing the campaign activities;
- make campaign organisers familiar with technical topics so that they can assess the most important aspect to be addressed.

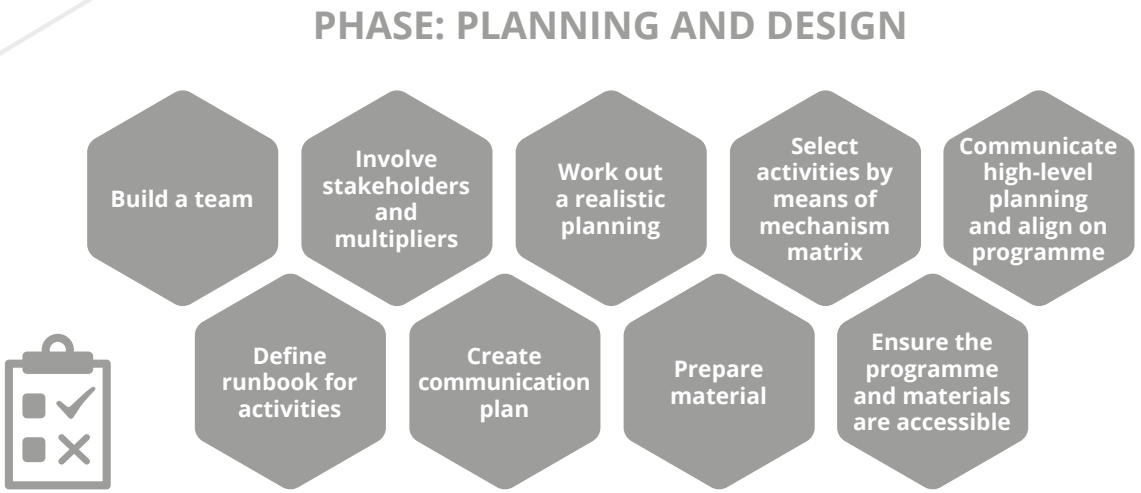


PHASE 2:
PLANNING AND DESIGN

The planning and design phase contains all the preparatory work that needs to be done for a campaign. Data gathered in the analysis and measurement phase will serve as a starting point.

Good practice hints are as follows:

- get blockers (i.e. people who are pushing back on the campaign and its objectives) on board early;
- select the right stakeholders and multipliers and treat them as a sounding board to test the campaign or provide feedback prior to campaign execution;
- create a network of amplifiers who will promote and embed positive information on cybersecurity behaviour;
- it is preferential to disseminate little but often;
- material should be inclusive and diverse;
- create a mascot (a specific character) to put a friendly face on cybersecurity;
- create material based on the visual identity and the branding strategy of your organisation;
- make sure the material can be easily shared, reused and updated;
- translate material, taking into account cultural nuances;
- create a library / awareness hub showcasing all material.



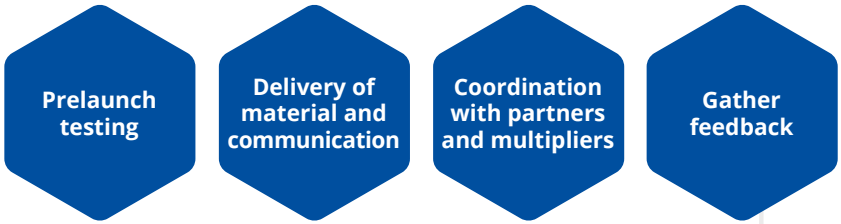
PHASE 3:
IMPLEMENTATION

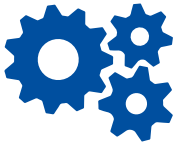
In the implementation phase, all the awareness-raising activities analysed, planned and designed in previous phases will be deployed and communication will be delivered to the predefined target audiences. The delivery of the awareness campaign is structured based on the previous steps.

Good practice hints are as follows:

- content review, pilot testing on activities and testing of the user interface are common steps to undertake;;
- there should be a strong focus on the facilitation of the potential multipliers, stimulating them to use the developed material and encouraging them to implement activities regionally.

PHASE: PLANNING AND DESIGN





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