AR-IN-A-BOX

CYBER AWARENESS – MEASURING IMPACT

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

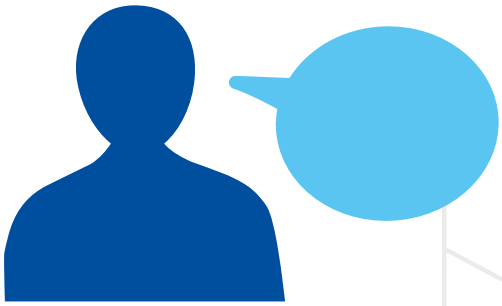
Chloe Blondeau, Goran Milencovic, Theodoros Nikolakopoulos (ENISA)

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue number: TP-09-22-593-EN-N
ISBN: 978-92-9204-594-4

FOREWORD



Measuring impact and behavioural change after the design and implementation of a cyber-awareness programme is crucial to understanding whether the primary objectives were met or changes are required. It is done on the basis of key performance indicators (KPIs), which derive from the objectives of the awareness-raising programme/campaign and need to be defined at an early stage of its design.

This document provides a guide for the definition of KPIs and their translation into metrics.

SELECTION OF KEY PERFORMANCE INDICATORS

A KPI is a value that measures a component of an awareness-raising campaign or programme. KPIs are used at different levels within an organisation to evaluate success and determine whether predefined objectives have been achieved. They give insight into whether campaign target groups are learning and applying new knowledge, and whether the campaign is helping them change behaviour. The KPIs presented in this document were defined based on common trends, best practices and objectives within the field of awareness-raising campaigns and programmes.

Corresponding metrics for KPIs are also identified. Keeping track of metrics facilitates the measurement of the defined KPIs. Metrics of an awareness-raising activity concern the aspects that can be monitored over time, which help identify a campaign's impact and progress.

KPIs will support buy-ins from stakeholders when discussing another edition of the cyber-awareness campaign and, together with metrics, they help identify best practices and lessons learned in the closing phase.

There are five reasons why KPIs fail to improve performance:

1. the KPIs are poorly defined;
2. they lack accountability;
3. they are not achievable;
4. they are not specific enough;
5. they are too hard to measure.

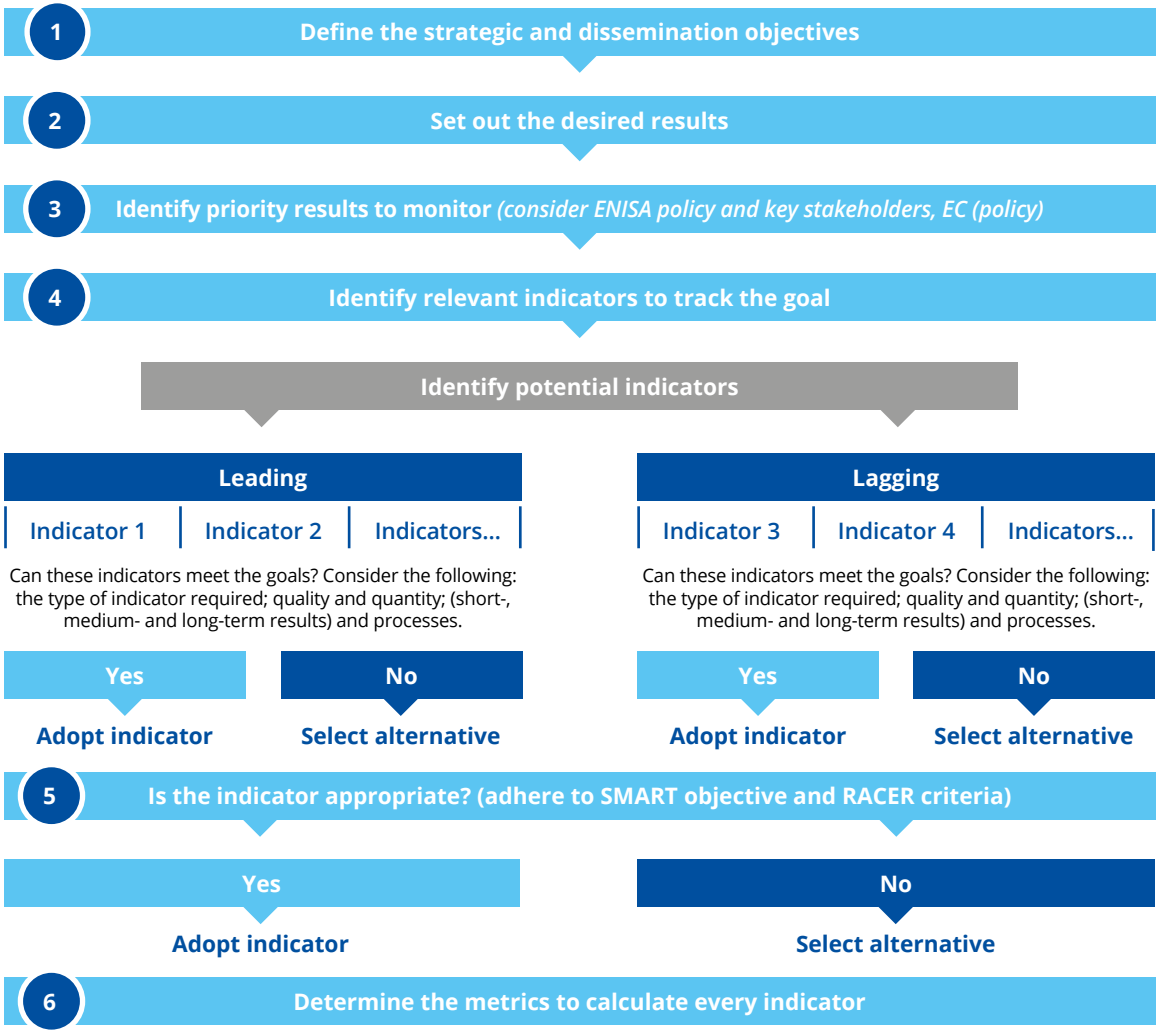
The KPI decision tree (Figure 1) summarises how to define, select and measure KPIs.

Table 1. Indicative overview of KPIs and corresponding metrics

Scale of outreach (KPI)				
Metrics	Number of participating countries	Number of reached individuals	Number of communication partners	Number of mentions in media
Facilitating the multipliers (KPI)				
Metrics	Number of multipliers	Number of multipliers that contributed to the campaign	Number of multipliers that downloaded the material	
Level of behavioural change achieved (KPI)				
Metrics	Percentage decrease of incidents	Number of reported incidents	Number of positive test results	Level of increased knowledge
	Qualitative feedback on security good practices			
Public perception (KPI)				
Metrics	Qualitative feedback on activities from the participants (on level of satisfaction)	Qualitative feedback from the participating EU Member States (on level of satisfaction)	Engagement rate (e.g. followers, likes)	
Durability (KPI)				
Metrics	Level of reusability (for example ranging from 1 to 5)	Resources needed to reach objectives	Costs – contribution partners / stakeholders	

NB: Every KPI should be monitored regularly. Tracking the progress against the KPIs is essential to their maintenance and development. Not all KPIs are successful, though. Some have objectives that are unachievable, while others may fail to track the underlying goal they were supposed to achieve.

Figure 1. A decision tree for the selection of KPIs



NB: Do bear in mind that the above list in not exhaustive.

DESCRIPTION OF METRICS

The following section gives a more in-depth description of the defined awareness-raising KPIs and corresponding metrics. Each metric is described based on the following categories:

- **indicators:** trends that provide data on and insight into the progress of the metric;
- **means of measurement:** how the metrics and KPIs will be measured (e.g. by tracking, a survey or a questionnaire);
- **strengths**;
- **limitations**;
- **advanced suggestions**.

Metrics for scale of outreach (KPI)

The first KPI, on the scale of outreach, concerns the extent and limit of exposure of an awareness campaign or programme. It determines the extent to which an organisation has been able to reach its target audiences and defines how the messages and purpose of the activities have echoed across different ecosystems and have been able to spark interest.

Metrics for scale of outreach (KPI)

The first KPI, on the scale of outreach, **concerns the extent and limit of exposure of an awareness campaign or programme**. It determines the extent to which an organisation has been able to reach its target audiences and defines how the messages and purpose of the activities have echoed across different ecosystems and have been able to spark interest.

Number of reached individuals

Indicators	• Social media impressions and engagement with campaign posts. • Number of people participating in the locally deployed activities and events (i.e. physical v online). Possibly on a more fine-grained level with attention to the number of participants of specific target audiences.
Means of measurement	• Social media analytics provided by the platform (e.g. Twitter, Facebook, Instagram, LinkedIn). • Media monitoring tool. • Measure the number of views, likes, clicks and shares. • Information from the communication partners on how many people they reach.
Strengths	• Effective way of measuring outreach on a large scale. • Quantitative information to measure the number of citizens or professionals engaged and participating. This is a proof of interest in the security topics discussed.
Limitations	• The use of the appropriate social media to disseminate the campaigns according to the target (other than existing accounts on Facebook, LinkedIn and Twitter). • Media monitoring tools can be costly. • This can only be achieved if the participating Member States collect the information from the events and activities.
Advanced suggestions	• Ask partners and customers to benchmark activities and track campaigns and the number of individuals reached. Reporting on national activities – and pointing to gaps in that reporting – might motivate less-active entities to increase their efforts.

Number of communication partners

Indicators	• Institutions, associations, agencies or bodies that are affiliated with the campaign as communication partners, and support dissemination and communication.
Means of measurement	• Tracking matrix (e.g. Excel) of communication partners managed by the campaign team.
Strengths	• Communication partners can help visualise how the outreach and the interest have grown over time. • Makes the communication support of the campaign formal through mutual engagement. • Displays, at a glance, the strong communication assets within the organisation's community for the campaign.
Limitations	• It is difficult to assess whether the communication partners bring added value to the outreach of the campaign. • It is difficult to assess the ecosystem and target audiences that are reached thanks to cooperation with the communication partners.
Advanced suggestions	• Formalise cooperation by giving a concrete list of expectations to the communication partners. This ensures that cooperation is more than a visibility move and encourages true efforts in supporting the campaign. Maybe even hand out an award for the most active communication partner.

Number of mentions in media

Indicators	• Media mentions of the campaign in traditional or online media. • Speaking engagements as aftermath of the campaign.
Means of measurement	• Social media analytics provided by the platform (e.g. Twitter, LinkedIn). • Media monitoring tool.
Strengths	• Number of mentions in the media is a clear indicator for measuring the outreach of a campaign. • This provides solid information on the public interest.
Limitations	• Only focusing on the number of mentions in the media does not say anything about the content of that message. Mentioning a campaign in a negative way counts as a mention but may be ineffective for a campaign. • This may rely on effective cooperation with partners and external stakeholders.
Advanced suggestions	• An analysis of the number of mentions in the media could be enriched by adding a more comprehensive media resonance analysis, where you dig a level deeper and also look at the media tenor and in-depth perception of the messages shared. Also consider whether there are advanced tools that can assist with this.

Metrics on the level of behavioural change achieved (KPI)

The ultimate goal of awareness-raising campaigns and programmes is to establish long-lasting behavioural change. A cyber-awareness programme's effectiveness can be measured by **capturing data on changes in the way people react to threats and act according to desired cybersecurity behaviours**. Identifying the cyber-awareness maturity level of the target audience is important to identify what is needed to create a culture of cybersecure behaviour. Therefore, the awareness campaign's objectives must align with the target audience's capabilities, and the language and message should be adapted accordingly.

Number of mentions in media

Indicators	**• Media mentions of the campaign in traditional or online media. • Speaking engagements as aftermath of the campaign.**
Means of measurement	• Social media analytics provided by the platform (e.g. Twitter, LinkedIn). • Media monitoring tool.
Strengths	• Number of mentions in the media is a clear indicator for measuring the outreach of a campaign. • This provides solid information on the public interest.
Limitations	• Only focusing on the number of mentions in the media does not say anything about the content of that message. Mentioning a campaign in a negative way counts as a mention but may be ineffective for a campaign. • This may rely on effective cooperation with partners and external stakeholders.
Advanced suggestions	• An analysis of the number of mentions in the media could be enriched by adding a more comprehensive media resonance analysis, where you dig a level deeper and also look at the media tenor and in-depth perception of the messages shared. Also consider whether there are advanced tools that can assist with this.

Number of incidents

Indicators	• Return on investment (how investing in security saves money by preventing incidents). • EU annual focus budget allocated to incident response. • Notifications of incidents. • Observations of the threat landscape to assess whether threat attackers' attempts are evolving (e.g. increase v decrease of ransomware attacks in comparison to other attack techniques). • Overview of security topics addressed by awareness-raising campaigns (e.g. ransomware) and correlation with incidents (or mitigation).
Means of measurement	• Tracking of incidents by an incident response team within an organisation. For example, by using security information and event management software, which monitors the number of incidents. Based on these results, the increase or decrease of security incidents can be measured over time. • Tracking incidents reported to a national computer emergency response team or supporting channels by local government to facilitate reporting of malicious activities experienced by citizens. • Reports from national competent authorities, in the context of the directive on security of network and information systems (NIS directive), on cross-border incidents or large-scale incidents (i.e. in connection with ENISA as secretariat for computer security incident response teams).
Strengths	• The measurement of these metrics stimulates collaboration with partner organisations, such as national computer emergency response teams and incident response teams within organisations.
Limitations	• Decreased incidents cannot be directly linked to cyber-awareness activities. • It is (highly) challenging to gather this data at the EU level to get an accurate picture. Collaboration with third parties is key. • Note that not all incidents are caused by behaviour, it is therefore not always an indication of behavioural change.
Advanced suggestions	• Collaborate with large partners such as telecom providers, Google, banks and service providers to get figures on how many phones are infected. • Set up a group of organisations across EU countries, who are willing to provide metrics before and after campaigns. • Leverage the network established by EU information sharing and analysis centres (e.g. gain insight into how companies handle incidents and their level of awareness on cybersecurity as an urgent matter; establish trends on incidents and whether they decrease).

Scores on cyber-awareness tests

Indicators	• Quantitative and qualitative test results on an organisational, national or sectoral level.
Means of measurement	• Tests organised by the organisation to directly gather input. • Tests organised by national competent authorities or multipliers.
Strengths	• Tests provide insight into what happens in practice. • Tests are as accurate as one can come to actually measuring behaviour or knowledge.
Limitations	• Organising or collecting input from cyber-awareness tests can be very time (and resource) consuming. • Tests need to be consistent over the years to be of actual value.
Advanced suggestions	• Reaching out to vendors who execute these tests to discuss whether they can share (high-level and anonymous) changes in relevant metrics.

Level of knowledge

Indicators	• Interest in security topics. • Performance in cyber-awareness tests. • (Cyber) security topics addressed in the media (i.e. radio, TV) that inform and educate, instead of broadcasting only the cyberattacks, or a report that includes tips and basic information. Think, for example, of the rise of cybersecurity-related podcasts on Spotify.
Means of measurement	• A cybersecurity knowledge assessment is a quantitative questionnaire in which people's knowledge on predefined security topics is measured. • Measurement should take place before and after the launch of a cyber-awareness campaign to assess people's knowledge level and its development.
Strengths	• A quantitative questionnaire is easy to build and does not take long for the participants to fill in. • Some vendors offer ready-made questionnaires in which an organiser can select the right security topics for a target audience. • The results can help steer the programme or campaign and the content of the deployed activities and tools (mechanisms).
Limitations	• Building the survey can be very time consuming since it should be adjusted to the target audience and the predefined security topics. • The risk of people filling in the questionnaire randomly. • Challenge in reaching out to a broad audience (i.e. general public).
Advanced suggestions	• Quantitative questionnaire to a sampled group to gain insight into the current level of cybersecurity topics within the defined target audience.

Qualitative feedback on security good practices

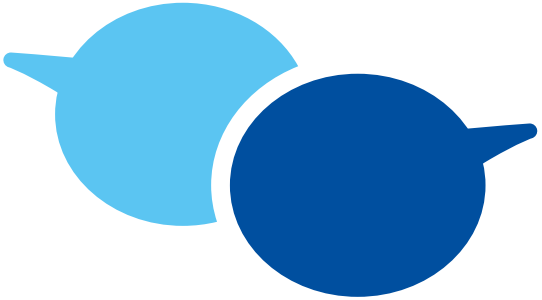
Indicators	• Changes observed after a cyber-awareness campaign in terms of new investments in and approach to security. • Number of people who have enabled multifactor authentication (MFA), configured automatic updates, installed antimalware or used a (reputable) virtual private network (VPN).
Means of measurement	• After a short time (e.g. 3 to 6 months), share questionnaires with participants or stakeholders from the activities to ask if they have changed their practices and behaviour regarding security (e.g. if their organisation invested more in security or if they feel more alert when receiving a phishing email). • During the activities, ask participants at the end of a session what they think should change in their environment or behaviour (e.g. create stronger passwords, use a VPN, activate MFA, encourage awareness on security in their work organisation).
Strengths	• Concrete insight into the impact of the awareness-raising campaigns and related activities in terms of what that impact helps to change in the environment.
Limitations	• Difficult to capture in detail the essence of this information, if new security practices are introduced or if more security technology is being used.
Advanced suggestions	• To get the figures on the number of incidents, collaborate with partners such as telecom providers, Google, banks and service providers, also collect information on how many people have enabled automatic updating, MFA or other security best practices.

Metrics on perception (KPI)

When deploying a cyber-awareness campaign, the organisation may seek to enhance its visibility and reputation on the theme. Achieving a positive reputation from both the public and the security ecosystem should be a prime objective. Although this KPI may be considered subjective, certain metrics will help gather facts to understand **trends on how the organisation is perceived**.

Qualitative feedback on activities from the participants

Indicators	• Number of attendees to national activities and users of tools. • Social media engagement on publications corresponding to the activities, where participants can comment on their experience (qualitative indicators, such as comments). • Rating from participants at local events and activities.
Means of measurement	• Sending a short scoring email to participants or a scoring survey for physical activities and events. • Evaluation surveys after events and campaigns.
Strengths	• This allows direct feedback and scoring from participants to be provided.
Limitations	• Subjective results. • Prior collaboration with partners should be in place. • Gathering feedback requires effort. If done by email, it has to be sent shortly after the event. If done during a physical event, it has to be done strategically to collect as much feedback as possible (e.g. position the quick scoring request next to the area where participants give back their badges).
Advanced suggestions	• Associate the request for feedback and scoring with a participant contest, to make it more attractive. For instance, a selected group of respondents might be given some benefits (e.g. entrance to a sponsored exhibition in their capital) or be invited for a university seminar/ conference on a cyber-related topic.



Engagement rate (e.g. followers, likes, opened discussions in comments)

Indicators	• Social media analytics. • Comments, likes, sharing numbers, views, comments.
Means of measurement	• Publicly available social media analytics. • Social media analytic tools.
Strengths	• Specific quantitative data on the amount of engagement online. • High impact for the communication strategy and results. • View on how many people interact with the organisation's social media content.
Limitations	• Engagement rate on social media may not necessarily reflect reality. • These metrics look at facts, and not content.
Advanced suggestions	• Combine the results with the monitoring and analysis of website traffic. • Align with partner communication officers and combine similar data to have a bigger picture.

Metrics on durability (KPI)

A KPI on durability will indicate whether the developed and implemented **process is long lasting, continuous and cost efficient**. It assesses the reusability of a programme and its components / materials used, the resources needed to reach objectives, and costs in relation to the contribution of partners and stakeholders. It is a very useful KPI, yet not all organisations opt to go to such lengths in their evaluations.

MEASURING IMPACT PER CHANNEL

Outreach and promotion activities are an important part of a cyber-awareness campaign or programme. Having set the theoretical strategy for developing KPIs, this section provides an overview of corresponding metrics for outreach activities, tools and channels as part of awareness-raising and education campaigns. The table below presents an overview of the KPIs and their metrics, based on the most common dissemination tools, channels and other communication activities.

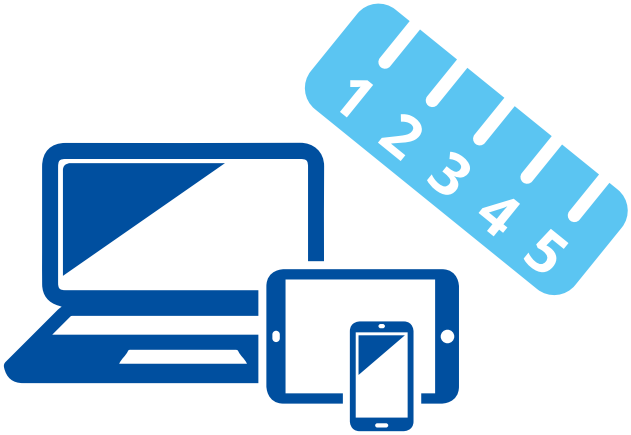


Table 2. Overview of corresponding metrics for tools, channels and other awareness-raising activities

Tool/channel/activity	Metrics
Websites/microsites	• Number of visits • Number of unique visitors • Number of pageviews • Number of actions (e.g. newsletter registrations, toolkits/materials, downloads, call-to-action clicks) • Average visit duration • Acquisition channels • Geolocation • Device type (mobile v desktop) • Top visited pages • Top landing pages
Blogs	• Number of posts published • Number of blog visits • Number of views per post • Number of comments per post • Number of social shares per post
Emails/newsletters	• Number of emails sent • Number of newsletters published • Number of subscribes/unsubscribes • Number of email forwards • Open/click rate • Bounce rate • Number of downloads
Helplines/hotlines	• Average handle time • Number of incidents/questions • Average duration of sessions
Videos	• Watch time • Average view duration • Average rate of completion • Number of engagements • Number of click-through rate • Quality of feedback (i.e. positive/negative comments)
Podcasts	• Number of unique listeners • Number of subscribers • Number of downloads • Ranking • Number of views • Number of shares

continued

Tool/channel/activity	Metrics
Publications, reports, factsheets, infographics, etc.	• Number of publications produced • Number of copies produced • Number of downloads
Events and match-making activities	• Number of registrations/invitations • Number of attendees • Number of partners • Number of events organised/hosted by the organisation • Number of events the organisation participated in • Satisfaction rates of attendees • Number of Q&As • Duration of the event/activity
Questionnaires and surveys	• Number of questionnaires/surveys conducted • Type of questionnaires/survey conducted (online/offline) • Number of questionnaires and surveys answered • Satisfaction rate
Applications	• User satisfaction • Number of downloads • Number of app abandonment • Rating • Number of error rates
E-learning modules	• Time to complete the online training course • Online assessment pass/fail • Material to stimulate lively and interactive learning processes • Ease of service accessibility • Quality of education
Media outreach activities (e.g. press releases, media briefings)	• Number of press releases produced/sent • Number of journalists contacted • Number of journalists reached • Number of press releases published • Number of mentions (online, print broadcast) • Number of interviews
Online self-diagnosis tests	• Number of new users • Number of self-diagnosis completion • Abandonment rate • Satisfaction rate
Online games, stimulations, exercises	• Number of new users • Daily/monthly active users • Abandonment rate • User satisfaction • Number of downloads • Overall rating

NB: As a rule, it is generally advised that two or three KPIs be assigned per objective.

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