Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D3.19

Guidelines for Enhancement of Societal Security Awareness

Document Identification	
Due date	28 February 2022
Submission date	28 February 2022
Revision	1.0

Related WP	WP3	Dissemination Level	PU
Lead Participant	NTNU	Lead Author	Sunil Chaudhary (NTNU)
Contributing Beneficiaries	GUF, UM	Related Deliverables	

Abstract: This report proposes a conceptual framework for the monitoring and evaluation of a cybersecurity awareness (CSA) program. In order to do so, it uses a nonsystematic or purposive literature review. Initially, it reviewed nine existing frameworks/models on CSA mainly to derive the skeleton (phases and sub-phases) of the framework. This is followed by a set of guidelines and practical advice in each phase and sub-phases of the framework that would be useful for the enhancement of a CSA program. The guidelines and advice on "*what to do in each phase*" as well as "*what to expect in each phase*" will be useful for CSA professionals, individuals, or organizations who intend to design a CSA program. In addition to this, the report also presents the evaluation criteria of two CSA mechanisms, which are posters and serious games.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

The main objective of Task 3.10 is to advance the state of the art by developing a novel conceptual model for the monitoring and enhancement of cybersecurity awareness (CSA). In order to achieve the objective, we have designed a conceptual framework for a CSA program. Unlike the existing frameworks/models for CSA programs, this framework does not limit to recommending "*what to do in each phase*" rather it also provides information on "*what to expect in each phase*" of the program. This information is essential for monitoring and evaluating a CSA program. Monitoring checks the output of the activity to determine if it has been carried out as required. Similarly, evaluating checks the outcome of the program to determine its overall effectiveness or success. Both can be possible only if it is known what to expect from each activity and the program. Since a CSA program evaluation has already been covered in another deliverable report D9.13 of CyberSec4Europe, this report focuses more on monitoring. In addition to that, this report also presents the evaluation criteria of two CSA mechanisms, which are posters and serious games.

Multiple methodologies have been used for the purposes. A nonsystematic literature review has been utilized for the conceptual framework and to elicit the evaluation criteria and a survey for the poster's evaluation.

In the framework, a CSA program has been divided into three phases where each phase has multiple sub-phases, and each sub-phase has multiple activities. The phase and sub-phase provide an idea of what to do in a CSA program.

- The pre-implementation phase involves sub-phases like setting up an effective team; establishing proper goals and objectives of the program; grouping the audience; receiving support and participation of the leaders; selecting and prioritizing the most relevant topics; and finally preparing the resources.
- The implementation phase involves conducting a pilot test (if it is the first time or required by rule); message effective delivery; and documenting the lessons learned.
- The post-implementation phase involves evaluating the program for its effectiveness; and adjusting, updating, and optimizing the program by considering the lessons learned and also new changes in the situation for the subsequent or future iteration.

For monitoring, this information is not adequate. It requires an answer to "*what to expect*" from each phase, sub-phase, and activity. This has been answered in the form of guidelines and practical advice in the framework. The guidelines and advice are targeted to CSA professionals and organizations who intend to design, develop, and implement CSA programs. A synopsis of the main guidelines and practical advice are as follows:

- The team should be inclusive with clearly defined roles, responsibilities, and accountabilities for each member. Moreover, it is advisable to have two full-time staff members, but one full-time staff member is a must for CSA. The individual(s) should be equipped with both technical and soft skills, and also be aware of the context.
- The goals should be clear and simple, and its objectives should be SMART (Specific, Measurable, Attainable, Relevant, Time-bound).
- The audience should be grouped preferably based on their beliefs and cybersecurity expertise.
- The program should receive appropriately high priority in terms of support and participation from the leaders, and budget allocation.
- The selected topics should cover threats prevalent to the audience roles and responsibilities, that include both common and new emerging threats.

- The topics relevant to critical security roles and controls, specific to the organization role and risk profile, relevant to critical projects, neglected by the audience, and with resources readily available should get the high priority.
- The message intensiveness or complexities should be adjusted from general to in-depth depending on the audience.
- The message framing should consider human psychological (cognitive, affective, and different biases) and other factors (usability and user experience) that influence the message reception and interpretation by the audience.
- The message delivery methods should be cost-effective; have a broad outreach; support diversity and inclusiveness; be easy and simple to develop, operate, manage, and update; include standardized assessment and feedback features; support information richness; require minimal additional requirements; and interest and motivate the audience.
- The message communication should consider the psychological and other influencing factors that increase the audience's participation and drive them to practice (or translate into actions) the security knowledge they have learned from the program.
- The enforcement approach used to non-compliance should be a soft approach (mainly using intrinsic incentives) unless a specific need arises for a tough approach.
- The program should be organized periodically, at least once every six months except for responding to new events and situations.
- The lessons learned during the different phases of the program should be properly captured, debriefed, and documented for the effective transfer and use of information.
- The evaluation should measure all four indicators (impact, sustainability, accessibility, and monitoring) to determine the overall effectiveness of the program. Moreover, the measurable parameters selected for each indicator should be economical to gather, consistent to measure, expressible in cardinal number and unit, and contextually specific.
- The program should be adjusted in accordance with the changes in the cybersecurity scenarios. It should also take into consideration the lessons learned and weaknesses identified from monitoring and evaluation.

Document information

Contributors

Name	Partner
Sunil Chaudhary	NTNU
Sebastian Pape	GUF
Marko Kompara	UM
Georgios Kavallieratos	NTNU
Vasileios Gkioulos	NTNU

Reviewers

Name	Partner
Outi-Marja Latvala	VTT
Eda Marchetti	CNR

History

Version	Date	Authors	Comment
0.01	2021-04-06	Georgios Kavallieratos, Sunil Chaudhary	Performed the literature review and comparison of the existing CSA frameworks.
0.02	2021-08-14	Sunil Chaudhary	Developed the conceptual framework and performed posters evaluation.
0.03	2021-11-16	Marko Kompara, Sunil Chaudhary	Integrated the feedback received from Marko Kompara.
0.04	2022-01-13	Sebastian Pape	Added the content on serious games.

0.05	2022-01-15	Marko Kompara, Sunil Chaudhary	Integrated the feedback received from Marko Kompara.
0.06	2022-01-17	Sunil Chaudhary	Finalized the 1st Draft of the report.
0.07	2022-01-21	Sunil Chaudhary	Integrated the feedback received from the WP leader and team members.
0.08	2022-01-24	Marko Kompara, Sunil Chaudhary	Integrated "state of the art" section.
0.09	2022-02-05	Sunil Chaudhary	Integrated the suggestions from the first internal review.
0.10	2022-02-15	Sunil Chaudhary	Integrated the suggestions from the second internal review.
1.0	2022-02-28	Ahad Niknia	Final check, preparation and submission

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**ABIS**	Abbreviated Impulsiveness Scale
	ATC-IB	Attitudes Towards Cybersecurity and Cybercrime in Business
B	**BYOD**	Bring Your Own Device
C	**CBS**	Conservative Behavior Scale
	CSA	Cybersecurity Awareness
E	**ENISA**	European Union Agency for Cybersecurity
	EOS	Exposure to Offence Scale
	EU	European Union
	EUROPL	European Union Agency for Law Enforcement Cooperation
F	**FUD**	Fear, Uncertainty, and Doubt
G	**GEQ**	Game Experience Questionnaire
	GDPR	General Data Protection Regulation
H	**HAIS-Q**	Human Aspects of Information Security Questionnaire
	HP	Hewlett-Packard
	HR	Human Resources
I	**ICT**	Information and Communication Technology
	IT	Information Technology
	ISC2	International Information System Security Certification Consortium
	ISO	International Organization for Standardization
K	**KAB**	Knowledge, Attitude, and Behavior
	KPI	Key Performance Indicator
L	**LR**	Literature Review
N	**NIST**	National Institute of Standards and Technology
O	**OCS**	Online Cognition Scale
P	**PCI**	Payment Card Industry

	PENS	Player Experience of Need Satisfaction
Q	**QR**	Quick Response
R	**RBS**	Risky Behavior Scale
	ROI	Return On Investment
	RPS	Risk Perception Scale
	RScB	Risky Cybersecurity Behaviors Scale
S	**SA-6**	Security Attitudes-6
	SDT	Self Determination Theory
	SeBIS	Security Behavior Intentions Scale
	SEI	Software Engineering Institute
	SMART	Specific, Measurable, Achievable, Relevant, and Time-Bound
	SME	Small and Medium Sized Enterprise
	SREG	Security Requirement Education Game
	SSBS	Smartphone Security Behavior Scale
	SToPPER	Security Tactic Planning Poker
T	**TET**	Testing, Evaluation and Training

1 Introduction

Cybersecurity awareness (CSA) mainly encompasses *cognition* (acquiring knowledge and understanding of cybersecurity) that leads to expected *behavioral* changes and *security culture* transformation brought through positive changes in *attitude* towards cybersecurity. Its ultimate goal is influencing or motivating the audience to adopt secure behavior and to discourage them from risky behaviors. This is most effectively done by communicating the *right* security information put into the *right* amount and formats to the *right* audience by using the *right* dissemination channels at the *right* time. The information provided is often enough to draw individuals' attention to security risks, comprehend their potential consequences, and respond appropriately. CSA activities are usually aimed at a large audience, who are primarily passive recipients of the information [1].

1.1 Purpose

CSA has existed for a long time, probably as long as cybersecurity itself, with a considerable amount of research studies on it. Ironically despite so much existing research works, the nature of CSA is still not well understood [2] [3], and it continues to fail in yielding the expected outcomes [4] [5] [6]. The poor performance of CSA is clearly evident from the cyberattacks caused due to human error, ignorance, and negligence; alarmingly, a large portion of cyber incidents stem from some type of human error or behavior [7]. Among other factors, the approaches used for CSA initiatives play a major role in their success or failure [4] [5]. Many CSA programs are limited to simply the delivery of security information or compliance with standards and procedures. Indeed information (or knowledge) dissemination is an important stage of CSA, but it is not equivalent to knowledge absorption and bringing the learned things into practice. Similarly, compliance with standards and procedures will definitely provide a level of security, however, this does not necessarily equate to creating the desired security behaviors. Such a narrow, and sometimes incorrect, understanding of CSA prevails maybe because CSA professionals disregard acknowledging awareness as a unique discipline that involves several important aspects (or determinants) related to influencing security behavior change. And more importantly, these necessary aspects require regular monitoring and evaluation in order to improve them, and without a doubt, the overall effectiveness of CSA programs.

The approaches adopted to understand problems relating to CSA primarily deal with either the CSA *framework* or its *content* [8]. In practice, content is also a component of the framework. There are several studies that have proposed CSA frameworks (discussed in section 3); however, they mainly focus on designing and developing a CSA program with little or no attention on monitoring and evaluating it. Therefore, the main objective of this study is to propose a novel conceptual framework that intends to overcome shortcomings of the past works, facilitate the comprehension and understanding of the crucial aspects of CSA programs, and provide guidelines for their monitoring, evaluation, and eventually enhancement. After all, this is also the objective (i.e., to develop a conceptual framework and monitoring and enhancement methods) set forth by Task 3.10. The proposed framework supplements other existing CSA frameworks.

1.2 Audience

The outcomes of this report will be useful to CSA professionals and organizations (both public and private) that intend to implement CSA programs for the general population or their employees. The provided framework, guidelines and practical advice, and evaluation criteria will help CSA professionals and teams to improve understanding and knowledge for monitoring and evaluating CSA programs.

1.3 Scope

The scope includes monitoring, evaluation, and enhancement of CSA programs implemented for general populations and employees. The scope of the provided guidelines covers mainly the following activities of a CSA program:

- Set up an effective team
- Establish appropriate goals and objectives
- Select and prioritize the relevant awareness topics
- Criteria for awareness resource preparation (content and its dissemination method)
- Criteria for the delivery of awareness messages
- Effectively capture and document the lessons learned
- Evaluate the awareness program for its effectiveness
- Adjust and optimize the awareness program for the subsequent iteration

1.4 Beyond the State of the Art and Main Contributions

The majority of existing conceptual frameworks for CSA (i.e., the current State of the Art), which we will discuss in Section 3, have been designed mainly for organizational purposes, with noted exceptions from NIST [9], ENISA [10], and Kortjan & Solms [11] which have also considered the general population's awareness. Furthermore, the frameworks by NIST and ENISA provide a more holistic and detailed view of CSA compared to others. Nonetheless, all the frameworks have their own strengths and limitations depending on the purposes for which they have been designed. They all predominantly focused on providing instructions for "*what to do*" to design, develop, and implement a CSA program (i.e., inputs and activities); however, they give very little, or no information on "*what to expect*" after the instructions are followed (i.e., outputs and outcomes). Without this knowledge of "*what to expect*" after an activity is executed, it would be almost impossible to monitor and finally evaluate a CSA program. It is this gap that we wish to address in this study. To achieve this goal, we propose a new framework for a CSA program, which answers both questions on "*what to do*" and correspondingly "*what to expect*" after you have done it. To the best of our knowledge, this is the first study of its type that focuses on monitoring a CSA program and is the main way in which this deliverable goes beyond the current State of the Art.

Moreover, several past studies have overlapping and non-overlapping recommendations for a CSA program. They have produced important findings but cover only very specific sections of a CSA program. More importantly, their results are for isolated contexts and currently remain scattered across publications, which need to be brought together and related or connected to produce a more comprehensive picture of a CSA program. This study has attempted to bring together these findings and present them in more usable formats, for example, as properties, factors, and criteria that would be comprehensible for the report's target audience.

In addition to the mentioned framework, the deliverable has produced some significant results that have standalone value and could be taken and applied in different situations and CSA programs. Here are the main such contributions:

- Unified conceptual framework
    - The main contribution and the aim of the whole research was the conceptual framework (Sections 4, 5, 6, and 7), unifying and connecting the structure and recommendations from many previous studies. It includes the whole life cycle of a cybersecurity awareness program, from the set-up of the program to the evaluation of its results and possible adjustments to improve them.
- Guidelines for each phase/activity of a CSA program

    - At the end of each phase/activity of a CSA program (in all Sections 5, 6, and 7 sub-sub-section - e.g., 5.1.1 Team Leader and Others), there is a condensed section on the most important aspects to consider or do in each of the phases/activities.
- Monitoring and enhancement Guidelines (i.e., "*what to expect*")
    - Table 8, Table 10, and Table 12 (in Sections 5.5, 6.4, and 7.3 respectively) document what to expect from correctly implementing each of the previously discussed phases/activities.
- Poster evaluation criteria
    - As part of looking into evaluation criteria for two specific cybersecurity awareness mechanisms, we have created a comprehensive list of criteria for measuring the quality of posters (for raising CSA). The criteria are a concatenation of Table 6 (in Section 5.4.2) and Table 14 (in Section 8.2.1).

Currently, the results of this research have not yet been published, but we do plan to publish them at a peer-reviewed conference. To find the end list of related publications or any other potential changes and additions to the research, visit our GitHub page (https://github.com/cs4ewp3/wp3/tree/main/3.10) where we plan to communicate any further related developments in the research and publications.

1.5 Report Outline

The report consists of seven sections. Section 1 introduces the purpose, scope, and audience of the study. Section 2 describes the research methodologies used for the study. Section 3 reviews some existing CSA frameworks. Sections 4, 5, 6, and 7 propose the unified conceptual framework and present the final guidelines and practical advice for monitoring and evaluation of CSA programs. Section 8 provides evaluation criteria for two CSA mechanisms, which are posters and serious games. Section 9 concludes the study and makes recommendations for CSA.

2 Research Methodology

This section briefly covers the methodologies used for developing the conceptual framework and poster's evaluation. Further, it provides the rationale for choosing a nonsystematic LR for the conceptual framework development.

2.1 Conceptual Framework

A conceptual framework is an abstract and logical representation of interconnected concepts that together provide a comprehensive understanding and functioning of a particular phenomenon [12]. It provides an interpretative approach to *social reality* and is *indeterminist* in nature (i.e., it does not enable the prediction of an outcome) [13]. However, it helps present possible courses of action or preferred approaches that can be used to arrive at a hypothesis. It can be applied where a holistic view of the phenomenon is needed. It does not simply provide the "*hard facts*" but, rather, "*soft interpretation of intentions*" [14]. A conceptual framework requires the selection of concepts relevant to the hypothesis, and the identification of logical relationships among those concepts to develop it. These concepts are derived from multidisciplinary bodies of knowledge. These steps can be performed through a process of qualitative analysis [13], for example, performing a comprehensive literature review (LR) to gather the relevant concepts and establish connections or relationships among them and with the desired objective. This study utilizes a *nonsystematic LR* for developing the conceptual framework. The main rationale for selecting a nonsystematic LR is the flexibility it provides to explore and better understand CSA from diverse perspectives. Further rationale for choosing this method has been provided in the succeeding section.

2.2 Nonsystematic Literature Review

We utilized a *nonsystematic LR* to identify earlier constructs, models, theories, as well as results and generalizations of earlier empirical studies relevant to the objective of this study. The same methodology has been used to establish relationships among constructs and with the hypothesis. In contrast to a systematic LR, a nonsystematic LR is not obligated to be explicit about the methods used. In terms of the SALSA framework [15], which signifies the four key elements or basic steps of a systematic LR process: Search (define search keywords and databases to be searched), Appraisal (pre-defined literature inclusion and exclusion, and quality assessment criteria), Synthesis (extract, summarized, and categorized the data), and Analysis (synthesize the literature and finally reach a conclusion), the LR used for this study did not follow explicit methods, particularly for the first two steps. However, in order to ensure the quality of selected literature, we used mostly peer-reviewed journal and conference papers, and the remaining are reports from EU, national and private organizations with a reputation for security research. Some organizations whose reports have been referred are ENISA, NIST, SANS Institute, HP, Microsoft, Kaspersky, Hoxhunt, PCI, SEI, ISC2, Osterman Research, Universities, and government ministries.

Designing a CSA framework is a very wide domain and encompasses knowledge and understandings from various disciplines, such as cybersecurity, teaching and learning, psychology, and human behavior, IT and Internet, economics, and so on. A nonsystematic LR would be the best option to cover such a wide range of domains. It will provide the flexibility and ability to cover a wider and more inclusive view of available research on the needful domains [16]. The literature selected for the review includes both academic papers (e.g., peer-reviewed journal, conference, and workshop papers) and industry reports (e.g., technical reports) with an intention to integrate both theoretical as well as practical findings on the topic.

Initially, we summarized (the summary is chronologically presented in Annex A: CSA Frameworks) and analyzed the existing nine CSA frameworks with an intent to determine the important phases, sub-phases, and activities in a CSA program, which eventually act as the skeleton of our framework. Next, we reviewed numerous relevant pieces of literature to comprehend "*what to do*" in each activity and correspondingly "*what to expect*" at its end. The final results have been presented in the form of guidelines and practical advice.

2.3 Online Survey

We also used an online survey about CSA posters in order to determine the degree to which each poster satisfies the presumably ideal properties for awareness posters. These properties were elicited using the LR. The evaluation includes 117 posters from organizations like ENISA [17], EUROPOL [18], Cyber Safe Work [19], Global Knowledge [20], SANS Institute [21], and INFOSEC Institute [22] that are available for free. We received valid submissions for 94 posters. Due to some unknown issues in Google Form, submissions for some posters did not register in its spreadsheet.

In order to carry out the survey, a Google Form survey was created. Each poster was displayed with the set of properties and the participants had to assess to what extent the poster satisfies the given properties in terms of a five-point Likert scale (Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree). All the posters evaluated in this study were in English. The evaluation was performed only by the team members from partner organizations contributing/participating in this task/deliverable, who had a consensus on the interpretation of the properties. Even though localization is essential to improve the effectiveness of CSA posters (and in general), this study did not evaluate it mainly because of these reasons: i) posters available in multiple languages had no other changes except a translation of the awareness text (it was not a complete localization), and ii) a very few posters were available in multiple languages.

3 Review of the Existing CSA Frameworks

In the beginning, this section provides a brief summary of the nine identified and selected CSA frameworks. This is followed by a comparison of all the other frameworks with the ENISA framework to derive the most important phases and sub-phases in a CSA program that will be used for the new proposed framework. Next, it defines and differentiates the monitoring and evaluation. Finally, it includes the state of the art in order to answer why this study is relevant.

3.1 Summary of the Selected CSA Frameworks

A brief summary of all the selected CSA frameworks has been presented in chronological order in Table 1. The key concepts of these frameworks in detail have been discussed in Annex A: CSA Frameworks. These CSA frameworks focus on several factors and levels: individual, organizational, societal, and technological factors. However, in this report each of the identified and selected frameworks has been discussed considering only two characteristics:

i. the scope (goals and domains), and
ii. the main steps/phases of the framework

Table 1: Comparison of different CSA frameworks

Framework	Goals	Domains	Main Phases/Steps
Vroom & von Solms (2002) [23]	Information security awareness program	Organizational	• Establishing the needs for information security awareness (Needs assessment) • Using sources for the information security awareness program (Standards to follow) • Responsibility of developing the information security awareness program (Team setup) • Constructing information security awareness program (Content preparation-intensiveness level)
Wilson & Hash (2003) [9]	Security awareness & training program	General, Organizational	• Designing an awareness and training program (Needs assessment; Strategy and plan-standards, define scope/ team/goals/objectives, topics selection, and other planning; Establishing priorities- implementation schedule; Setting the bar - intensiveness; Funding) • Developing awareness and training material (Developing awareness materials- topics selection, sources of materials) • Implementing the awareness and training program (Communicate the plan- get support, Delivery methods) • Implementing post phases (Monitoring compliance; Evaluation and feedback management; Managing change; Ongoing improvement- raising the bar)
ENISA (2010) [10]	Information security awareness	General, Organizational	• Planning, assessing, and designing (Team setup; Establishing goals and objectives; Identifying target group; Evaluating potential solutions; Funding; Defining communication; Defining indicators to measure success; Establishing a baseline for evaluation…) • Executing and managing (Confirming team; Reviewing plan; Launching and implementing the program; Delivering communication; Documenting lessons learned)

			• Evaluating and adjusting (Conducting evaluation and review; Implementing lessons learned; Adjusting the program as appropriate; Relaunching the program)
Kortjan & Solms (2014) [11]	Cyber security education and awareness	General, Organizational, National	• Strategic layer (Strategic planning; Forming team) • Tactical layer (Establishing partnerships with private and public sectors, academia, and other nations; Selecting potential communication tools) • Preparation layer (Identifying topics; Preparing content; Selecting suitable delivery media and tools) • Delivery layer (Identifying the target audience; Defining stakeholder's responsibilities) • Monitoring layer (Declaring benchmark for evaluation; Defining success indicators; Generating periodic status report) • Arranging resources to execute activities in each layer, (People; Information; Applications; Infrastructure; Funds)
Beyer et al. (2015) [24]	Cyber security awareness	Organizational	• Awareness profiling (company profiling; assessing the existing awareness program, including gap analysis; preparing awareness maturity level report) • Awareness planning (establishing goals and objectives; defining roles and responsibilities of the team members; planning overall activities of awareness program; planning improvements required for the existing awareness program) • Transforming plans into actions (creating, producing, and implementing measures; getting support from the internal core team) • Optimizing (comparing target state and actual state; adjusting and optimizing the program)
Ki-Aries et al. (2016) [25]	Information security awareness	Organizational	• Establishing needs and goals • Developing personas of the target audience based on empirical data collected through interviews and observations • Analyzing the personas against needs and goals to recommend suitable awareness approaches • Designing and developing awareness materials based on communication media and available funds • Implementing the program • Reviewing, evaluating, and optimizing the program
Ghazvini & Shukur (2017) [26]	Information security awareness	General, Healthcare	• Selecting information security topics • Refining information security policy • Developing awareness training content for the selected topics and security policies • Creating the target audience profile • Organizing the delivery process of the program • Defining the success factors • Determining the organization training needs assessment
Wang et al. (2018) [27]	Cyber security awareness	General, National, Organizational	• Understanding the threat landscape and relevant risks. • Assessing the security knowledge, skills, and risk understanding level of the audience

			• Preparing the awareness resources and implementing the program
Bada & Nurse (2019) [2]	Cybersecurity education and awareness	Small and medium-sized enterprises (SMEs)	• Engaging with Small and Medium-Sized Enterprises (SMEs) (Engaging and communicating with the target audience; Providing simple and practice advice relevant to the target audience- helping to understand the importance of CSA) • Improving security practices and culture (Performing needs assessment; Planning to address the risks; Implementing, testing, and refining CSA program; Reviewing the impacts of CSA program) • Preparing program resources (Using vetted resources; Focusing on general and specific topics) • Utilizing trusted third-party resources/services (Partnering with a vetted list of third parties) • Communication strategy (Communicating with stakeholders)

3.2 Comparison of the Selected CSA Frameworks

The ENISA framework has been used as the basis for comparison with other remaining CSA frameworks. The ENISA framework focuses on European organizations and citizens' needs and is relatively the most holistic and detailed among all, thus making it suitable as a baseline for the comparison. Particularly, the compared frameworks have been analyzed according to the three main processes and their respective sub-processes:

i. Plan, Assess, and Design,
ii. Execute and Manage
iii. Evaluate and Adjust

Table 2 illustrates the accordant sub-processes that each framework supports. This comparison is performed necessarily to determine the important phases and sub-phases in a CSA program that will also act as the skeleton of our proposed framework. While making this comparison, we encountered most frameworks do not have the process and sub-process differentiated as explicitly as they are in the ENISA framework. In that situation, we looked into the compared framework's description to determine whether it includes aspects that can correspond to the activities of the ENISA framework's process and sub-process to realize if they exist.

Table 2: Comparison different CSA frameworks with the ENISA framework

	A Plan, Assess & Design														B Execute & Manage					C Evaluate & Adjust						
ENISA [10]	A-010	A-020	A-030	A-040	A-050	A-060	A-070	A-080	A-090	A-100	A-110	A-120	A-130	A-140	B-010	B-020	B-030	B-040	B-050	C-010	C-020	C-030	C-040	C-050	C-060	C-070
Vroom & von Solms [23]			✓	✓	✓	✓	✓	✓			✓				✓		✓	✓		✓	✓					
Wilson & Hash [9]	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓		✓			✓			
Kortjan & Solms [11]		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓		✓			✓			
Beyer et al. [24]			✓	✓	✓	✓	✓	✓			✓		✓		✓		✓	✓		✓		✓			✓	✓
Ki-Aries et al. [25]			✓	✓	✓	✓	✓				✓						✓	✓		✓		✓		✓	✓	✓
Ghazvini & Shukur [26]			✓	✓	✓	✓	✓				✓		✓				✓	✓		✓		✓	✓		✓	
Wang et al. [27]			✓	✓	✓	✓	✓				✓						✓	✓		✓	✓		✓			
Bada & Nurse [2]			✓	✓	✓	✓	✓				✓						✓	✓		✓			✓		✓	

A-010 Establish Initial Program Team

A-020 Take a Change Management Approach

A-030 Define Goals and Objectives

A-040 Define Target Group

A-050 Identify Personnel and Material Need for the Program

A-060 Evaluate Potential Solutions

A-070 Select Solutions and Procedure

A-080 Obtaining Appropriate Management Support and Funding

A-090 Prepare Work Plan

A-100 Develop the Program and Checklists of Tasks

A-110 Define Communications Concept

A-120 Define Indicators to Measure the Success of the Program

A-130 Establish Baseline for Evaluation

A-140 Document Lessons Learned

B-010 Confirm the Program Team

B-020 Review Work Plan

B-030 Launch and Implement Program

B-040 Deliver Communications

B-050 Document Lessons Learned

C-010 Conduct Evaluations

C-020 Gather Data

C-030 Incorporate Communications Feedback

C-040 Review Program Objectives

C-050 Implement Lessons Learned

C-060 Adjust Program as Appropriate

C-070 Re-Launch the Program

Sub-processes common in all the compared frameworks and their corresponding sub-phase incorporated in the proposed framework are given in Table 3. Since CSA is a continuous effort, we have also included "*Lessons Learned*" and "*Adjustment*" in addition to the common sub-processes. These added sub-phases are necessary to improve the CSA program for subsequent or future iterations.

Table 3: Common sub-process and their corresponding sub-phase in the proposed framework

Common Sub-Processes	Corresponding Sub-Phase in Framework
• Define Goals and Objectives • Define target group	Establish Goals and Objectives
• Identify Personnel and Material Need for the Program • Evaluate Potential Solutions • Select Solutions and Procedure • Define Communications Concept	Resource Preparation
• Launch and Implement Program • Deliver Communications	Message Delivery
• Conduct Evaluations	Evaluation

3.3 Monitoring and Evaluation

Before delving into the actual framework and guidelines, it is important to understand the meaning of *monitoring* and *evaluation* and their differences. Monitoring is a routine tracking of inputs/activities and their respective outputs to determine how well a program is being implemented and is proceeding as planned. This usually focuses on processes and begins when the program starts and continues throughout the program's operational period. Monitoring is necessary to know the ongoing interventions required to direct the program to the expected outcome. In contrast, evaluation is conducted at specific moments and permits an assessment of a program's progress over a longer period of time. The evaluation focuses more on the outcome and impact level [28]. The main difference between monitoring and evaluation is illustrated in Figure 1 where monitoring routinely measures activities/inputs and their respective outputs, whereas an evaluation focuses on measuring outcomes and impacts with respect to the goals and objectives set at the beginning of the program. Finally, discrepancies detected by monitoring could accentuate the need for evaluation.

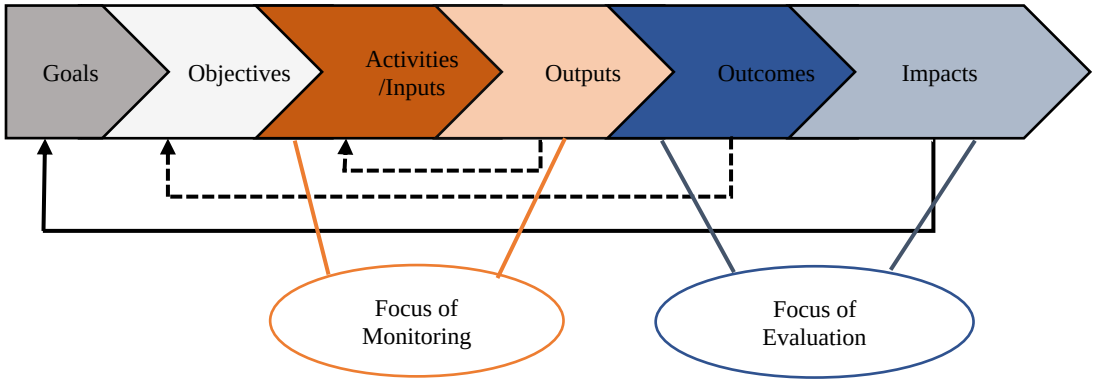

Figure 1: Difference between monitoring and evaluation [28]

4 Unified Conceptual Framework

A clear framework is essential to guide monitoring, evaluation, and enhancement of a CSA program. It should lay out the components of the initiative and the order or the steps required to accomplish the targeted outcomes, explaining how the program is expected to work. A framework clarifies the program's goals and objectives, establishes the links between important (both internal and external) components, and articulates how they should function and could affect the program's success. The developed CSA framework obtained after the review of frameworks listed in Table 1 and its consolidated information is shown in Figure 2. In general, the CSA program can be divided into three phases:

- *Pre-implementation phase*: In this phase, all the preparations for the program are done (Section 5). This preparation includes setting up the team (Section 5.1), establishing the program's needs, goals, and objectives (Section 5.2), selecting relevant topics (Section 5.3), and finally preparing contents and delivery methods for the program (Section 5.4).
- *Implementation phase*: In this phase, the program is executed or implemented (Section 6). This involves reaching out to the audience and delivering the awareness content to them in a way that can motivate them to learn cybersecurity (Section 6.2) and convert learning into action and behavior (Section 6.3).
- *Post-implementation phase*: In this phase, the effects and impacts of the program are assessed and measured (Section 7). This is necessary to realize the improvements required to achieve the expected goals (Section 7.1), but also to keep the programs up-to-date and relevant to the audience in future iterations (Section 7.2).

Each phase has multiple sub-phases that again comprise multiple activities. Sub-phases and activities represented by hardline borders are mandatory, and those represented by dotted border lines are optional. Optional sub-phases are done if needed or specified by the sponsors. For example, the Pilot Test can be of value if it is the first iteration, but for any iteration after the first, it may not be necessary. Similarly, a one-sided arrow indicates the flow of the program or activity that influences another activity. For example, if the CSA program targets managers and decisions makers in the organization, the message framing should be accordingly in the language understandable to them.

Attaining lasting changes in security attitudes and behavior requires CSA to be an ongoing program that has to be organized frequently. This, in a way, leads to revisiting, reviewing, and updating the current CSA programs for subsequent or future iterations. This essence of CSA is represented by the cyclic order of phases similar to other existing frameworks.

The motive of this derived framework is not to explain what each phase and sub-phases is meant for or what to do in each of it, which tentatively all the reviewed frameworks have already done to an extent. This framework intends to provide and explain the aspects that have been left unanswered by the frameworks developed in the past. It provides the guidelines that can be utilized to monitor different phases and sub-phases of a CSA program, and finally, evaluate its overall success. Since we already have worked on CSA program evaluation in another deliverable D9.13 [29] of CyberSec4Europe, this report primarily focuses on and contributes to CSA program monitoring.

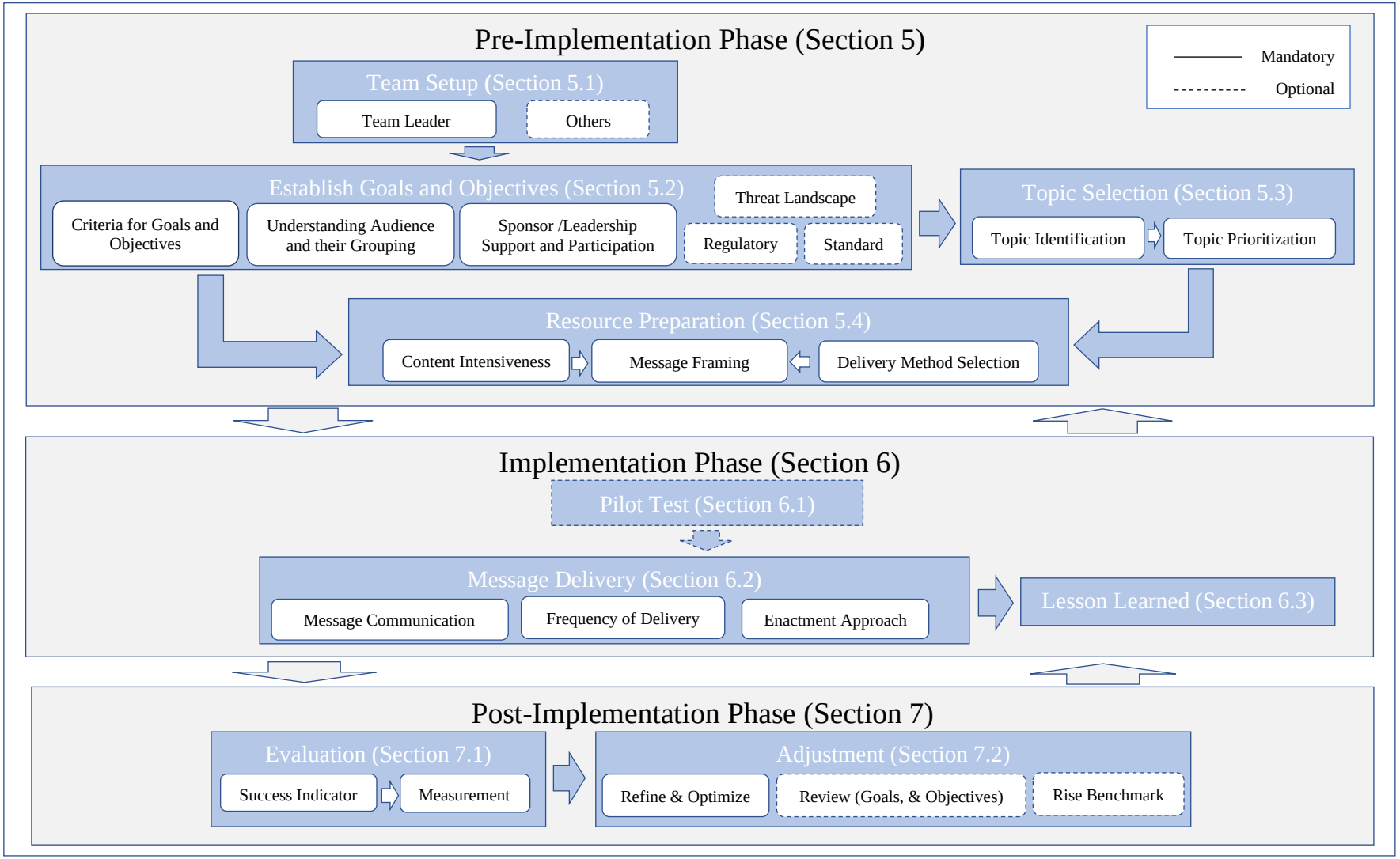

Figure 2: Consolidated CSA framework

5 Pre-Implementation Phase

5.1 Team Setup

The team is responsible for the development, delivery, and maintenance of CSA resources. Its efficient functioning and coordination are crucial for the success of a CSA program [30].

5.1.1 Team Leader and Others

The SANS Institute's study [31] found out that for most cybersecurity professionals in organizations, a responsibility to raise awareness is an addition to their other job responsibilities; over 75% of the professionals spend less than half their time on CSA. This is especially important because results from the same study established a correlation between full-time cybersecurity professionals an organization has and its ability to achieve *CSA maturity* (refer to [32] for CSA maturity levels). The study further revealed that an organization with at least two full-time cybersecurity professionals is more successful in changing its employee's security behaviors and the overall security culture of the organization. Therefore, preferably it is advised to have at least two full-time CSA professionals in an organization. For organizations, such as small and micro enterprises with resource constraints [33], at the very least an individual should be assigned for the development and implementation of a CSA program [34].

Moreover, the same study also ascertained that a majority of CSA professionals (around 80%) come from technical backgrounds [31]. Definitely, a technical background is an advantage, but these professionals often lack the *non-technical skills* (also referred to as *soft skills*) necessary to communicate the CSA contents and engage the audiences in a way that motivates them to learn and practice cybersecurity [31] [35]. Due to the missing skills, CSA professionals fail to align what they intend to communicate with what their audiences want to comprehend and apply. Therefore, it has been recommended to have someone with predominately soft skills as a CSA professional [31]. Winkler & Manke [36] have suggested some soft skills specifically required in CSA professionals. Similarly, a more comprehensive list of soft skills essential for successful cybersecurity advocates has been elicited by Haney and Lutters [35], which can be equally valid for CSA professionals. A consolidated list of soft skills obtained from these two studies and the ways they can be leveraged for CSA purposes is presented in Table 4.

Table 4: Soft skills for cybersecurity advocates [35] [36]

Soft Skill	Description
Communication skills	The individual should have the ability to frame communications for diverse audiences and communicate in terms the audiences best understand. These require him/her to have skills to: • use a variety of communication approaches, such as videos, presentations, blogs, training classes, etc., and • motivate and engage diversified audience types, for example, use imagery or metaphors to explain technical concepts to non-technical audiences.
Familiar with learning concepts	The individual should have knowledge and understanding of different concepts of learning, and also know how to effectively employ them for CSA purposes.
Knowledge of awareness tools and techniques	The individual should be familiar with various tools and techniques designed for awareness purposes.
Personal attributes	The individual should exhibit humility (see, listen, and accept others), a positive attitude, and optimism towards solving security problems.

Career and collaborative attributes	The individual should have critical thinking, adaptability, and innovativeness. These require him/her to have: • an ability to be flexible in the face of changing circumstances and new information, and • realize the importance of cultivating partnerships and building consensus.
People skills	The individual should possess an understanding of human behaviors, biases, limitations, and the ability to build relationships (rapport and gain trust). Further, the individual should have empathy (have a conversation and think from the perspective of the person an individual is working with) and know the best ways to reinforce the desired behavior to the audience.

In addition to technical and soft skills, the individual should be *context-aware*, i.e., understand each group has different sets of values, challenges, and strengths [35]. The CSA professional should know the audience, including their level of awareness of the security issue, their needs, and the issues they are concerned about, as well as where they get the information and what information they prefer to receive [10]. This requires the CSA professional to:

- have an awareness of the environment, including the technology, people, and social and cultural structure,
- understand and communicate the '*why'* behind security recommendations and how security can be beneficial,
- look at the bigger context and provide accurate and sensible technical guidance, and
- recognize and understand the barriers (that may come from economic, social, political, or structural issues) others face when trying to make decisions about implementing security practices, and at the same time also try to devise ways to overcome these barriers.

The other team members should be staffed with personnel from different expertise areas or departments of the organization [10] [37] if possible, for example, IT, human and resources, finance, legal, marketing, risk management, and privacy and physical security, etc. In an organization, this partnering with other departments can help in three ways:

- avoiding resistance or obtaining support from these departments for CSA in making it mandatory [10],
- helping to understand the audience (e.g., their specific concerned security issues and dissemination channels effective for them) in the department, and
- possibly getting additional resources, such as funding and distributions [38].

Many small organizations may not have distinct departments, in that case, they should engage the unit or team manager with authority and who understands the overall operations as well as possess both persuasion and necessary technological skills.

EXTRACTED GUIDELINES

- Team size and membership are dependent on the needs; however, the team should have a dedicated full-time CSA professional (preferably as a team leader) [31] who is equipped with both technical and soft skills and is context-aware [35].
- Other team members should be people from groups applicable to cybersecurity and other different expertise areas (departments of the organization) [10] [30] [37]. Such a team will have the ability to understand the needs and problems from multiple perspectives.

- The roles, responsibilities, and accountabilities of each team member, including the team leader should be clearly defined in a way that aligns with the goals and objectives of the program [9] [10] [30].

5.2 Establish Goals and Objectives

A goal is a strategic outcome that a program intends to achieve at a high level, whereas an objective specifies measurable steps/actions/results that are needed to attain the goal [39]. The goal and objective serve to uphold the reason for creating the program, i.e., what the program wants to achieve, and can be exclusive to a target group. The needs (or baseline) for a CSA program can be identified by conducting a *needs assessment* [9] [30]. Moreover, threat landscape reports, regulatory bodies (when required to comply with national or regional regulations, e.g., awareness on GDPR compliance), standardization bodies (when required to obtain standards certification, e.g., ISO 27001 compliance), and groups working in cybersecurity can also help in establishing goals and objectives [23] and also provide reference materials that may help in the development of a CSA program [37].

5.2.1 Criteria for Goals and Objectives

In general, a goal to be accomplished should be clear and simple. However, properties like clarity and simplicity are dependent on individual interpretation. A relatively concrete guide in the setting of objectives is the SMART criteria [40]. These criteria could also be applicable for establishing the objectives of a CSA program. The SMART acronym stands for:

- *Specific*: definite security threat or issue, policy, regulation, and others of which the program expects to raise awareness.
- *Measurable*: quantifiable indicators (how much/many) to measure the progress of goal/objective.
- *Attainable*: realistic and achievable goal/objective based on constraints like budget, time, resources, scope, and others.
- *Relevant*: goal/objective applies to the problem the target group or organization faces and has a positive *ROI*.
- *Time-bound*: definite starting and ending points to reach the goal/objective.

The *measurable* objective is crucial to continually monitor and analyze the success of a CSA program. Against this objective and baseline, the effectiveness of the program is monitored and evaluated, and accordingly, the program is updated and optimized for subsequent iterations.

Examples of goals and their respective objectives are shown in Figure 3.

Goal: Achieve compliance with the required EU regulations and directives

• **Objectives**:
  • Achieve GDPR compliance
  • Achieve ePrivacy Regulation compliance
  • Achieve NIS Directive compliance

Goal: Identify and manage human risks to an acceptable level

• **Objectives:**
  • Reduce accidental data loss incidents by 70%
  • Reduce costs related to human-related incidents by 50%
  • Improve incident reporting to 100%

Figure 3: Examples of goals and their respective objectives

EXTRACTED GUIDELINES

- The goals and objectives should support the reason for creating the CSA program (or the security behavior ought to be reinforced).

- The goals should be clear and simple. The SMART criteria should be used for establishing the objectives of a CSA program [40].

5.2.2 Understanding Audience and their Grouping

In order to design, develop, and implement a CSA program effectively, it is necessary to know the audience that the program intends to reach and their behaviors. Based on the knowledge-behavior spectrum, the audience's behavior can be broadly classified into the *rebel*, the *discerning*, the *oblivious*, and the *obedient* [41]. It is the rebels who are the most challenging to change through a CSA program. Similarly, Stanton et al. [42] have developed the taxonomy of end-user security behaviors based on intentions and expertise. Their taxonomy categorizes the security-related behaviors into *detrimental misuse*, *intentional destruction*, *naïve mistakes*, *dangerous tinkering*, *basic hygiene*, and *aware assurance*. Among these categories, the earliest two behaviors (which are deliberate malicious acts) are presumably impractical to target using CSA. However, the middle two behaviors (i.e., naïve mistakes, dangerous tinkering) that CSA should target and shift them towards the latter two behaviors respectively. Knowledge and understanding of these different behaviors that people enact can be beneficial for CSA professionals and teams, who intend to influence or motivate their target group to change security behavior.

Furthermore, audience feedback can highly contribute to the design, development, assessment, and update of a CSA program. Their *socio-demographic factors* (e.g., age, gender, education level, the field of study, occupation, job hierarchy, frequency of ICT usage, prior cyber-attack experience, and job experience) [43], *cultural values* (e.g., Hofstede's cultural dimensions theory) [44], and *personality traits* (e.g., Big five personality traits) [45] can be useful information in shaping the CSA program so that it best fits their needs and requirements. One must also realize that the impacts of some of these factors may overcome others [41].

It has been found that the below 30 years age group is relatively more risk-taking in nature than other age groups [46] [43]. This age group, irrespective of their academic qualification and organizational position, was found to be less inclined towards compliance with security practices [41]. Similarly, females are more vulnerable to cyberattacks than their male counterparts [46] [43], which may be because they are less technology savvy [46] or have different personality traits (essentially a form of neuroticism) [47] [48], however, they are found to be more conforming to security practices [41] [49]. Moreover, factors like individuals with higher education level, prior exposure to cyberattacks, high frequency of ICT usage [43] [50], study and occupation from IT-related disciplines [49], and more years of job experience [51] are found to be more well behaved from security perspectives. Next, individuals from a certain national culture show more compliance to security behavior than those from other cultures [49] [44]. Among the five of Hofstede's cultural dimensions, power distance (significantly negative), individualism vs. collectivism (significantly positive except for technical measures), and long vs. short-term orientation (failed to pass the significant test) are found to have a correlation with the cybersecurity development index [52]. This implies that countries with smaller power distance and high individualism tend to have a high level of cybersecurity development index. In the same way, uncertainty avoidance, power distance, individualism vs. collectivism, and masculinity vs. femininity are found to have a stronger effect on intention towards smartphone security behavior [44]. Finally, the answer to employees' security behavior can partly lie in their personality traits. Among the five psychological traits (big five personality traits [53]), it has been found that an individual who scores high in *neuroticism* and *openness* is more likely to respond to prize scams and is less strict about privacy settings respectively [48]. Although there does not exist a direct relation between personality traits and information disclosure, an individual scoring high in *openness* is found to spend more time online, and online time is found to be significantly correlated with information disclosure to unknown persons and friends in online communities [54]. Such revealing nature can make the individual more susceptible to spear phishing and hacking, for instance, the revealed information can be used to design and send a customized spear-phishing message or to guess password and security questions. Identically, *neuroticism* is

found to be negatively correlated with secure cyber behaviors whereas individuals high in *conscientiousness* are less likely to engage in insecure cyber behaviors [55]. Apart from that, the type of devices that employees use for their work purposes, such as BYOD or smartphones, also impact their security behaviors [44]. For example, smartphone users are found to be poor at security behaviors irrespective of their background [44]. The bottom line is "*one size fits all*" tendency in CSA does not work, and thus, different audience groups, even if they pose the same security risks, may require to be treated differently.

Although the audience can be categorized or grouped based on different factors (e.g., behavior, profession, culture, age group, education level, etc.), for CSA purposes using pre-existing beliefs and cybersecurity expertise makes the best criteria [56]. In the case where it is not possible to use the two recommended criteria, other relevant factors can be used to categorize the audience group.

EXTRACTED GUIDELINES

- The audience categorization or grouping should be done based on their pre-existing beliefs and cybersecurity expertise [56]. Another relevant factor for the audience grouping is security behavior. However, determining these factors required an assessment of the audience beforehand.
- In an organization, the grouping should be role-based (i.e., employees' roles and responsibilities in the organization) [37].
- In the situation where these factors are difficult or infeasible to obtain, other discerning factors like profession, education level, culture, and age group should be utilized to categorize or group the audience.

5.2.3 Sponsor /Leadership Support and Participation

The sponsor's or leadership's support for a CSA program directly affects the priority level it will receive. In an organization, full support of the leadership is found to be vital for CSA success [23] [34] [40] [57]; the programs that have garnered the support of top management are more successful [38]. This could be because of various reasons. Firstly, the leadership or sponsor holds the authority over the budget, and without his/her support, any cybersecurity program including its awareness will suffer a fund and other resource deficit. Secondly, the leadership is often authorized to access sensitive information and cyber assets so should participate in a CSA program and be aware of the cyber risks s/he may encounter or is susceptible to. Thirdly, the leadership displaying a commitment towards the program will send a positive message to employees [58] and presumably motivate them to participate in the program and practice the knowledge learned. Finally, the leadership's support will help to gain support from all other departments in the organization for the program [59].

There are different constructs in practice to frame cybersecurity information so as to motivate finance decision-makers and change their mental model towards cybersecurity. These constructs chiefly explain, for example, risk of breach, the potential loss from a breach, benefit of cybersecurity, cost of mitigation, performance comparison with similar firms, etc. [60] [61].

The leadership should contribute to and participate in a CSA program in the following ways:

- Cybersecurity should be on the agenda of the organization's leadership since s/he holds the authority of the budget, and without his/her support, any CSA program will suffer a budget deficit.
- Using the *top-down approach* [62] in CSA and engaging the leadership in practicing good security behaviors will set positive examples and possibly motivate other employees to adopt the same good security behaviors as well.
- The leadership holds the authority to access sensitive information and cyber assets, so s/he should be aware of the cybersecurity risks they may encounter or are susceptible to.

While specifying the fund for CSA, it can be expressed in terms of, for example, percent of overall learning and development budget, percent of overall IT security budget, allocation per target individual, or an explicit amount for each component required for the overall implementation [9]. In this, the value of percent depends on the CSA maturity level of the organization. Organizations with CSA programs in place, i.e., most of the resources are available, may require allocating less percent of funds for CSA than those in their first CSA program. To be specific, it has been suggested to spend 40% of the first-year IT security budget on CSA [34].

EXTRACTED GUIDELINES

- The CSA program should receive appropriately high priority. This is indicated by, for example,
  - allocation of adequate budget for CSA programs,
  - participation of leadership in CSA programs relevant to his/her roles and responsibilities, and
  - practice of security behaviors by the leadership.
- The funds for CSA should be asked in terms of one of the following:
  - percent of overall learning and development budget,
  - percent of overall IT security budget,
  - budget allocation per target individual,
  - an explicit amount for each component required for the overall program implementation.

5.3 Topic Selection

Various techniques like survey, interaction, and others are utilized to elicit relevant CSA topics. In the case of a small enterprise, relying on a small sample of qualitative or even informal chat with employees (that include management and specialized roles) at the organizational level [10] can be sufficient and economical. However, for other organization types, a variety of sources can be used for a needs assessment that includes but is not limited to interviewing different key groups, reviewing the current CSA initiatives, analyzing cyber incidents to the organization or trends in the industry, reviewing technical or infrastructure changes made in the organization, and so forth [9]. An equally viable technique is to utilize materials like cybersecurity landscape published by various organizations, for example, ENISA [63] and others to get an overview of cyber threats, together with current and emerging trends. These topics should be of interest and use to the target audience.

5.3.1 Topic Identification

It is essential to analyze the needs and demands of the audience and identify CSA topics prevalent and relevant to them. When doing so, ideally it is recommended to consider the goals of the organization (specifically what the organization does and the critical assets it possesses) but one must consider the following [23]:

- *Include common threats*: Every audience group's risk profile and threat landscape differ, however, there are common threats that most of the audiences have to deal with, for example, social engineering, ransomware, and malware attacks.
- *Include threats relevant and prevalent to the target group or organization or industry:* CSA topics should be inclusive of all relevant and prevalent threats to the target group, organization, or industry based on their job definitions, business goals, and risk profiles.
- *React to new events and situations:* Reactive measures should be launched in response to events and situations [10], for example, new laws and regulations; new or updated security policies, procedures, standards, or guidelines; implementation of new technology; new employees, contractors or outsourced personnel; new management; more automation; launch of new product

and services; acquisition, mergers, and divestitures; recent security breaches, threats, and incidents; new risks; certification, etc.

- *Proact to potential future threats*: Security is an ever-evolving field, with new threats and techniques, countermeasures, and philosophies born each day. The awareness should consider the dynamically changing risk environment within which most organizations are expected to survive and thrive.

EXTRACTED GUIDELINES

- Topics should be relevant to and align with the roles and responsibilities of the audience (or the goals and objectives of their organization). Moreover, they should be inclusive to cover everyone in the audience group [64].
- Topics should cover:
  - common threats,
  - threats relevant and prevalent to the audience group or organization or industry,
  - reaction to new events and situations, and
  - proactiveness to potential future threats [10].

5.3.2 Topic Prioritization

Every CSA topic may not be feasible to cover, so categorizing the cyber threats and prioritizing those that are highly damaging, and imminent can be a good compromise. And for this purpose, the *probability/impact matrix* can be used [65]. The matrix will help to identify the threats with high-risk levels (i.e., severe impact and more likely to occur).

More explicitly, the following key factors can be helpful during the prioritization of CSA topics:

- *Specific roles and security controls*: CSA topics relevant to the employees who get access to and interact with sensitive cyber assets should get preference over those who do not. This will reduce the number of attendees, minimize the general overhead in terms of course materials and time away from workplace productivity, and more importantly, add a long-term value for attendees [66].
- *Organizational role and risk*: Broad-based CSA topics that address the enterprise-wide mandate can receive high priority.
- *Critical project dependencies:* CSA topics related to critical projects can receive high priority.
- *State of current compliance* [9]: If there is any known or existing major gap in compliance or awareness, this can receive high priority.
- *Availability of resources* [9]: If the required resources (e.g., course materials and instructors) for an awareness topic are readily available, this can be scheduled early; otherwise, it has to wait until requirements are ready.

EXTRACTED GUIDELINES

- It is important to prioritize the topics. The following topics should receive high priority:
  - that specific to critical security roles and controls,
  - that relative to critical projects,
  - that align with the organizational role and risk,
  - that is important but neglected by the target audience (i.e., low adherence), and
  - that has resources readily available.

5.4 Resource Preparation

It is not always necessary to design and develop every resource for a CSA program. There is a variety of awareness and related materials available on the Internet that can be incorporated into a CSA program [9] [10]—some freely available CSA materials have been listed in report D9.11 of CyberSec4Europe [67]. Such materials are produced and distributed by various European agencies & organizations, academic and research institutions, European federations, National organizations for cybersecurity, and European and national funded projects. The materials can address a specific issue, or in some cases, can describe how to begin to develop an entire awareness program, session, or campaign. They can be on general cybersecurity issues or issues specific to a business sector. Access to such materials can be free of charge, on a fee basis, or only for members. However, before using such materials, they must be reviewed to know if they suit the needs of the program or require any tailoring. Whether the awareness materials are self-designed and developed or obtained from third-party sources, it is advisable that they satisfy the guidelines in sections 5.4.1, 5.4.2, and 5.4.3.

In general, CSA materials must align with the goals and needs of the target audience and organization [9]. Moreover, their development should be affordable, fit the target organization's culture and infrastructure, and not require effort-taxing activities that can slow down the users' tasks. Specific properties wise, the awareness materials should be accessible, suitable for the user's circumstance and situations or conditions, communication strategies and techniques that suit the preference of the users, interactive and innovative to engage the audiences, and be inclusive so that no subset of the audience feels left out. Some ways to achieve them are to comprehend and incorporate factors like audience's roles, prior knowledge, and experiences, learning styles, and security perceptions or misconceptions [68] while developing or tailoring the materials. Moreover, integrating *threshold concepts* (i.e., provide the audience with an ability to integrate different aspects of cybersecurity into the analysis of a problem) [69], for example, through analysis of real-life problems (*problem-based learning*) or scenarios (*case-based learning*) can help in framing the messages in the way that would potentially yield a better result [70]. Apart from that, they should include features for tracking capabilities (e.g., self-assessment and feedback that can help verify whether people are actually learning by using them and allow interested people to participate and contribute to the future improvement of the awareness materials) and asking questions (where the audience can ask questions to address concerns at the earliest possible time).

5.4.1 Content Intensiveness and Complexities

Each audience group should be delivered the right depth or intensiveness of CSA appropriate to their personal or professional life. Doing so will interest them in the CSA program and increase their participation and the chance of incorporating the learned things into practice [9]. Broadly, the intensiveness of CSA activities can be *general, intermediate,* and *in-depth* depending on the increasing level of risks the target audience is expected to encounter [9] [64].

- *Advanced or in-depth level*: Suitable for specialized roles and some management whose jobs incorporate the highest level of trust and accompany a high level of IT security responsibility.
- *Intermediate level*: Suitable for management, decision-makers, and some specialized roles, who are more experienced and assigned with more responsibility in a discipline.
- *Beginner level*: Suitable for general population/employees not working in IT security and beginners of IT security.

The different intensiveness of a CSA program influences the design of its content. For example, in an organization, the higher authority employees such as decision-makers and those with specialized roles have complete access to sensitive information and other digital assets, so the level of cybersecurity risk they

possess is higher than other personnel. In case of compromise, they can cause the most severe harm to the organization. Moreover, their needs and expectations from CSA differ from other employees, as shown in Figure 4 [64]. Besides, there are some cybersecurity activities common to a particular department in the organization (e.g., people in the accounting department can be exposed to different threats than those in the HR department) or some cyber threats that are common to all employees (e.g., social engineering), about which they all need to remain fully aware. The content intensiveness and complexities should be mainly based on these two criteria: i) the target audience category (e.g., position within the organization), and ii) knowledge of security skills required for the target audience group [9].

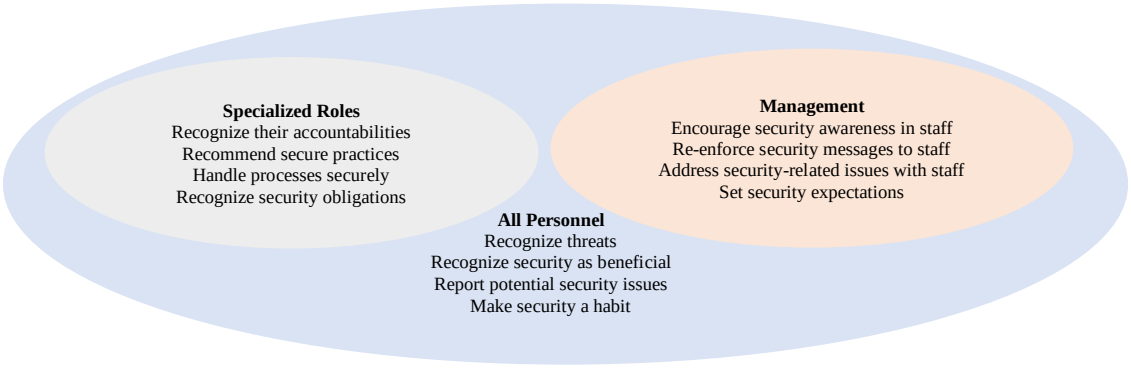

Figure 4: CSA roles for organizations [64]

EXTRACTED GUIDELINES

- The content intensiveness and complexities should be based on these two main factors:
  - the target audience group, and
  - the knowledge of security skills required for the target audience [9].
- The content intensiveness should be adjusted from general to in-depth depending on the audience type [9] [64].

5.4.2 Message Framing

The content presentation continues to be a critical concern especially because it has significant impacts on how the information will be processed in the memory and affect the decision-making performance of the audience [71] [72]. Moreover, message framing affects the amount of persuasion it elicits [73]. Effective content is not just about what has been expressed but more importantly how it will be received, interpreted, and absorbed by the users. The same message can be framed and communicated in different ways without changing its facts, resulting in varying effects on people. Furthermore, a complex issue can be communicated in a simple and convincing manner if it is framed effectively, and on the contrary, a simple problem can become confusing and difficult to understand if it is poorly framed.

Although there does not exist consensus upon what properties can make CSA contents more effective and usable, some studies have attempted to draw out relevant properties for awareness message framing [3] [4] [5] [10] [56] [68] [58] [74] [75] [76] [77]. Along with those properties, they also have pointed out some psychological factors that can guide in achieving the properties for message framing.

EXTRACTED GUIDELINES

A consolidated list of psychological factors and how they should be leveraged for awareness message framing has been listed and comprehensively explained in Table 5.

Table 5: Psychological factors for message framing

Psychological Factor	Rationale	Utilization Mechanisms
Loss aversion	People are more likely to be concerned by information on the losses of inaction than the gains obtained from the action.	The message should emphasize the losses or damages incurred to individuals and organizations due to inaction or bad action rather than gains obtained by acting. Moreover, the losses should be: • immediate, • related to the personal or professional (to the organization) life of the audience, and • make sense (or significance) to the audience.
Incentive effects	People are less incentivized by rewards a long time in the future. People think of the future in a more abstract way.	The message should explain "*why is it important to know about the threats*" for future events (e.g., common and future threats), and "*how to protect from the threats'* for imminent events (e.g., react to new events and situations).

Emotion effects	Emotion has a wide range of effects on people's judgments and decisions.	The effectiveness of a CSA initiative can be significantly improved by altering the emotional appeal of the message. For example,
		• The message should not focus on fear, uncertainty, and doubt (FUD). It should evoke positive emotion (e.g., prestige, hope) that also improves learnability and memorability.
		• Only, if necessary, the message should evoke negative emotions at a controlled level. For example,
		  ○ Fear-centric message should be used to generate information-seeking behavior.
		  ○ Anger-centric message should be used for prompt action.

Memorability	Memorable (comprehension and retention) message has proven to lead to behavior change.	The information memorability can be improved by incorporating these techniques, for example, • The message should use different cues to represent the information (use information-rich media) [78] [79]. • The message should avoid memory overload and use a cognitive-friendly presentation (provide only essential information that needs to be known). • The message should be unique.
Salience	People's attention is drawn to things that seem novel and relevant to them.	The message salience can be improved by using these techniques, for example, • The message should highlight the important information to make it noticeable. • The message should not exaggerate the cybersecurity issues. Exaggerating the problem could be unproductive and lead to evidence being overlooked. Rather the message should put the need for cybersecurity in a realistic perspective. • The message should be delivered in creative ways to make it noticeable, for example, by using central and consistent themes and/or slogans. • The message should be tailored to fit the knowledge or technical aptitude of the audience group. • Use the information and images that people can understand and relate to their lives and experiences.

		• Keep communication simple (plain and clear language, cognitive friendly presentation), personalize (how knowing the information is beneficial in personal or professional life), and accessible. • Connect security to values other than security alone.
Bandwagon effect or norms	People tend to adopt certain attitudes and behaviors if shown others also do them.	The message should use different techniques to inform the audience what others do, for example, • The message should promote good security behaviors as social etiquette and normal behaviors. If applicable, it should use statistics to show that others also practice security behaviors. • The message should inform the audience about colleagues, executives, or leaders whom others emulate, who practice good security behaviors by commending them publicly. • The message should use a statistical presentation to visualize data (e.g., visualize data, frequency presentation) and improve clarity. But the visualization should show the absolute value and contextualize the statistical information (a number without context is meaningless).
Confirmation bias	People are biased towards the status quo (interpret information in a way that supports one's prior beliefs or values), and hard to change from this.	The same message may not work for different contexts and situations. Such contexts and situations should be recognized and provided with alternative messages that can disprove the audience's prior beliefs and values, or clarify misconceptions (e.g., utilize compromise effect).

The list of general properties for awareness message framing and how they should be utilized for message framing is presented in Table 6.

Table 6: General properties for message framing

Property	Sub-Properties	Description & Utilization Mechanisms
Topic	Specific topic	The awareness message should focus on one specific cybersecurity issue relevant to the audience at a time [80]. Focusing on a variety of issues at the same time can be complex, confusing, and more importantly, *cognitively overloading* for the audience. Some topics may require discussion on multiple issues, for example, phishing includes email phishing, website forgery, smishing, vishing, spear phishing, whaling, clone phishing, and social engineering. Such a topic should be broken down into smaller, more manageable, and cognitively friendly sub-topics, and each sub-topic is discussed or organized separately. For example, • password security should not be mixed with phishing, and • email phishing, smishing, vishing, website forgery, etc., should be organized and discussed separately.
Overall information	Credible and consistent information	Accuracy and consistency in information help to build trust [81] and trust fosters compliance [82]. The awareness message should be correct (i.e., as advised by a cybersecurity expert) and consistent in language, design, and more importantly in the information (i.e., facts). No message in the awareness material should conflict with other messages in it.

	Up to date information	Cybersecurity is dynamic in nature. The awareness message should continually manage to include current changes in cyber risk profiles [4]. It should cover new security threats and technologies and also changes in policies and procedures relevant to the audience's job functions.
	Complete information	The awareness message should deliver the complete information that the audience needs to be informed and, if applicable, act. The Entman's [75] message-framing process, if adapted for a CSA purpose, then a message should state: • the threat applicable to the audience, • how to identify the threat, • why it is relevant to the audience, and • preferably what they should do and sometimes not do to stay protected. In addition, it should also provide how the lessons learned can be applied in the right way if applicable. For example," *use a strong password*" is an important suggestion but a more preferable way would be to also provide tips on creating a strong password. The audience should not be left wondering how to apply a suggestion. This will also prevent from making undoable or uncompilable suggestions to the audience. When it is difficult to accommodate all the information (e.g., in an awareness poster), in that case, a reference from where to get it should be provided. Suggesting this reference can motivate interested audiences to further explore it. Herold [83] has used WH question words to suggest the things that a CSA communication should include (also recommended by the ENISA framework) in a more comprehensive manner, which are: • WHAT is expected from the audience after participation (for example, compliance to certain standards and procedures, or changes in knowledge, attitude, and behavior) • WHY the target audience should participate (for example, how the cyber issues are relevant to the audience and their organization, what damages the issues could cause) • WHEN to perform the requested actions (for example, risks and threats identification and mitigations) • HOW the actions relate to the audience personal and professional life (for example, the benefits from acting as advised) • WHO sponsors the program (for example, government, organization) • WHO to contact for further information (for example, details of contact person or link with information)
Message	Positive framing of message	The awareness message should focus on good security habits (i.e., *informing what to do*) rather than explaining bad security habits (i.e., *informing what not to do*) and their consequences. Fear and anxiety undermine the cognitive capacity and hamper the learning process [84]. Moreover, positively framed messages are more persuasive where there is little emphasis on details [85], which is suitable in the case of CSA that deals with providing enough information to make an individual stay vigilant about cyber risks and know what to look out for [1].
	Direct message	The awareness message should be explicitly directed to the target audience. A message is more likely to be accepted and acted upon if the individual feels that it is explicitly directed at him or her rather than generically to everyone.
	Descriptive message	The awareness message should provide information in descriptive format [76]. It should include information in the format of how things are done and not what to do in

		steps if possible. Stepwise instructions can introduce the risk of inculcation [76] and discourage proactive thinking (or the ability to project threat trends).
Suggestions	Doable suggestion	The awareness message should offer meaningful suggestions to the audience (i.e., avoid impractical suggestions). The audience should be able to correctly apply or implement the suggestions. The concept of impracticability is again dependent on the computer literacy of the audience or their interest and ability to learn new computer skills.
	Convenience suggestion	Security is not the primary objective of the audience, so the awareness message should avoid the suggestions that are either taxing or noticeably (hinder or) slow down the primary responsibility of the audience. Like everybody, the audience is also wired to take the path of least resistance, even if it means exposing themselves to threats.
Content presentation	Clarity	Clarity should be in both the purpose and content of the awareness message. Fuzzy and general messages can get misinterpreted. For this purpose, it is suggested to consider a specific goal at a time and to use exact, appropriate, and concrete words. The words and phrases used to present information (i.e., avoid technical jargon) should be familiar to the audience. This will help the audience to understand the message quickly. After all, no one complains about the content being too simple to understand.
	Conciseness	The awareness message should be brief, to the point, and comprehensible for the audience. This can be performed by including only what the audience *needs to know* but *not what would be nice to know*.
	Well-structured	The awareness message should follow a clear information architecture, for example, in the sequence of "*what is the problem*", "*what solution fits*", and "*how to achieve the solution*". Unclear and disoriented information can be confusing and difficult to follow and can get misinterpreted.
	Uses multi representation	The awareness message should use various representations to complement each other, for example, graph or image to complement the text, and reinforce the main message by highlighting them. This richer representation improves understandability [79] and, at the same time, accessibility for different types of audiences, for example, differently abled audiences.
	Understandability of the main message	The audience should be able to understand the main message in a very short span of time in order to attract their attention to it. Average human attention dwindled to only 8 seconds in 2013 [86], so if the main message (or goal) of the awareness is not understandable in 8 seconds, the probability of the audience getting uninterested in learning it will increase.
Localization		Localization is about attempting to remove the cultural barriers that may exist. The awareness message should adapt the contents to an audience (for specific countries, regions, cultures, or groups). Along with language translation, use, for example, suitable terminologies, images, cases, and examples that the audience can relate to. Localization improves user experience, and that will lead to a better understanding. Eliminate things that the audience could not relate with or require mapping to relate and understand as far as possible. Localization should consider: • performing accurate translation of all information into the target language. • adapting graphics to the preferences of the target audience. • adapting layout and design so text can properly be displayed. • converting elements such as units of measurement and currency to local requisites. • using correct formats of phone number, address, and dates.

5.4.3 Delivery Method Selection

A multitude of delivery methods are used for raising CSA, for example, workshops, newsletters, posters, screensavers, emails, games, videos, audios, simulations, online quizzes, and so on. These methods can broadly be categorized into the following three types: instructor-led, computer-based, and text-based [87]; though, instructor-led can utilize technology and text-based materials. This classification can be further sub-classified, for example, computer-based can be sub-classified into online and offline based.

- *Instructor-led*: Instructor or facilitator who is knowledgeable and experienced in the learning materials teach participants in a classroom setting. Real-time feedback, as well as shifting of focus to suit the learner's needs, are possible.
- *Computer-based*: Necessarily aided by technology (e.g., computer, tablet, mobile phone). Learners can use it individually at the most convenient times and can always stop learning to return at a later point in time. It allows direct feedback on the learner's performance.
- *Text-based*: It does not require an instructor or technology, and due to its static nature, it does not offer individual feedback or other interactive elements. However, it offers self-paced, individualized learning of the content.

The instructor-led method can be suitable when the audience group is small, feedback is required in real-time, and awareness contents require tailoring to fit learners' needs. But it can be expensive as the sponsor or organizer has to incur major direct costs (i.e., salary to the awareness coordinator or team, teacher fees, rent of space used, and costs of logistics and other materials like slides, posters, videos, handouts, and gadgets) and indirect costs (i.e., time of organizer and audiences away from their work time) [88]. Similarly, the computer-based provides flexibility to reach a mass audience at a lower cost, and increased learner control (i.e., control over contents, sequence, and pace) irrespective of learner's physical location and duration of the day. It includes feedback and performance test features, and also benefits from the richness of multimedia. Support for multimedia helps to represent information in multiple formats at the same time that complements each other. However, it requires access to technologies, e.g., computer, software, and Internet bandwidth. Furthermore, its development and usage demand expertise in technologies. In some cases, for example, video content, simulation, animation, and games, the development of its content can be expensive for the organization and cannot be cost-effective for a small audience. Moreover, if the representations in different formats do not align to or conflict with each other, for example, increment in a value is represented by a downward arrow, then use of multimedia can cause more harm than good. Finally, text-based content is simple to design and has benefits like learner's control. But it does not contain feedback or performance tests and may not be environment friendly due to the use of paper. Apart from the aforementioned benefits, the text-based delivery method is found to be better for achieving perception due to its low cognitive load (i.e., clear, concise, and easy to follow information), whereas the computer-based can be more appropriate to achieve comprehension and projection [78]. Furthermore, computer-based is recommended for both the general as well as the advanced level of CSA (suitable for specialized role employees with a high level of security responsibility) [89] [90].

The delivery methods can [9]:

- be suitable for the *dissemination of a single message*, for example, awareness tools, posters, access lists, screensavers and warning banners, desk-to-desk alerts, agency-wide e-mail messages, brown bag seminars, and awards programs.
- more easily *include a number of messages (do and don't list),* for example, newsletters, videotapes, web-based sessions, computer-based sessions, teleconferencing sessions, in-person instructor-led sessions, and brown-bag seminars.

- be fairly inexpensive to implement, for example, awareness tools, posters, access lists, "*do and don't list*," checklists, screensavers and warning banners, desk-to-desk alerts, agency-wide e-mail messages, in-person instructor-led sessions, brown bag seminars, and rewards programs.
- require more resources to implement, for example, newsletters, videotapes, web-based sessions, computer-based sessions, and teleconferencing sessions.

Whichever delivery method is selected, one should keep in mind that it fulfills the need of end-users (meets specific customer needs), is affordable in terms of cost, fits the organization's culture and infrastructure, and does not require taxing activities that can slow down the users' task. Furthermore, it should be accessible to the audience, appropriate for the audience's circumstances and scenarios, use communication strategies and approaches that suit the audience's preference, be interactive and innovative to engage the audience, and be inclusive so that no subset of the audience feels excluded. A simple way to achieve them is to provide multiple methods that can fulfill the needs of diversified users [2] [80], and retain the information richness as much as possible. Moreover, include tracking capabilities like self-assessment and feedback that can help to verify whether people are actually learning and also facilitate interested users to participate and contribute to the future improvement of the awareness program.

Availability of such materials in different formats helps to cover a larger mass of audience with different learning preferences [91], for example, someone with no interest in reading can utilize CSA materials available in the form of video, game, or simulation. Moreover, if people are acclimated to a specific format of receiving information that will reduce the effectiveness of learning the information. Further, using multiple channels also ensures that the target audience is exposed to the same information multiple times in different ways that greatly increase users' retention of awareness lessons or issues [9].

EXTRACTED GUIDELINES

Deciding which delivery methods will perform better for a given case is a tedious task. To help with this task, some past studies [17] [43] [78] [92] [93] [94] have evaluated the effectiveness of different delivery methods used for CSA. Their evaluations are based on varying sets of properties. A consolidated list of relevant properties (applicable to every delivery method) that are included in these studies, except Nachin et al. [92] who have used the aspects that should be the objectives of a CSA program and not comparative properties for dissemination channels, has been given in Table 7. The table also provides how the properties should be utilized for the suitable delivery method selection.

Table 7: Criteria for the delivery method selection

Properties	Utilization Mechanisms
Cost to apply the delivery method	The delivery method should be cost-effective to develop, implement, operate, and maintain. Some relevant questions to be raised are: • How expensive is it to set up the environment for the method? • How expensive is it to operate the method (or deliver content) for the required period? • How expensive is it to create awareness content for the method? • How expensive is it to update and maintain awareness content? The cost-effectiveness is affected by: • cost per audience - an online method can be used to target a mass audience. So, its cost per audience could be small.) • prior experience of using the delivery method – once digital content has been created, it can be cheaper to reuse unless some serious update is required. Similarly, once the technologies to apply the delivery method are acquired, it becomes cheaper to apply the method again.

Outreach to the audience	The delivery method should be appropriate for reaching the target audience. Some relevant questions to be raised are: • How difficult is it to reach the target audience using the method? • Does it support reaching a geographically dispersed audience? • Does it support reaching a mass audience? For example, if the target audience is geographically dispersed or in a mass, then using an online solution could be preferable.
Support for diversity and inclusion	The delivery method should support multiple formats of awareness content. Some relevant questions to be raised are: • Does the method support awareness contents in multiple formats (e.g., text, image, audio, video, simulation, and animation; static and dynamic)? • Does it support content for multiple types of audiences? • Does it support content customization for different target groups? With multiple format contents support, it will be easier to target different audience groups using the same delivery method. For example, a website can integrate information in the forms of texts, videos, animations, and games that can be customized for different audience groups.
Effort and skills required for awareness content development and update	The effort and skills required to develop and update awareness content should be minimal for the delivery method. Some relevant questions to be raised are: • How difficult is it to develop content for the method? • How difficult is it to update the content? • Do the content development and updating require any special technical skills? • Are the content development and updates time-consuming? For example, developing simulation content could require specific technical skills and high effort and time.
Features for standardized assessment and feedback and ease to use them	The delivery method should include features for standardized assessment and feedback of the awareness program. Some relevant questions to be raised are: • Does the method integrate standardized assessment to measure the audience's learnings after participating in the awareness program? • Does it support (or integrate) features to collect the audience feedback on the awareness program? • Do they include relevant and valid questions to measure learnings? • Are the features user-friendly? Availability of these features will help to assess the audience's learning and also get their feedback immediately after the completion of the awareness program. For example, a website can have an inbuilt questionnaire or quiz and also a feedback section integrated that appears after the completion of the awareness program.
Information richness or information-carrying capability	The delivery method should support information richness or high information-carrying capability. Some relevant questions to be raised are: • Does the method support communication between the awareness professional and the audience (to clear doubt)? Is this real-time or non-real-time communication? • Does it support multiple cue communication, e.g., visual, auditory, verbal, and tactical cues? • Does it support language variety (use of vocabulary based on the target audience)? • Does it support message personalization (one or two-way information exchange, adjust or tailor interaction based on feedback, tailor learning pace)? • Does it support incorporating detailed information?

	For example, a workshop includes real-time communication, supports language variety, different cues, and message personalization. Moreover, depending on the time availability, can incorporate detailed information.
Need for additional means	The delivery method should require minimum additional means to deploy and operate. Some relevant questions to be raised are: • What skills, knowledge, and abilities are required to apply and operate the delivery method? • What technologies and resources (hardware, software, Internet connection, and other resources) do it require to apply and operate? • What additional information like an email address (for email as a channel), contact number (for SMS and phone call as delivery methods) is required to apply and operate? For example, a website requires a computer, software, and Internet connection. Likewise, a workshop setting requires the presence of an instructor and other resources like a computer, projector, pen, pencil, paper, etc.
Interest and motivation to participate and learn	The delivery method should interest and motivate the audience to participate and learn. Some relevant questions to be asked are: • Is the delivery method preferable (or suitable) for the audience group based on their age, gender, education level, field of study, occupation, and other socio-demographic factors? • Will it contribute to improving the audience's interest and grab their attention? • Does the method support and facilitate user interaction? • To what extent does it support the audience's involvement in the learning process? For example, the game is found to be popular among the young age group and attention-grabbing. Likewise, a workshop supports user interaction within the audience group and with the instructor.
Efforts and skills required to operate and manage	The delivery method should be simple and easy to operate and manage. Some relevant questions to be raised are: • How difficult is it to operate and manage the delivery method? • How difficult is it to present awareness information using it? • How difficult are the assessment and feedback features to use? • How difficult is the delivery method for the audience to use? For example, a website requires different technical aspects to manage. Likewise, a workshop could require managing the people.

5.5 Monitoring and Enhancement Guidelines for Pre-Implementation Phase

The consolidated guidelines presented in Table 8 deliver the outputs and outcomes to expect in each sub-phase and activity of the per-implementation phase after the suggested (or the right) actions have been performed. This information should be utilized for the phase's monitoring and enhancement.

Table 8: Consolidated guidelines for monitoring and enhancement of pre-implementation phase

Activity	Sub- Activity	Monitoring Guidelines
Team setup	Team Leader and Others	1. Adequate team size depending on the scope of the program. 2. Team with at least a full-time dedicated CSA professional. The CSA professional is equipped with: • soft skills (communication skills; familiarity with learning concepts as well as awareness tools and techniques; personal attributes; career and collaborative attributes; and people skills) • contextually aware (situation of entities)

		• technical skills 3. Heterogenous team (remaining members coming from the interested groups applicable to cybersecurity and departments in the organization). 4. Well-defined roles, responsibilities, and accountabilities for every team member.
Establish goals and objectives	Criteria for Goals and Objectives	1. Goal and objectives support the reason for creating the program (or the security behavior ought to be reinforced). 2. Goal is simple and clear. 3. Objectives follow the SMART (Specific, Measurable, Attainable, Relevant, Time-bound) criteria.
	Understanding audience and their grouping	1. Audience grouping (or classification) is done based on pre-existing beliefs and cybersecurity expertise. 2. In an organization, audience grouping is done based on employees' roles and responsibilities. 3. Otherwise, audience grouping is done based on factors like profession, education level, culture, or age group.
	Sponsor/leadership support and participation	1. Appropriate priority for the program is indicated by • adequate funds received for the program • leaders'/managers' participation in the programs applicable to them. • leaders/managers practice security behaviors 2. Funds received for the program are asked and expressed in terms of one of these: • percent of the overall learning and development budget, • percent of the overall IT security budget, • budget asked per target individual, or • explicit amount asked for each component of the program.
Topic selection	Topic identification	1. Topics are relevant to and align with the roles and responsibilities of the target audience. Moreover, the topics include (or interest or of value to) everyone in the target group. 2. Topics cover common threats, threats specific to the target group, new events and situations, and potential future threats.
	Topic prioritization	1. Topics receiving high priority are: • that specific to critical security roles and controls, • that relative to critical projects, • that align with the target group (or organizational) role and risk, • that are important but neglected by the target audience (i.e., low adherence), • that with resources are readily available
Resource Preparation	Content Intensiveness and Complexities	1. Content intensiveness and complexities match with the audience's security knowledge and skill level. 2. Content intensiveness is adjusted from beginner to in-depth levels depending on the audience.
	Message Framing	**Message framing utilizes these psychological factors** 1. *Loss aversion:* emphasize the losses or damages incurred due to inaction or bad actions. The losses focused are: • immediate or closer, • related to the personal or professional life of the audience, and • that make sense (or significance) to the audience

		2. *Incentive effects:* refrain from incentive techniques, rather applies non-incentive motivational techniques, for example, • explain *why* to act for future events • explain *how* to act for imminent events 3. *Emotion effects:* evoke positive emotion unless necessary otherwise. If necessary, evoke negative emotion at a controlled level for instant compliance, for example, • use fear for information-seeking behavior • use anger for prompt action 4. *Memorability:* facilitate memorability (or retention) of the information using techniques, for example, • use multiple cues • present the message in a cognitively friendly manner • use unique and compelling messages 5. *Salience:* draw the audience's attention using techniques such as: • put a need for cybersecurity in a realistic perspective • use creative ways to deliver the message, for example, use central and consistent themes and/or slogans • tailor the message to fit the knowledge or technical aptitude of the target group • convey information and images understandable and relatable to the target audience's lives and experiences • communicate in simple (plain and clear), personalize (suitable to the target audience's personal and professional life), and accessible way • convey the benefits of security learning in terms of values other than security alone 6. *Bandwagon effects:* inform about what others do (good behaviors) • promote good security behaviors as social etiquette and normal behaviors • inform about the people (whom others can emulate) practicing security behaviors • use available statistical information, however, statistical information contains the absolute value and numerical information placed in a context 7. *Confirmation bias:* come up with alternative messages without distorting the information for the occasion when the message does not work.
		Message framing meets these general properties 1. *Specific topic:* focus on a specific cybersecurity issue relevant to the target audience at a time. To discuss multiple interrelated topics, breaks them into multiple sub-topics. 2. *Credible and consistent information:* have correctness and consistency in language, design, and information (facts). 3. *Up-to-date information*: stay abreast of cybersecurity trends. 4. *Complete information*: deliver the complete information the audience needs to be informed and, if applicable, to act. For example, • information states the relevant threat, why is it important to know, how to identify it, how to protect against it, and how to correctly apply the suggested mitigations • more comprehensively, information states, WHAT to expect after participation, WHY to participate, WHEN to perform the requested actions, HOW the actions are related to personal and professional, WHO are the sponsors, and WHO is the contact person • provide a reference where information could be found, if it becomes difficult to accommodate all the information 5. *Positive framing of message:* inform good security habits rather than bad security habits. 6. *Direct message:* direct the message explicitly to the audience.

		7. *Descriptive message:* provide information in the format of how things are done and not stepwise instruction, if possible. 8. *Doable suggestion:* make practically feasible suggestions. 9. *Convenience suggestion:* make suggestions that can be performed comfortably without hindering the primary responsibilities. 10. *Clarity*: be clear in purpose and content, i.e., • consider a specific goal at a time • use exact, appropriate, and concrete words • avoid technical jargons 11. *Conciseness*: inform about what needs to know and not what would be nice to know. 12. *Well-structured:* follow a clear information architecture, for example, in the sequence: • what is the problem, • what solutions fit, and • how to achieve the solutions 13. *Uses multiple representations:* use different representations, for example, graphs and images to complement textual information wherever necessary. 14. *Understandability of the main message:* use a simple and clear main message. 15. *Localization*: adapt contents for specific countries, regions, cultures, or groups using localization techniques, for example, • accurately translates the text • adapt graphics, layout and design, measurement and currency unit, formats of phone number, address, dates, and so on

6 Implementation Phase

6.1 Pilot Test

A small-scale preliminary test with the target audience can be performed to assess the efficacy of awareness resources prepared or improved [26]. Such a test will help to identify the issues in the design of resources that require revisions before they could be used for the anticipated awareness program. Although it is not mandatory to have a pilot test, particularly for the existing or continuing and small-scale awareness program, it can have significance for a new (or first-time) and large-scale (or mass) awareness program. A pilot test is an added step to the CSA process (or a burden for resources) and has no guarantee that it will identify and help to avoid all issues. However, if the awareness program is for a mass, the benefits of a pilot test may outweigh the efforts and resources spent on it.

EXTRACTED GUIDELINES

- A pilot test to assess the efficacy of awareness resources should be performed for a new (or first-time) awareness program and that with mass participation.

6.2 Message Delivery

The CSA message can address one topic or a number of related topics at a time. The message should ideally reach everyone in the target audience or as broad an audience as possible in practice. But simply reaching the target audience could not ensure that the awareness message will be received, read, and taken seriously by the audience. For example, many people in organizations are not enthusiastic about participating in a CSA initiative [57]. Therefore, it is important the message reaches the target audience and positively impact them (influence or motivate them to adopt good security practices and advice in the message).

6.2.1 Message Communication

It is often recommended to make a CSA program engaging, entertaining, and fun as a potential solution in order to encourage large participation [57] [68]. Although there does not exist consensus upon how message delivery can be improved, some studies have attempted to draw out relevant properties [3] [4] [5] [10] [56] [58] [68] [76] [77].

EXTRACTED GUIDELINES

A consolidated list of factors that should be utilized for message delivery has been listed and briefly explained in Table 9.

Table 9: Factors for message communication

Factor	Utilization Mechanisms
Targeted message	• The message should be established for a specific audience group (how grouping can be done has been explained in section 5.2.2). People, in general, have varying opinions, beliefs, interests, expertise, and experiences. So, the message should target a specific audience group and be tailored accordingly to meet their needs and concerns.
Relevant topic	• People's emphasis on the type of cybersecurity issues could vary depending on their interest, expertise, and experiences. So, the selected topic (how topics can be selected and prioritized have been explained in section 5.3) for CSA should be specific and relevant (or of use) to the audience group or critical to their organization.
Effective delivery method	• The most effective delivery methods should be used (how delivery methods can be selected has been explained in section 5.4.3), which are preferred and used by the audience to get information. This will maximize the appeal of the message and persuade the audience to act especially if the message fits with the target group's interests and needs. In order to reach and cover as broad a range of audiences as possible within the target group, multiple delivery methods should be used.
Appropriate messenger	• The messenger should be someone credible or influential whom the audience trusts, likes, or listens to for security advice, e.g., authorized security expert, trained executive or peer, or an organization authorized for cybersecurity.
Coalition	• The awareness team should build coalitions with other parties to reach a broader pool of audiences. Partners can be utilized as a multiplier in the dissemination of the awareness message. However, this requires knowledge and experience in coalition management.
Security by default	• Security choices that reflect the organization's norms and regulations should be preselected by default or have smooth pathways, e.g., security software should be installed and be part of the initial setup.
Priming	• The awareness team should create an environment where the participants frequently get exposed to awareness messages or cues that reflect and remind them of security, e.g., posters and banners around the organization's premise, and periodically simulated attacks.
Effective conveyance	• The message conveyed should not be unduly concerned or overly negative about a situation. It should use real-life examples and experiences to explain cybersecurity issues.
Affect	• Emotional associations can powerfully shape people's actions. The participants should be informed about the purpose of a CSA program and their role in preventing security attacks. The security message should be presented in counterintuitive manners so that it provokes emotions (attitudes to cybersecurity) but without obviously connecting it to a change in security behavior.

Incentive	• The awareness team should use *extrinsic* incentives when temporary compliance is needed (e.g., increasing attendance and enrollment for a CSA program) and *intrinsic* incentives for attitude and behavior change.
Commitments	• People seek to be consistent with their public promises and reciprocal acts. So, the awareness program should establish clear goals and expectations concerning the desired behavioral changes following a CSA program and make it public. If possible, it should also set a deadline by when the goals should be achieved.
Ego	• People act in ways that make them feel better about themselves. So, the awareness team should consider the capabilities and motivation of the participants and possibly begin with small and easy changes. Further, the team should provide structured and constructive feedback on the participants' behaviors (performance). The message should be expressed in a courteous manner (without hurting the feelings of the audience, unbiased and focused on the audience)
Engagement	• The awareness team should build CSA programs for the audience rather than assuming they will be driven to educate themselves. This includes: ○ to communicate how the security learnings are beneficial in personal life, ○ not to focus on FUD but to leverage technology, ○ to use the communication media the participants are used to, and ○ to make awareness interesting and fun to attend (e.g., game).
Representational	• A face should be given to the threat actors and defenders. ○ It should be clear who the villains are. The villains should be clearly recognizable as evil. Cast only unambiguous cybercriminals as villains, for example, Nigerians who are notorious for their scam emails. ○ Those who are guarding and protecting should be placed in the spotlight as heroes. They could be the cybersecurity specialists in the organization. Explain the complex work they are undertaking to keep the systems safe and secure.

6.2.2 Enactment Approach

To deal with non-compliance of cybersecurity policies and procedures, organizations apply one of the two reinforcement approaches, i.e., *soft approach or tough approach* [95].

- *Soft approach*: Utilize various persuasion techniques, for example, organizing needful training and awareness programs for employees, boosting employees' motivation, rewarding employees for participation, and making the policies and procedures relevant and compliable. In this, the organization treats its employees as an asset and places trust in them by promoting self-regulated behavior.
- *Tough approach*: Emphasizes coercive strategy to enforce employees behave in a desirable way and attempts to deter non-compliance with punishments, generally thorough warnings, and sanctions. It treats employees as a liability and continually monitors employees' behavior.

In the case of CSA and behavioral change, the persuasive approach is often recommended [95] [96] [97]. There are different reasons behind this, mainly because organizations cannot afford to continuously monitor employees' behavior and to dismiss or discipline a large number of skilled staff needed for a tough approach [98]. Moreover, treating employees as an enemy and using forceful enforcement can increase tension between enforcers and the rest of the organization [97]. In addition, to keep up with the ever-evolving digital landscape and constantly changing cybersecurity, a long-term behavioral change is required, which can be possible through a soft approach. This is also supported by Thorndike's law of effect [99] used for learning theory, which states that "*behaviors that are rewarded (or whose responses produce a satisfying effect) are*

more likely to recur again, while behaviors that are punished (or whose responses produce a discomforting effect) tend to weaken." The main logic behind this law is that punishment or discomforting effect leads to avoidance of the situation or initiates feelings of anxiety or fear. Feelings of fear or anxiety in cybersecurity are considered to be counterproductive, especially, in the absence of clear communication and efficacious information about how to respond to the threat [100]. However, some researchers who keep contrary views advocate for a level of fear in cybersecurity to produce a positive effect [101]. Their rationale behind this is that through persuasion, the probability of compliance is improved, whereas evoking fear by highlighting the unpleasant consequences of non-compliance makes people care about compliance [101].

The debate on which approach is better, soft, or tough, has no end unless other conditions are considered. If the *perceived efficacy* is higher than the *perceived threat*, then fear in cybersecurity can produce a positive effect, otherwise, it will backfire and produce unintended outcomes [101]. Employees will not act if they believe that their actions will not ameliorate the threat. Finally, the major challenge in using either a soft approach or a tough approach is determining critical factors that can motivate the employees for compliance or deter them from non-compliance respectively. More importantly, due to various intervening factors, it is difficult to prove unequivocally that a certain persuasive factor has motivated compliance behavior or punishment has prevented non-compliance behavior. The views on these critical factors often vary with no common ground; different experts may offer different perspectives based on their personal experiences.

EXTRACTED GUIDELINES

- Soft approach should be used to enforce compliance or discourage non-compliance [95] [96] [97].
- In certain situations, a tough approach should be applied but at a controlled level, for example, fear-centric approaches should be applied to achieve information-seeking behavior and anger-centric approaches should be applied if action is required from the participants) [56].

6.2.3 Frequency of Delivery

Cybersecurity is dynamic in nature; therefore, CSA programs should be regularly updated and organized to stay up to date about new threats and the techniques of bad actors [10] [57]. Moreover, the effects of CSA attenuate over time, essentially the knowledge that is no longer in practice (e.g., we do not encounter social engineering attacks every day, but it is important to be always alert and prepared for it), so the shorter the period between two consecutive programs the better would be the improvement on CSA [27]. This is why a CSA program should be organized sufficiently frequent to maintain its effectiveness and also update and reinforce security knowledge. However, the CSA program consumes cost and time that should be considered when determining its frequency.

A question that requires to be answered is "*how often CSA programs should be organized?*" Its simple answer would be the frequency adequate to maintain the topic in the minds of individuals [10]. In order to realize a more explicit value for the frequency of delivery, it is necessary to determine how long the impact of a CSA program lasts. To an extent, its answer can be derived from the *Curve of Forgetting* [102] which describes how human memory retains or forgets information. According to the curve, if we assume 100% of the information learned at the end of a lecture and there is no attempt made to retain the information, we remember only 30%-50% of the information by day 2, and this dwindles to only 2%-3% by day 30. However, this trend of forgetting information can be changed by applying Dale's Cone of Experience Model in the information delivery [103]. The model conveys that people retain information told, shown, and experienced (done) to them in ascending order, i.e., shown remains for longer than told, and experienced remains for longer than shown. Therefore, by utilizing the delivery methods that support the perceptual learning styles, information retention can be improved. This memory retention can be further positively influenced by managing *cognitive overload* [104].

The most relevant answer regarding the frequency of CSA programs is given by Reinheimer et al. [105]. In this study, the authors investigated the effectiveness of a CSA program over time. The study ascertains that a CSA program continues to be significantly effective even after four months. However, its effectiveness decreases to an unacceptable level after six months. Thus, it recommends organizing a CSA program every six months. Although this recommendation (or information) is valuable for determining the frequency of a CSA program, it is based on a study conducted in the context of phishing awareness (general intensiveness). So, the situation may change in the case of intermediate or in-depth intensive CSA programs. Moreover, in an organization apart from responding to a new arise situation and event (e.g., evolving technology and threat, suffered cyberattacks, and introduction of new regulation and law) it should be made mandatory upon new hire as well as role changes of the existing personnel, along with its periodic sessions [37].

EXTRACTED GUIDELINES

- CSA programs should be organized periodically, at least once every six months [105] except if it is about responding to new events and situations.

6.3 Lesson Learned

By incorporating feedback from the audiences and lessons learned from the implementation of CSA programs, the program's effectiveness can be improved in subsequent or future initiatives [30]. Moreover, in terms of materials and experience, advice and lessons gained from colleagues and/or organizations that manage other awareness programs could be quite useful [10]. One department can share experiences with other departments so that they can prepare beforehand to avoid repeating the same mistakes.

But to have the lessons learned and make their optimal use, first and foremost, they must be captured and documented. In order to do so, the ENISA framework [10] suggests every individual in the team or group responsible for implementing a component can write notes or stories of lessons learned and submit them to a designated person who can polish them and submit them to the database. This is followed by a debriefing session and then the final documentation of the lessons learned. The debrief session should follow these guidelines:

- The lessons learned are program management-oriented and not work product-oriented
- Use case examples to make a point.
- Both praise and criticism can be used. However, criticism should be constructive, thoughtful, and non-personal.
- If there is no fix, improvement, mitigation, or way to influence an issue, do not discuss it.

EXTRACTED GUIDELINES

- The lessons should be properly captured, debriefed, and documented.
- The lessons learned should be program management-oriented (plan, assess & design; execute and manage; evaluate and adjust) [10].

6.4 Monitoring and Enhancement Guidelines for Implementation Phase

The consolidated guidelines presented in Table 10 deliver the outputs and outcomes to expect in each sub-phase and activity of the implementation phase after the suggested (or the right) actions have been performed. This information should be utilized for the phase's monitoring and enhancement.

Table 10: Consolidated guidelines for monitoring and enhancement of implementation phase

Activity	Sub- Activity	Monitoring Guidelines
Message Delivery	Message Communication	1. *Targeted message:* select a topic and message that target a specific audience group at a time. 2. *Relevant topic:* select a topic that is relevant and of use to the audience group and critical to their organization. 3. *Effective delivery method:* select communication methods that are preferred or used by the audience group; use multiple delivery methods so that everyone in the audience group can be covered. 4. *Appropriate messenger:* use someone whom the audience trust, like, or listen to for security purpose, e.g., authorized security expert, or trained executive/peer as the messenger. 5. *Coalition:* build a coalition with others and use partners to reach a broader pool of audience. 6. *Security by default:* preselect default or smooth pathways to security/right choices and create barriers to risky/wrong behaviors. 7. *Priming*: create an environment where the participants frequently get exposed to messages or cues that reflect and remind them of security. 8. *Effective conveyance:* refrain from unduly concerned or overly negative thoughts on cybersecurity issues. 9. *Affect*: inform the audience about the purpose of the program and the audience's roles in security attacks prevention. Present the message in counterintuitive manners so that it provokes emotions but without obviously connecting it to a change in security behavior. 10. *Incentive*: use extrinsic incentives when temporary compliance is needed (e.g., increasing attendance and enrollment for a CSA program) and intrinsic incentives for attitude and behavior change. 11. *Norms*: repeatedly promote good security behaviors as a social etiquette or normal behavior. 12. *Commitments:* establish and clarify the behaviors expected from the audience after attending the program and set a deadline to achieve the behavior change if applicable. 13. *Ego*: provide constructive feedback on the audience's behavior or performance. Express message in a courteous manner. 14. *Engagement*: build the programs for the audience. Do not assume that the audience will be driven to educate themselves. Use these techniques for improving audience engagement: • communicate how the security learnings are beneficial in personal and professional life • do not focus on FUD but leveraging technology • use the communication media the participants are used to • make awareness interesting and fun to attend 15. *Representational*: give the fight against cybersecurity a face (place those who are guiding and protecting at the spotlights as heroes, and cybercriminals as villains or evils (cast only unambiguous cybercriminals as villains).
	Enactment Approach	1. Use soft approaches for enactment. If necessary, use hard approaches at a controlled level • fear-centric for information-seeking behavior • anger-centric for action
	Frequency of Delivery	1. Organize the program periodically, at least once every six months except if it is about responding to new events and situations.

Lesson Learned		1. Properly capture, debrief, and document the lessons learned. 2. The lessons learned are program management-oriented (plan, assess & design; execute and manage; evaluate and adjust).

7 Post-Implementation Phase

7.1 Evaluation

A CSA program must be evaluated to determine its outcomes and impacts. The evaluation helps to determine the weaknesses in the existing CSA initiatives so that they can be improved for the subsequent or future iterations of the program. Moreover, because cybersecurity is dynamic in nature, the program must be kept updated and relevant to the target audience. The program evaluation is generally conducted through a formal quantitative/ qualitative analysis, or informal review and monitoring of changes in participant's behavior or attitudes [106]. The measurement or assessment used is either subjective (e.g., ask the audiences about their experience) or objective (e.g., ask the audiences to do something) [107]. The evaluation is conducted mostly using indirect measurement, i.e., assessing or measuring the factors like the audience's learning and experience. A few studies make random attacks on the audience in order to directly assess their cybersecurity attitude, cognition, and behavior. But a major issue with most of these studies on CSA evaluation is that they assess or measure only some key performance indicators (KPIs) to justify their models or frameworks. The chosen KPIs do not generally represent the complete program evaluation. A CSA program includes many aspects and involves different stakeholders; its evaluation should reflect that.

There are some major studies [108] [109] that provide the KPIs that can be measured to realize the success of a CSA program. But more consolidated metrics for CSA evaluation have been proposed in the CyberSec4Europe's deliverable report D9.13 [29]. This report incorporates information from the two studies [108] [109] along with many other important and relevant studies. The proposed metrics are shown in Table 11. The report recommends measuring all indicators by using at least one or multiple factors and measurement methods depending on the need and relevancy. Further, it recommends to adhere to these criteria for good metrics [110] during measurement: i) consistently measure (no subjective criteria), ii) cheap to gather (preferably automated), iii) expressed as a cardinal number or percentage, iv) expressed using at least one unit of measure, and v) contextually specific (i.e., relevant to decision-makers so they can take action). Most importantly, the organization needs to ensure that lessons are learned from the evaluation that can be used to update and optimize CSA in order to achieve a better one in the future.

Table 11: Metrics for the evaluation of CSA [29]

Indicator	Measured Factor	Measurement/Assessment Method
Impact indicators measure and assess the learning (i.e., knowledge and skills gained by the audience as a result of the awareness), and the impact on the audience's performance and attitude towards cybersecurity.	Impact of awareness on: • Cybersecurity knowledge & competence • Attitude to cybersecurity • Cybersecurity behavior It also comprises touchability (i.e., information is perceived positively by the audience).	• (Pre- and post-, quantitative) web-based test (vocabulary and scenario type questions) to determine if the audience knows more about the issues covered by the awareness program than before participating in the program. • (Pre- and post, online, standardized, quantitative) questionnaire-based survey to determine if the audience knows more about the issues covered by the awareness program or not, and if they understand the sense of urgency of fighting and preventing the issue or not.

		• (Pre and post) statistical analysis of passive data to know if there is a decline in security incidents and violations, for example,
		  ○ Data from audits and risk departments
		  ○ Count and severity of security incidents occurred due to staff behavior
		  ○ Other best behavior data that can be automatically collected (e.g., anti-virus and firewall log data, and helpdesk data)
		• (Pre and post) simulated and tool-based attack to determine if the audience understands the sense of urgency of fighting and preventing the issue or not.

Sustainability indicators measure the direct and indirect values added to the organizations as a result of implementing CSA. These indicators are critical for the management or sponsors in their decision-making on whether to invest in the program or not, and this is necessary for the continuity of the program.	Impact of awareness in the change of:
	• Organizational policies
	• Regulatory framework
	• Organizational arrangement
	Change in top management and sponsor support and commitment for the awareness program
		• Valued-added by the awareness program evaluation based on, for example,
		  ○ Recognition of security contributions, e.g., count and reputation of awards and contests won due to the awareness program
		  ○ Percentage of awareness processes incorporated in the organization's policies, processes, and arrangement
		• Change in funding and resources allocated for the awareness program to realize the management/ sponsor interest in the awareness program
		• Cost-benefit analysis of the program (i.e., ROI)

Accessibility indicators measure the quality of resources and delivery channels used in the awareness program.	• Quality of awareness resources
	• Effectiveness of awareness resources
	For example, whether the content was relevant and easy to follow or not, what were the strengths and weaknesses of the program, and whether the delivery methods were able to accommodate the audience's pace and learning style or not. It comprises of usability and reachability.
		• Survey to evaluate (using closed quantitative questions, such as Likert scale):
		  ○ relevancy of topics
		  ○ content quality
		  ○ delivery assessment
		• Percentage of security topics covered with respect to expected topics to learn if all relevant or demanded topics are covered or not
		• System and log data analysis (e.g., attendance, website visit, email recipient, etc.) to determine if the target group has accessed the awareness resources or not.

Monitoring indicators measure how the audiences, sponsor, senior management have perceived or reacted to the awareness program	Interest, support, commitment, and participation of different stakeholders in the program	Evaluate interest and active participation using: • System and log data analysis (e.g., attendance when it is not mandatory, number of attendees who registered and completed the e-learning program with respect to those who visited, hit counts to the link for more information, etc.) • Post-event survey (using closed quantitative questions, such as Likert scale; preferably anonymous) to receive overall feedback on the awareness program. • Availability of required resources for the program (funds and other resources for future iterations).

EXTRACTED GUIDELINES

- All indicators (Impact indicator, Sustainability indicator, Accessibility indicator, and Monitoring indicator) should be measured by using one or multiple factors and measurement methods depending on the need and relevancy [29].
- Measurement should adhere to the good metrics criteria [110], which are:
  - consistently measure (no subjective criteria),
  - cheap to gather (preferably automated),
  - expressed as a cardinal number or percentage,
  - expressed using at least one unit of measure, and
  - contextually specific (i.e., relevant to decision-makers so they can act).
- Evaluation results should be utilized for the update and optimization of CSA programs.

7.2 Adjustment

Cybersecurity posture constantly changes and evolves, and so should the CSA efforts. Many factors contribute to the changing cyber threat landscape, for example,

- rapidly and constantly emerging and evolving technologies that induce new threats every day,
- existing digital divide in the society where large segments have only limited access to technology and often lack knowledge and skills needed to use it securely, and
- major events and situations that drive the emergence of new cybercrimes (e.g., cybercriminals exploiting fear and uncertainty caused due to the COVID-19 pandemic).

In addition, external (e.g., new or amended cybersecurity laws, regulations, directives, and decisions) and internal (e.g., new or updated cybersecurity policies, procedures, standards, and guidelines in an organization) factors influence the cybersecurity posture [10]. These changes in the cybersecurity posture and landscape must be encompassed by CSA programs. This is necessary to ensure that the program, as structured, continues to be updated as new technology and associated security issues emerge. Also, the lessons learned, and weaknesses identified by the evaluation processes must be utilized to improve the program.

EXTRACTED GUIDELINES

- A CSA program adjustment should include the changes in the cybersecurity scenario, lessons learned, and weaknesses identified by the evaluation processes.

7.3 Monitoring and Enhancement Guidelines for Post-Implementation Phase

The consolidated guidelines presented in Table 12**Error! Reference source not found.** deliver the outputs and outcomes to expect in each sub-phase and activity of the post-implementation phase after the suggested (or the right) actions have been performed. This information should be utilized for the phase's monitoring and enhancement.

Table 12: Consolidated guidelines for monitoring and enhancement of post-implementation phase

Activity	Sub- Activity	Monitoring Guidelines
Evaluation		1. Measure all indicators by using one or multiple factors and measurement methods depending on the need and relevancy (Impact indicator, Sustainability indicator, Accessibility indicator, Monitoring indicator). 2. Adhere to the good metrics criteria for the measurement, which are:

		• consistently measure (no subjective criteria), • cheap to gather (preferably automated), • expressed as a cardinal number or percentage, • expressed using at least one unit of measure, and • contextually specific (i.e., relevant to decision-makers so they can act)
Adjustment		1. Use evaluation results for the update and optimization of CSA programs. 2. Adjust the program by considering: • the changes in the cybersecurity scenario, • lessons learned, and • weaknesses identified by the evaluation processes.

8 Evaluation Criteria of Selected CSA Mechanisms

With the previous section describing Monitoring and Enhancement guidelines, it is still necessary to evaluate the progress of CSA measures. Thus, in this section, we first describe evaluation scales to measure CSA and related constructs. As the introduced scales measure CSA, they are useful to evaluate any kind of CSA measure. Next, we discuss specific criteria for CSA posters and CSA serious games. Within the resources of the work package, it was not possible to elaborate criteria for all CSA measures, such as traditional training and seminars, Capture the Flag and Cybersecurity exercises, books, videos, etc. Thus, we chose CSA posters as they have a wide distribution, e.g., ENISA [17], Europol [18], and SANS [21] offer posters on their websites. Naturally, posters are not very interactive, thus we also elaborated corresponding evaluation criteria for serious games to complement our evaluation with the CSA measure. Serious games are gaining more and more popularity recently and are highly interactive. This way, we have covered both sides of the complexity scale.

For all CSA measures, it is important that they are adapted to the intended target group [2]. For example, CSA measures targeting organizations need to have a different focus than those targeting the general public or parents of children as each of the target groups has a different background and knowledge about CSA, and thus needs a different level of details to prove useful. In a certain way, this also holds for scales and questionnaires aiming to measure CSA.

Traditionally, CSA effectiveness is assessed in terms of the count of cyber breaches suffered (to be precise, reported) and their impact on individuals or organizations. Besides including a potential bias since cyber incidents remain widely under-reported [111], the approach lacks measuring the effectiveness of a security measure on an individual level. Since in particular, CSA measures target individual persons, it is important to include what the participants think, know, or do about security issues. This is the only way to measure the effectiveness of a CSA since the overall security (measured by the number of recognized and reported incidents) is influenced by many more factors such as the number of attacks, the exposure of the organization, and the organization's security level which is a composite of CSA and "*technical security*". Since these factors are hardly the same for different organizations, it would be particularly hard to conclude about CSA by only measuring the overall security of an organization.

8.1 Evaluation Scales/Questionnaires

An effective approach could be to use field observation to assess the security attitude and behavior of participants. However, this approach also has some major downsides; it is both expensive as well as time-consuming, and assessing the full aspects of security behaviors using the approach can be a challenging

endeavor. This may be a reason why most studies rely on self-reported measures (e.g., surveys and interviews) for assessing the cybersecurity knowledge, attitude, and behavior (KAB) of participants. Self-reported measures are less resource constraining and can easily integrate different aspects of cybersecurity behaviors. A major problem with many studies exercising self-reported measures is they develop their own questionnaires (or measurement), which are often non-standardized (does not follow a standard process to design questionnaires and analyze the data). Moreover, such works often examine only one or a few selected components of cybersecurity. Even worse, some studies delivering security tools or proposing a framework perform surveys with the sole intention to establish and prove their work is relevant and useful. In order to overcome these issues related to the use of self-reported measures, some selected studies, listed in Table 13, have produced standardized and well-validated scales and questionnaires intended to measure the cybersecurity KAB of participants. These scales and questionnaires have either followed standard procedures for their design or adapted scales already established in other fields of study.

Table 13: CSA evaluation scales /questionnaires

Scale/Questionnaire	Measurement	Development Processes

Human Aspects of Information Security Questionnaire (HAIS-Q) [112]	• Measures security knowledge, attitude, and behavior
	• Focuses on 7 security areas
		• Used a hybrid methodology that incorporates the inductive and exploratory approaches as recommended by Karjalainen [113] to design the questionnaire.
		• The questionnaire was empirically validated in three phases
		  ○ First phase validation used a survey in addition to think-aloud and verbal probing by an expert.
		  ○ Second phase validation used a pilot survey with 113 valid responses
		  ○ Third phase validation was performed using a survey with 500 valid responses

Security Behavior Intentions Scale (SeBIS) [114]	• Measures adherence to computer security advice (i.e., attitude and behavior)
	• Focuses on 4 security areas/dimensions
		• Followed the four-step approach as outlined by Netemeyer et al. [115] to develop the scale:
		  ○ Construct definition and content domain
		  ○ Generate and judge the measurement items
		  ○ Design and conduct studies to deploy and refine scale, and
		  ○ Finalize the scale
		• The scale was validated using a multi-round sequential survey
		  ○ First-round validation used a survey with 479 valid responses
		  ○ Second-round refining used a survey with 456 valid responses

SA-6 scale [116]	• Measures security attitude
	• Focuses on 6 security items/questions (using a question for each item)
		• Utilized Netemeyer et al. [115] and other studies, as well as authors' own experience and that of colleagues for the scale development
		  ○ Item generation:
		  ○ Survey development:
		  ○ Finalizing candidate items:
		  ○ Finalizing scale items
		• The scale was validated with a U.S. Census-tailored Qualtrics panel. This is followed by a survey with a sample size of 209.

Rajivan et al.'s questionnaire [117]	• Measures security skills and knowledge • Focuses on 4 security items/questions	Used the four-step procedures from Netemeyer et al. [115] for the questionnaire development. • Identify and define the variable intended to be measured using the scale. • Develop the actual items for the scale • Perform exploratory factor analysis to reduce the scale and extract latent factors that summarize the relationship among original variables to build a prediction model. • Confirm the scale fits the intended model
Hadlington's scale [118]	• Measures human factors in cybersecurity (attitude and behavior)	• Utilized two existing established scales and developed two remaining scales with the help of experts from related fields of study. o Abbreviated impulsiveness scale (ABIS) [119] o Online cognition scale (OCS) [120] o Risky cybersecurity behaviors scale (RScB)- this scale was based on the SeBIS and was created with input from digital forensic investigators and law enforcement o Attitudes towards cybersecurity and cybercrime in business (ATC-IB)- this scale was constructed using expertise from the Police, Digital Forensics, Criminal Psychology, and Cyberpsychology
Öğ˘ütçü et al.'s scale [121]	• Measures security attitude, behavior, and overall awareness	• Utilized the existing established scales: o Risky Behavior Scale (RBS) o Conservative Behavior Scale (CBS) o Exposure to Offence Scale (EOS) o Risk Perception Scale (RPS)
Smartphone Security Behavior Scale (SSBS) [122]	• Measures security behavior • Focuses on 4 security dimensions/areas using 14 security items/questions	• In the first phase, the authors attempt to adapt the SeBIS for smartphone users. But this did not result in the best-fit items. • In the second phase, the authors employed the procedures used by SeBIS for the development of a new set of items for smartphone users.

However, self-reported questionnaires might be biased, as they might not only be influenced by the participants' mood, but participants also often get annoyed if they need to repeatedly answer the same questions. In order to measure the effect of any CSA approach, it is necessary to measure CSA at least before and after the CSA approach. If one wants to study the long-term effect, as one would expect the effects of each CSA approach to fade over time, it might even be necessary to measure CSA more often. This would allow conclusions on how often a certain CSA approach should be repeated. As it is not well researched how repeatedly answering the security and privacy awareness questionnaires might change the results, the repetition might also have an effect on the measurement. On the other hand, it is not possible to just use different scales as the scales are hard to compare and this would not allow a conclusion on how a participant's CSA develops over time.

On the other hand, if CSA is measured for a certain time frame, other events in the participants' life, such as reports in the media about data leaks or security incidents, might also influence their CSA. Thus, it is inevitable to have a control group that is not affected by the CSA measure.

8.2 Poster Evaluation

Alike in other fields, the use of posters is widely popular and common in CSA. Many organizations still produce and use posters for CSA purposes. This popularity of a poster could be because it is one of the simplest mechanisms. Poster initially used to be a conventional method of CSA (i.e., generally uses textual and image content), but this has changed with digital transformation. Utilizing the features of digital technology, its information richness can easily be improved, for example, including a clickable link or QR code that can direct the interested people to a website with detailed information on the subject or with a feedback form. Moreover, using mass media like email, social media, and websites, such posters can be easily disseminated, and their message can be communicated to a large mass audience.

8.2.1 Criteria for Poster Evaluation

Despite the wide use of posters in CSA, there hardly exists any study that has worked on improving the quality or effectiveness of posters for CSA purposes. Therefore, the main objective of this section is to formulate criteria or guidelines, which can facilitate the designer in designing an effective or quality poster for the CSA purpose and to assess the existing CSA posters for their appropriateness. The elicited list of criteria is in Table 6. In addition to that, more criteria on CSA message framing, which are equally applicable to posters, are in Table 14.

Table 14: Additional criteria for poster evaluation

Property	Sub-Properties	Description & Utilization Mechanisms
Style and formatting	Visibility of overall message	The main message (or take-home message) on a poster should be readable from a reasonable distance. There does not exist any defined rule on how far the message should be visible primarily because visibility is influenced by the dimension of a poster as well as where it is placed. If a poster contains any detailed information, it should be distinctly separated from the main message by using a smaller font. Other less important information can be placed at the bottom of the poster in smaller font. However, all font sizes used should be large enough, so the audience does not have to peer at it in order to read.
	Placement of the main message	The main message of a poster should be placed so that it does not get lost, among other details. Based on design conventions, placing the priority content at the front and center [123] of a poster improves its visual prominence.
	Color	Appropriate color and color contrast should be used for a poster design. Answering what color will be suitable for a poster is dependent on a variety of factors, for example, color symbolism (e.g., blue color often symbolizes serenity, stability, inspiration, or wisdom in various cultures), color conventions for scientific purposes (e.g., red color is used to symbolizes stop, bad, danger, warning, enemy, and unsafe), official colors of an organization (e.g., White and Blue are the official colors of the United Nations), and consideration for health issues (e.g., individuals may face difficulty distinguishing certain colors due to color vision deficiency). Further, creating a complementary contrast in the color of content and background improves their visibility [124], i.e., the text is easily visible and readable from a distance. This complementary contrast can be determined by using the *color wheel*. The *color theory* can greatly help with these issues.

	Typography	A poster's text should be easily readable. Making the audience spend extra time to read text is highly discouraging. When selecting an appropriate typeface, ensure the legibility and readability of text [124]. For example, • A poster should select a typeface that works well in multiple sizes and weights to maintain readability in different-sized posters. • A poster should avoid fancy or artistic fonts. • A poster should use decisively contrasting typefaces if multiple typefaces have to be used. • A poster should use mixed or lower case rather than upper case characters [125]. • A poster should use boldface and italic, only if necessary. Underline should be reserved for identifying links. • A poster should avoid reverse type (for example, white text on a dark background). • A poster should appropriately space the elements among themselves.
	Use of image	Including an appropriate image that complements the text on a poster is worth many words. Moreover, it improves the *information richness* [79] and *memorability* [126] of the contents. The memorability of an image depends on various factors, for example, images with people in them are the most memorable [126]. Further, positioning an image in the middle of a poster will make it visible from a distance and help attract the audience's attention.

8.2.2 Outcomes

We evaluated CSA posters for the criteria in Table 6 and Table 14 using an online survey (methodology explained in Section 2.3). We received a valid evaluation for 94 posters out of 117 posters. In total five participants (team members from partner organizations contributing/participating in this task/deliverable, who had a consensus on the interpretation of the properties) assessed to what extent the poster satisfies the given properties in terms of a five-point Likert scale. The posters used for the evaluation purpose were from reputed organizations like ENISA, EUROPOL, Cyber Safe Work, SANS Institute, Global Knowledge, and INFOSEC Institute. They covered security issues and concerns like phishing and social engineering protection, security hygiene, unattended device protection, online child safety, data protection, email protection, malware protection, password protection, and privacy protection. The intention behind this evaluation is never to show whose posters are superior or inferior in quality; rather realize the disparity, if there is any, between the academic recommendations and real-life practice in poster design.

Analysis of the survey data resulted in two important findings, which are:

- The meaning of criteria like "*understandability of the main message*", "*doable suggestion*", "*convenience suggestion*", "*clarity*", and "*use of image*" differ for each individual. They are dependent on the audience's ability (such as security expertise and experience). For example, the same recommendation could be doable for an individual with security knowledge and experience whereas undoable for a naïve person. Similarly, an image that could make sense to one individual would make no sense to another. So, while defining them for usable meaning, one should consider the target audience's ability.
- Interestingly, we found some disparity between academic recommendations and real-life practice in poster design. Almost 50% of the posters did not meet one or multiple of the criteria mentioned

in Table 6 and Table 14. Most of these posters did not meet the aforementioned criteria (i.e., audience's ability dependent). Apart from them, some posters predominantly did not meet these two criteria: "*complete information*", and "*concision*"; particularly, posters with only a slogan on them and with excessively lengthy text respectively. Indeed, putting just a catchy slogan on the poster will help in attracting attention and is easy to remember, however, something without a clear call for actions can cause behavioral change is questionable since behavior change requires also telling what the audience needs to do [127]. Similarly, posters with excessively lengthy text will be demotivating for the audience to read, understand, and practice in everyday life. Instead, these lengthy posters can use an option like providing a link from where to get detailed information for the interested audience.

8.3 Serious Game Evaluation

The term "*Serious Game*" was coined by Abt in the 70s [128], although the idea was not new at that time, e.g., the "*Landlord's game*"', a predecessor of Monopoly, was already created in 1902 to illustrate the dangers of capitalist approaches [129]. Serious games refer to the idea to explore the application of games for other purposes than entertainment. The main challenge of designing serious games is to keep the balance between entertainment and other purposes [130]. As the boundaries between playing and not playing are fuzzy [131], whether the designer succeeds will also depend on the player characteristics and preference for the game type [132]. However, compared to traditional forms of learning serious games are more entertaining and engaging, and have demonstrated potential in industrial education and training disciplines [133].

8.3.1 Criteria for Serious Game Evaluation

There are numerous dimensions to evaluate for serious games. The most obvious dimensions are the entertainment factor and the effectiveness of the serious game. However, there is one other highly important dimension that is worthwhile to investigate. As serious games are highly interactive, it is important to ensure no harm is done to the players or employees. While this might sound surprising at first glance, it can easily be possible that players may be bullied during the game or that their personal data is exposed.

8.3.1.1 Effectiveness

To the best of our knowledge, regarding the general evaluation of serious games, there is not much literature. However, there is a literature survey in a related area on gamification [134], which observes that many papers just offer descriptive statistics and only papers with either all or at least a portion of the tests being positive get published (publication bias). Further problems reported were small sample size, self-developed questionnaires omitting validated psychometric measurements, very short time frames, and the lack of control groups. The literature review also denotes several other points of criticism, such as lack of clarity in reporting the goals of the game and the results. A similar literature review was done on positive effects on computer games in general [135], which also includes a limited number of serious games. Their result was comparable, in particular, they only found one paper explicitly making use of correlations. The only study specifically on serious games for CSA from Tioh et al. [136] also found that evaluations were done with small sample sizes and rather informally. However, the study also covers only a small set of games.

For serious games on CSA, the most natural way to evaluate their effectiveness is to specify their goal as specifically as possible (e.g., knowledge about certain topics, raised awareness about certain issues) and use one of the proposed scales from Section 8.1.

EXTRACTED GUIDELINES

- The desired outcome of the serious game should be specified as specifically as possible.

- Suitable validated and reliable CSA scale(s) should be identified.
- The population should be split into players of the game and a control group who is not participating in the game.
- CSA should be measured at least before and after the game and preferably several times after the game for the group of players as well as the control group.

8.3.1.2 Entertainment

Measuring the entertainment factor is not specific to serious games on CSA. Asking the players directly if they had fun might lead to desirability and social biases. However, not specifically for serious games but for games in general, there are several validated and reliable approaches:

- The game experience questionnaire (GEQ) is used immediately after the game and consists of three parts where the first two probe the players' feelings and thoughts while playing the game; and the third part assesses how players felt after they had stopped playing [137].
- The Player Experience of Need Satisfaction (PENS), elaborated from self-determination theory (SDT), which is a widely researched theory of motivation that addresses both intrinsic and extrinsic motives for acting investigates the effects of gameplay on the player's wellbeing [138].

Johnson et al. [139] provide validation of both questionnaires and list some alternatives in their related work section. Since there is a variety of different game types, e.g., video games, card games, board games, the challenge is to identify a suitable questionnaire that is able to consider the specific properties of the used game type.

Another concept, GameFlow [140] adapts the concept of flow to games. Flow is an experience "*so gratifying that people are willing to do it for its own sake, with little concern for what they will get out of it, even when it is difficult or dangerous*" [141]. In theory, it is also possible to measure physiological measures such as heart rate, respiration rate, electromyography (muscle activation), or electroencephalography (cortical activity [142]. However, these measurements are in general hard to interpret and to connect to the entertainment factor of the player.

EXTRACTED GUIDELINES

1. Identify suitable validated and reliable Game Experience or Game Flow scale(s) according to the properties of the serious game
2. Measure the selected scales during and/or after the game, depending on the requirements of the selected scale

8.3.1.3 Legal and Ethical Assessment

In order to describe the necessity of legal and ethical assessments, we briefly introduce the game HATCH [143], a serious game on social engineering. The aim of HATCH is to foster the players' understanding of social engineering attacks. When playing HATCH, players attack personas in a virtual scenario [144] based on cards with psychological principles and social engineering attacks. While personas are by definition imaginary, they provide a realistic description of stakeholders or in this case employees, who have names, jobs, feelings, goals, and certain needs [145]. This way players can learn about the attackers' perspective, their vulnerabilities and get a better understanding of potential attack vectors. HATCH builds on previous work examining the psychological principles of social engineering [146] and investigating which psychological techniques induce resistance to persuasion applicable for social engineering [147].

However, HATCH can not only be used for training purposes but also to elicit security requirements to prevent social engineering [148]. Instead of the virtual personas, players describe social engineering attacks

on their colleagues. Since players know their colleagues, no persona descriptions are necessary and players can exploit their knowledge about processes in their work environment, i.e., about how to cut through the red tape and informal ways of handling tasks. As a result, at the end of the game, a list of potential attacks can be investigated by the IT department.

HATCH is the first in a cascade of three serious games [149], each with a different purpose as shown in Figure 5 [150]. However, since PROTECT [151] and the CyberSecurity Awareness Quiz [150] are both single-player games, HATCH is the obvious candidate for a legal and ethical assessment. Due to its multiplayer character and when eliciting threats with real scenarios, care has to be taken that no personal data of the players or other employees of the organization are at risk, or some of the players start bullying others.

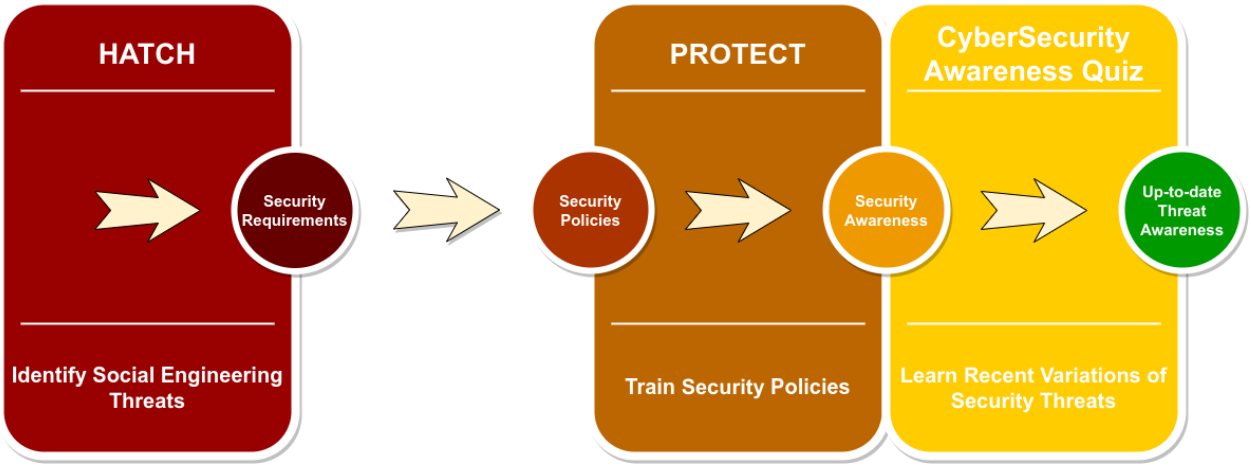

Figure 5: Relation [149] of HATCH [148], PROTECT [151], and the CyberSecurity Awareness Quiz [150]

When playing HATCH with a realistic scenario, the employees' personal information might be at risk if players use it to describe their attacks. Legal requirements demand a careful consideration of conditions the game can be used in. Therefore, a legal analysis of the requirements to use HATCH for threat elicitation was done [152]. The main outcome is that the virtual scenario may be employed without hesitation since players are not victims in the game, and therefore other players do not attack them in the game. The realistic scenario should only be used for threat elicitation since the risk of players accidentally or intentionally exposing other players is real. The use of personas also reduces the risk that players accidentally or intentionally harm other players by revealing personal data in the proposed attacks.

While the assessment was specifically investigating HATCH and one would need to do a legal assessment for each considered serious security game before playing it in an official context, some general conclusions can be drawn. The most important question arising is if employees' personal characteristics are subject to the game. If they are, the organization needs a justification why a more gentle type of training without considering the employees' personal characteristics is not appropriate. This could be the case if the organization wants to conduct threat analysis, for example, because there already have been some incidents, or the organization is specifically exposed to social engineering attacks and wants to mitigate that [153].

From an ethical perspective, one also needs to carefully consider other aspects, such as discrimination. This in particular concerns the virtual scenarios. While it might be natural to develop personas that realistically reflect the situation in most companies, this could lead to stereotypes discriminating certain groups, e.g., women when the managing positions are all modeled with men and subordinate positions such as cleaning

staff are modeled only with female personas. One solution to this problem is to design gender-inclusive personas (cf. [154]). However, this can only be the first step as this version only addresses gender but does not consider any minorities [155].

This shows that legal and ethical aspects are also important evaluation criteria for serious games. While in particular discrimination issues can also occur with posters, they tend to be more obvious there since for a serious game not only the material but also the game's mechanism should be evaluated to investigate if it could support discriminating or bullying behavior of the players.

EXTRACTED GUIDELINES

1. Investigate if the serious game poses a risk to humans, e.g., if their data is used or if the game is a multiplayer game and the interaction between the players could be abused.
2. If any risk is identified, before playing the game do a legal analysis if the game can be played and under which condition, e.g., is it necessary to involve the works council, could there be some other way of raising CSA with less risks.
3. Check ethical aspects of the game, i.e., for the discrimination of groups.

8.3.2 Outcomes

Based on Shostacks's collection of serious games on security [156], we identified relevant serious games with a focus (but not a restriction) on board games and investigated if the games have a scientific background and if so, how the games were evaluated. We had a look at the following games: Control-Alt-Hack [157] [158], OWASP Cornucopia [159], CyberSecurity Awareness Quiz [150], Data Breach [160], d0x3d! [161] [162], Decisions and Disruptions [163], Friend Inspector [164], HATCH [143] [148], NeoSens Training Method [165], OWASP Operation Digital Chameleon [166], Operation Digital Snake [167], PERSUADED [168], Playing Safe [169], Project config.Play [170], PROTECT [151], Protection Poker [171], Security Requirement Education Game (SREG) [172], Security Tactic Planning Poker (SToPPER) [173], Snakes and Ladders [174], The Agile App Security Game [175], and What.Hack [176].

We did a brief check of papers on serious games and could confirm that the patterns for the evaluation of gamification [134] and serious games on CSA [136] also exist for serious games on CSA we investigated. In particular, many papers have small sample sizes and only report descriptive statistics. We did not find any experiment with a control group; most papers were focused on the description of the game and did not provide clear and measurable formulated goals of the game. In almost all cases if there was any measurement it was directly before and/or after the game.

9 Conclusions and Recommendations

The main objective of Task 3.10 was to develop a CSA conceptual model, and monitoring and enhancement methods. It targets both societal security awareness and staff knowledge regarding up-to-date security solutions. Further, there is a responsibility to provide guidelines for the enhancement of societal security awareness as set forth in the proposal. In order to cover these diversified objectives, a conceptual framework for a CSA program has been proposed in this report. The proposed framework answers both "*what to do*" and "*what to expect*" for each activity of the framework that can be useful for the effective monitoring and evaluation of a CSA program. The framework intends to complement other existing frameworks.

In addition to the framework, this report also provided evaluation criteria for two CSA mechanisms that lie on the opposite sides of the complexity scale, which are posters (not interactive but with the simplest form and widely in use for CSA purposes), and serious games (interactive and currently in trend but can be

technically sophisticated). The short analysis of the evaluation criteria showed that some of the recommended criteria for posters can be very subjective, while an inspection of papers introducing serious games on CSA has shown they have fairly deficient evaluations of the games' effectiveness.

As research methodologies, this study used both a nonsystematic LR and an online survey. The LR was used for the conceptual framework, and to elicit the evaluation criteria for the two CSA mechanisms. Likewise, the online survey was used to evaluate selected awareness posters.

The guidelines and practical advice resulting from this study have been issued for CSA professionals and organizations who plan to design, develop, and implement a CSA program more effectively. More specifically, these guidelines and advice will help the individuals in monitoring and evaluating a CSA program. Monitoring assesses the performance of ongoing activities in the light of specified objectives. Similarly, evaluation assesses the overall effectiveness and impacts of the program in the light of specified objectives. Both continuous monitoring of activities and evaluation of programs help in identifying their issues or deficiencies so that they can be corrected as quickly as possible, thus enhancing the effectiveness of CSA activities and programs. A synopsis of the guidelines and practical advice resulting from this study are as follows:

- The team should be inclusive with clearly defined roles, responsibilities, and accountabilities for each member. Moreover, it is advisable to have two full-time staff members, but one full-time staff member is a must for CSA. The individual(s) should be equipped with both technical and soft skills, and also be aware of the context.
- The goals should be clear and simple, and its objectives should be SMART (Specific, Measurable, Attainable, Relevant, Time-bound).
- The audience should be grouped preferably based on their beliefs and cybersecurity expertise.
- The program should receive appropriately high priority in terms of support and participation from the leaders, and budget allocation.
- The selected topics should cover threats prevalent to the audience roles and responsibilities, that include both common and new emerging threats.
- The topics relevant to critical security roles and controls, specific to the organization role and risk profile, relevant to critical projects, neglected by the audience, and with resources readily available should get the high priority.
- The message intensiveness or complexities should be adjusted from general to in-depth depending on the audience.
- The message framing should consider human psychological (cognitive, affective, and different biases) and other factors (usability and user experience) that influence the message reception and interpretation by the audience.
- The message delivery methods should be cost-effective; have a broad outreach; support diversity and inclusiveness; be easy and simple to develop, operate, manage, and update; include standardized assessment and feedback features; support information richness; require minimal additional requirements; and interest and motivate the audience.
- The message communication should consider the psychological and other influencing factors that increase the audience's participation and drive them to practice (or translate into actions) the security knowledge they have learned from the program.
- The enforcement approach used to non-compliance should be a soft approach (mainly using intrinsic incentives) unless a specific need arises for a tough approach.
- The program should be organized periodically, at least once every six months except for responding to new events and situations.

- The lessons learned during the different phases of the program should be properly captured, debriefed, and documented for the effective transfer and use of information.
- The evaluation should measure all four indicators (impact, sustainability, accessibility, and monitoring) to determine the overall effectiveness of the program. Moreover, the measurable parameters selected for each indicator should be economical to gather, consistent to measure, expressible in cardinal number and unit, and contextually specific.
- The program should be adjusted in accordance with the changes in the cybersecurity scenarios. And it should also take into consideration the lessons learned and weaknesses identified from monitoring and evaluation.

10 References

[1] S. K. Katsikas, "Health care management and information system security: Awareness, training or education?," *International Journal of Medical Informatics*, Bd. 60, pp. 129-135, 2000.

[2] M. Bada und J. R. C. Nurse, "Developing cybersecurity education and awareness programmers for small and medium-sized enterprises (SMEs)," *Information & Computer Security*, Bd. 27, Nr. 3, pp. 393-410, 2019.

[3] H. Bruijn und M. Janssen, "Building Cybersecurity Awareness: The need for evidence-based framing strategies," *Government Information Quarterly*, Bd. 34, Nr. 1, pp. 1-7, January 2017.

[4] M. Bada, A. M. Sasse und J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?," in *International Conference on Cyber Security for Sustainable Society*, Coventry, UK, 2015.

[5] L. Spitzner, "Top 3 Reasons Security Awareness Training Fails," Available online: https://www.sans.org/blog/top-3-reasons-security-awareness-training-fails/ (5 August 2021, last accessed).

[6] Hoxhunt, "How to create behavior change with securtiy awareness training? A practical guie," *Available online: https://pages.hoxhunt.com/hubfs/eBooks/How%20to%20create%20behavior%20change%20with%20security%20awareness%20training_.pdf (20 August 2021, last accessed).*

[7] Kaspersky, „The threats from within: How educating your employees on cybersecurity can protect your company,„ http://go.kaspersky.com/rs/802-IJN-240/images/Threats-From-Within-EDU-Ebook%20FINAL.pdf (5 August 2021, last accessed).

[8] M. Siponen, "A conceptual foundation for organzational information security awareness," *Information Management & Computer Security*, Bd. 8, Nr. 1, pp. 31-41, 2000.

[9] M. Wilson und J. Hash, "Building an Information Technology Security Awareness and Training Program - NIST 800-50," U.S. Government Printing Office, 2003.

[10] ENISA, "The new users' guide: How to raise information security awareness," European Union Agency for Cybersecurity, Athens, Greece, November 2010.

[11] N. Kortjan und R. v. Solms, "A conceptual framework for cyber-security awareness and education in SA," *SACJ No. 52,*, July 2014.

[12] M. D. Svinicki, "A guidebook on conceptual frameworks for research in engineering education," National Science Foundation, Alexandria, Virginia , USA, 2010.

[13] Y. Jabareen, "Building a conceptual framework: Philosophy, definitions, and procedure," *International Journal of Qualitative Methods,* Bd. 8, Nr. 4, pp. 49-62, 2009.

[14] B. Levering, "Concept analysis as empirical method," *International Journal of Qualitative Methods,* Bd. 1, Nr. 1, pp. 35-48, 2002.

[15] A. Booth, A. Sutton und D. Papaioannou, Systematic Approaches to a Successful Literature Review, SAGE Publications, 2012.

[16] M. Allen, "Narrative literature reviwe," *The SAGE Encyclopedia of Communication Research Methods*, 2017, https://methods.sagepub.com/reference/the-sage-encyclopedia-of-communication-research-methods/i9413.xml.

[17] ENISA, "Material," Available online: https://www.enisa.europa.eu/media/multimedia/material (3 June 2021, last accessed).

[18] EUROPOL, "Public Awareness and Prevention Guides," Available online: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides (3 June 2021, last accessed).

[19] Cyber Safe Work, "Security Awareness for a Culture of Security," Available online: https://cybersafework.com/free-security-posters/ (3 June 2021, last accessed).

[20] Global Knowledge, "Cybersecurity Awareness Posters," Available online: https://www.globalknowledge.com/us-en/topics/cybersecurity/cybersecurity-awareness-posters/#gref (3 June 2021, last accessed).

[21] SANS Institute, "Posters," Available online: https://www.sans.org/security-awareness-training/resources/posters (3 June 2021, last accessed).

[22] InfoSec Institute, "Top 20 security awareness posters with messages that STICK," Available online: https://resources.infosecinstitute.com/topic/top-20-security-awareness-posters-messages-stick/ (3 June 2021, last accessed).

[23] C. Vroom und R. v. Solms, "A Practical Approach to Information Security Awareness in the Organization," in *Ghonaimy M.A., El-Hadidi M.T., Aslan H.K. (eds) Security in the Information Society*, Boston, MA, USA, Springer, 2002, pp. 19-37.

[24] M. Beyer, S. Ahmed, K. Doerlemann, S. Arnell, S. Parkin, M. A. Sasse und N. Passingham, "Awareness is only the first step: A framework for progressive engagement of staff in cyber security," Hewlett Packard Enterprise, December 2015.

[25] D. Ki-Aries, S. Faily und K. Beckers, "Persona-Driven Information Security Awareness," in *30th British Human Computer Interaction Conference*, Bournemouth, UK, 11-15 July 2016.

[26] A. Ghazvini und Z. Shukur, "A Framework for an Effective Information Security Awareness Program in Healthcare," *(IJACSA) International Journal of Advanced Computer Science and Applications*, Bd. 8, Nr. 2, 2017.

[27] Y. Wang, B. Qi, H.-X. Zou und J.-X. Li, "Framework of raising cyber security awareness," in *18th IEEE International Conference on Communication Technology*, 2018.

[28] The United Nations Office for Disaster Risk Reduction, "Monitoring and Evaluation Framework," Available online: https://www.undrr.org/publication/monitoring-and-evaluation-framework (17 August 2021, last accessed).

[29] S. Chaudhary, "D9.13: Awareness effectiveness study 1," CyberSec4Europe, Brussel, Belgium, 2021.

[30] A. Hueca, B. Manley und L. Rogers, "Building a cybersecurity awareness program," Software Engineering Institute, Carnegie Mellon Universtiy, Pittsburgh, PA, USA, 2020.

[31] L. Spitzner, D. deBeaubien und A. Ideboen, "The rising era of awareness training," SANS Security Awareness Report, Bethesda, MD, USA, 2019.

[32] SANS, "Maturity Model," Available online: https://www.sans.org/security-awareness-training/resources/maturity-model/ (12 Jan 2022, last accessed).

[33] N. Farvaque, E. Voss, M. Lefebvre und K. Schütze, "Guide for Training in SMEs," Available online: https://ec.europa.eu/social/BlobServlet?docId=3074&langId=en (01 February 2022, last accessed).

[34] B. D. Voss, "The Ultimate Defense of depth: Security Awareness in Your Company," SANS Institute, Bethesda, Maryland, USA, 2020.

[35] J. M. Haney und W. G. Lutters, "Skills and characteristics of successful cybersecurity advocates," in *Workshop on Security Information Workers, Symposium on Usable*, Santa Clara, CA, USA, 12-14 July , 2017.

[36] I. Winkler und S. Manke, "7 reasons for security awareness failure". *Available online: https://www.csoonline.com/article/2133697/7-reasons-for-security-awareness-failure.html (11 November 2021, last accessed).*

[37] PCI Security Standards Council, "Information Supplement: Best Practices for Implementing a Security Awareness Program," PCI Security Standards Council, Wakefield, Massachusetts, United States, October 2014.

[38] S. Manke und I. Winkler, "The Habits of Highly Successful Security Awareness Programs: A Cross-Company Comparision," Secure Mentem & Wombat Security Technologies, USA, 2012.

[39] L. Spitzner, "Goals and Objectives: Where to Start with Your Awareness Program," SANS, https://www.sans.org/blog/goals-and-objectives-where-to-start-with-your-awareness-program/, 30 January 2019.

[40] S. Mustaca, "Define S.M.A.R.T IT Security Goals," (ISC)2, https://blog.isc2.org/isc2_blog/2013/02/define-smart-it-security-goals.html, 14 February 2013.

[41] Z. Ahmad, M. Norhashim, O. T. Song und L. T. Hui, "A typology of employees' information security behaviour," in *4th International Conference on Information and Communication Technology*, Bandung, Indonesia, 25-27 May 2016.

[42] J. M. Stanton, K. R.Stam, P. Mastrangelo und J. Jolton, "Analysis of end user security behaviors," *Computers & Security*, Bd. 24, Nr. 2, pp. 124-133, March 2005.

[43] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor und J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," in *CM Conference on Human factors in Computing System*, Atlanta, GA, USA, 10-15 April 2010.

[44] N. Ameen, A. Tarhini, M. H. Shah und N. O. Madichie, "Employees' behavioural intention to smartphone security: A gender-based, cross-national study," *Computers in Human Behavior*, Bde. %1 von %21-14, pp. 106-, 2020.

[45] A. T. Shappie, C. A. Dawson und Scott M. Debb, "Personality as a predictor of cybersecurity behavior," *Psychology of Popular Media*, Bd. 9, Nr. 4, p. 475–480, 2020.

[46] T. N. Jagatic, N. A. Johnson, M. Jakobsson und F. Menczer, "Social Phishing," *Communications of the ACM*, Bd. 50, Nr. 10, pp. 94-100, 2007.

[47] Y. Amichai-Hamburger und E. Ben-Artzi, "Loneliness and Internet use," *Computers in Human Behaviour*, Bd. 19, Nr. 1, pp. 71-80, January 2003.

[48] T. Halevi, J. Lewis und N. Menon, "A pilot study of cybersecurity and privacy related behaviour and personality traits," in *22nd International Conference on World Wide Web*, Rio de Janeiro,Brazil, 13-17 May 2013.

[49] A. Farooq, J. Isoaho, S. Virtanen und J. Isoaho, "Information security awareness in educational instituion: An analysis of students' individual factors," in *IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 20-22 Aug. 2015.

[50] A. Bostan und İ. Akman, "ICT user and usage characteristics and e-mail security awareness," in *International Conference on Electronics, Computer and Computation*, Ankara, Turkey, 7-9 Nov. 2013.

[51] W. Kruger und H. Kearney, "Can perceptual differences account for enigmatic information security behaviour in an organisation?," *Computers & Security*, Bd. 61, pp. 46-58, 2016.

[52] A. Onumo, A. Cullen und I. Ullah-Awan, "An emipircal study of cultural dimensions and cybersecurity development," in *IEEE 5th International Conference on Future Internet of Things and Cloud*, Prague, Czech Republic, 2017.

[53] L. R. Goldberg, "The Structure of Phenotypic Personality Traits," *American Psychologist*, Bd. 48, Nr. 1, pp. 26-34, January 1993.

[54] J. Schrammel, C. Köffel und M. Tscheligi, "Personality traits, usage patterns and information disclosure in online communities," in *23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, Cambridge, UK, September 2009.

[55] J. D. Russell, C. F. Weems, I. Ahmed und G. .. R. III, "Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors," *Journal of Cyber Security Technology*, Bd. 1, Nr. 3-4, pp. 163-174, 2017.

[56] E. Bottomley, C. Munnelly, L. Tryl und S. Wride, "What makes a successful campaign?," *Available online: https://cms.wellcome.org/sites/default/files/public-first-literature-review.pdf (19 August 2021, last accessed).*

[57] Osterman Research, "The ROI of Security Awareness Training," *Available online: https://www.mimecast.com/globalassets/documents/whitepapers/osterman-the-roi-of-security-awareness-training.pdf (23 September 2021, last accessed).*

[58] L. Coventry, P. Bridge, J. Blythe und M. Tran, "Using behavioural insights to improve the public's use of cyber security best practices," Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf (17 August 2021, last accessed).

[59] S. Manke und I. Winkler, "The habits of highly successful security awareness programs: A cross-company comparision," Secure Mentem, Severna Park, Maryland, USA, 2012.

[60] A. Blau, "The behavioural economics of why executives underinvest in cybersecurity," *Harvard Business Review*, pp. Available: https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity, 07 June 2017.

[61] N. M. Menon und M. T. Siponen, "Executives' commitment to information security: Interaction between the preferred subordinate influence aproach (PISA) and proposal characteristics," *The DATABASE for Advances in Information Systems*, Bd. 51, Nr. 2, pp. 36-53, May 2020.

[62] M. A. Sasse, D. Ashenden, D. Lawrence, L. Coles-Kemp, I. Flechais und P. Kearney, "Human vulnerabilities in security systems," Human Factors Working Group, Cyber Security KTN Human Factors White Paper, London, UK, 2007.

[63] ENISA, "ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected," 2020, Available online: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020 (14 September 2021, last accessed).

[64] A. Caballero, "Security education, training, and awareness," in *Computer and Information Security Handbook*, Burlington, MA, USA, Morgan Kaufmann Publishers, 2017, pp. 497-505.

[65] DNV, "Probability and uncertainty: Some things are more uncertain than others," Available online: https://www.dnv.com/Images/Cyber-security-whitepaper-Probability-and-uncertainty_tcm8-137894.pdf (12 January 2022, last accessed).

[66] J. A. Valentine, "Enhancing the employee security awareness model," *Computer Fraud & Security*, Bd. 6, pp. 17-19, 2006.

[67] S. Chaudhary, "SME cybersecurity awareness 2," CyberSec4Europe, Brussel, Belgium, 2021.

[68] S. Furnell und I. Vasileiou, "Security education and awareness: Just let them burn?," *Network Security*, Bd. 2017, Nr. 12, pp. 5-9, December 2017.

[69] J. H. Meyer und R. Land, "Threshold concepts and troublesome knowledge: Linkages to ways of thinking and practising within the disciplines," in *10th Improving Student Learning Symposium*, Brussels, Belgium, 2002.

[70] S. Talib, Personalising information security education, Plymouth, UK: University of Plymouth, 2014.

[71] I. Vessey, "Cognitive fit: A theory-based analysis of the graphs versus tables literature," *Decision Sciences*, Bd. 22, p. 219–240, 1991.

[72] A. Kelton, R. R. Pennington und B. M. Tuttle, "The effects of information presentation format on judgement and decision making: A review of information system research," *Journal of Information Systems*, Bd. 24, Nr. 2, pp. 79-105, November 2010.

[73] S. M. Smith und R. E. Petty, "Message Framing and Persuasion: A Message Processing Analysis," *Personality and Social Psychology Bulletin* , Bd. 22, Nr. 3, pp. 257-268, March 1996.

[74] R. v. Bavel und N. Rodríguez-Priego, "Nudging Online Security Behaviour with Warning Messages: Results from an Online Experiment," Available online: https://publications.jrc.ec.europa.eu/repository/handle/JRC103223 (12 November 2021, last accessed).

[75] R. M. Entman, "Framing: Towards Clarification of a Fractured Paradigm," *Journal of Communication*, Bd. 43, Nr. 4, pp. 51-58, 1993.

[76] M. Siponen, "Five dimensions of information security awareness," *Computer and Society*, Bd. 31, Nr. 2, pp. 24-29, 2001.

[77] P. Dolan, M. Hallsworth, D. Halpern, D. King und I. Vlaev, "MINDSPACE Influencing behavior through public policy," Available online: https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf (17 August 2021, last accessed).

[78] R. Shaw, C. C. Chen, A. L. Harris und H.-J. Huang, "The impact of information richness on information securit awareness training effectiveness," *Computers & Education*, Bd. 52, Nr. 1, pp. 92-100, 2009.

[79] R. Daft und R. Lengel, "Information richness: A new approach to managerial behavior and organizational design," *Research in Organizational Behavior*, Bd. 6, pp. 191-233, 1984..

[80] U. E. Gattiker, "Can an early warning system for home users and SMEs make a difference? A field study," in *International Workshop on Critical Information Infrastructures Security*, Samos Island, Greece, 2006.

[81] R. E. Lundgren und A. H. McMakin, "Social media," in *Risk communication: A handbook for communicating environmental, safety, and health risks*, Hoboken, NJ, USA, Wiley,, 2018, pp. 347-368..

[82] J. Braithwaite und T. Makkai, "Trust and compliance," *Policing and Society*, Bd. 4, Nr. 1, pp. 1-12, 1994.

[83] R. Herold, Managing an Information Security and Privacy Awareness and Training Program, Boca Raton, USA: Auerbach Publications, 2005.

[84] L. Darling-Hammond, L. Flook, C. Cook-Harvey, B. Barron und D. Osher, "Implications for educational practice of the science of learning and development," *Applied Developmental Science*, Bd. 24, Nr. 2, pp. 97–140,, 2020.

[85] D. Maheswaran und J. Meyers-Levy, "The influence of message framing and issue involvement," *Journal of Marketing Research,* Bd. 27, Nr. 3, pp. 361-367,, August 1990.

[86] Microsoft Canada, "Attention spans," Available onlie: https://dl.motamem.org/microsoft-attention-spans-research-report.pdf (5 Auguts 2021, last accessed).

[87] S. Stockhardt, B. Reinheimer, M. Volkamer, P. Mayer, A. Kunz, P. Rack und D. Lehmann, "Teaching phishing security: Which way is best?," in *31st International Conference on ICT Systems Security and Privacy Protection*, Ghent, Belgium, 2016.

[88] E. C. Johnson, "Security Awareness: Switch to a better programme," *Network Security*, Bd. 2006, Nr. 2, p. 15–18, 2006.

[89] E. S. Ruboczki, "How to develop cloud security awareness," in *10th Jubilee International Symposium on Applied Computational Intelligence and Informatics*, Timisoara, Romania, 21-23 May 2015.

[90] D. D. Maeyer, "Setting up an effective information security awareness programme," in *SECURE 2007 Conference*, Warsaw, Poland, 2007.

[91] M. Pattinson, M. Butavicius, B. Ciccarello, M. Lillie, K. Parsons, D. Calic und A. McCormac, "Adapting cyber security training to your employees," in *12th International Symposium on Human Aspects of Information Security & Assurance*, Dundee, Scotland, UK, 2018.

[92] N. Nachin, C. Tangmanee und K. Piromsopa, "How to increase cybersecurity awareness," *ISACA Journal,* Bd. 2, Nr. 2018, pp. 45-50, 1 March 2019.

[93] C. S. G. González, P. Toledo und F. B. Izquierdo, "Integrating the principles of DGBL, CSCL and playability in the design of social videogames: a case of study," in *Student Usability in Educational Software and Games: Improving Experiences*, Hershey, USA, IGI Global, 2012, pp. 293-304.

[94] K. Mabitle und E. Kritzinger, "School teacher Preference of Cyber-Safety Awareness Delivery Methods: A South African Study," in *Silhavy R. (eds) Artificial Intelligence and Bioinspired Computational Methods. CSOC 2020. Advances in Intelligent Systems and Computing*, Springer, Cham, 2020.

[95] I. Kirlappos, S. Parkin und M. A. Sasse, ""Shadow security" as a tool for the learning organisation," *SIGCAS Computers & Society,* Bd. 45, Nr. 1, pp. 29-37, 2015.

[96] M. A. Bawazir, M. Mahmud, N. N. A. Molok und J. Ibrahim, "Persuasive technology for improving Information security awareness and behavior: Literature review," in *6th International Conference on Information and Communication Technology for The Muslim World*, Jakarta, Indonesia, 22-24 Nov. 2016.

[97] A. Adams und M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, Bd. 42, Nr. 12, pp. 40-46, 1999.

[98] I. Kirlappos, A. Beautement und A. Sasse, "Comply or Die Is Dead: Long live security-aware principal agents," in *Adams A.A., Brenner M., Smith M. (eds) Financial Cryptography and Data Security*, Okinawa, Japan, 1 April 2013.

[99] E. G. E. Kyonka, "Law of Effect," in *Naglieri J.A. (eds) Encyclopedia of Child Behavior and Development*, Boston, MA, Springer, 2011.

[100] S. T. Lawson, S. K. Yeo, H. Yu und E. Greene, "The cyber-doom effect: The impact of fear appeals in the us cyber security debate.," in *8th International Conference on Cyber Conflict*, Tallinn, Estonia, 31 May-3 June 2016.

[101] K. Renaud und M. Dupuis, "Cybersecurity fear appeals: Unexpectedly complicated," in *New Security Paradigm Workshop*, San Carlos, Costa Rica, 23-26 September 2019.

[102] University of Waterloo, "Curve of Forgetting," Available online: https://uwaterloo.ca/campus-wellness/curve-forgetting (20 September 2021, last accessed).

[103] B. Davis und M. Summers, "Applying Dale's Cone of Experience to increase learning and retention: A study of student learning in a foundational leadership course," in *Engineering Leaders Conference 2014 on Engineering Education*, Doha, Qatar, 8-11 Nov 2014.

[104] F. Pass und J. J. G. v. Merriënboer, "Cognitive-Load Theory: Methods to Manage Working Memory Load in the Learning of Complex Tasks," *Current Directions in Psychological Science*, Bd. 29, Nr. 4, p. 394–398, 8 July 2020.

[105] B. Reinheimer, L. Aldag, P. Mayer, M. Mossano, R. Duezguen, Bettina, T. v. Landesberger und M. Volkamer, "An investigation of phishing awareness and education over time: When and how to best remind users," in *Sixteenth Symposium on Usable Privacy and Security*, 10-11 August 2020.

[106] S. Hansche, "Designing a security awareness program: Part 1," *Information Systems Security*, Bd. 9, Nr. 6, pp. 1-9, 2001.

[107] B. Timmermans und A. Cleeremans, "How can we measure awareness? An overview of current methods," in *M. Overgaard (Ed.), Behavioural Methods in Consciousness Research*, Oxford, UK, Oxford University Press, 2015, p. 21–46.

[108] ENISA, "Information security awareness initiatives: Current practice and the measurement of success," Available online: https://ifap.ru/library/book206.pdf (11 September 2021, last accessed).

[109] C. Manifavas, K. Fysarakis, K. Rantos und G. Hatzivasilis, "DSAPE: Dynamic security awareness program evaluation," in *16th International Conference on Human-Computer Interaction*, Crete, Greece, 2014.

[110] A. Jaquith, Security metrics: Replacing fear, uncertainty, and doubt, Boston, Massachusetts, United States: Addison-Wesley Professional, 2015.

[111] W. Ashford, "Cyber crime widely under-reported, Isaca study shows," ComputerWeekly, 04 Jun 2019, https://www.computerweekly.com/news/252464401/Cyber-crime-widely-under-reported-Isaca-study-shows .

[112] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson und C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Computer & Security*, Bd. 42, pp. 165-176, 2014.

[113] M. Karjalainen, "Improving employees' information systems (IS)security behaviour: toward a meta-theory of is security training and a new framework for understanding employees' is security behaviour," University of Oulu, Oulu, Finland, 2011.

[114] S. Egelman und E. Peer, "Scaling the security wall: Developing a security behaviour intention scale (SeBIS)," in *CHI*, Seoul, Republic of Korea, 18-23 April 2015.

[115] R. G. Netemeyer, W. O. Bearden und S. Sharma, Scaling Procedures: Issues and Applications, SAGE Publications Inc., 2003.

[116] C. Faklaris, L. D. und J. I. Hong, "A self-report measure of end-user security attitudes (SA-6)," in *USENIX Symposium on Usable Privacy and Security (SOUPS)*, Santa Clara, CA, USA, August 11 - 13, 2019.

[117] P. Rajivan, P. Moriano, T. Kelley und L. J. Camp, "Factors in an end user security expertise instrument," *Information & Computer Security*, Bd. 25, Nr. 2, pp. 190-205, 2017.

[118] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, Bd. 3, Nr. 7, Jlu 2017.

[119] C. G. Coutlee, C. S. Politzer, R. H. Hoyle und S. A. Huettel, "An Abbreviated Impulsiveness Scale (ABIS) Constructed through Confirmatory Factor Analysis of the BIS-11," *Arch Sci Psychol*, Bd. 2, Nr. 1, p. 1–12., April 2014.

[120] R. A. Davis, G. L. Flett und A. Besser, "Validation of a new scale for measuring problematic internet use: implications for pre-employment screening," *Cyberpsychol Behav*, Bd. 4, Nr. 5, pp. 331-345, August 2002.

[121] G. Öğ˘ütçü, Ö. M. Testik und O. Chouseinoglou, "Analysis of personal information security behavior and awareness," *Computer & Security*, Bd. 56, pp. 83-93, 2016.

[122] H.-Y. Huang, S. Demetriou, R. Banerjee, G. S. Tuncay, C. A. Gunter und M. Bashir, "Smartphone Security Behavioral Scale: A New Psychometric Measurement for Smartphone Security," in *https://arxiv.org/abs/2007.01721*, 2020.

[123] J. Nielsen, "Horizontal attention leans left," Nielsen Norman Group, Fremont, CA, USA, 22 October 2017, https://www.nngroup.com/articles/horizontal-attention-original-research/.

[124] P. Kahn und K. Lenk, "Design: Prnciples of typography for user interface design," *Interactions*, Bd. vol. 5, Nr. no. 6, pp. 15-29,, Novmber 1998.

[125] M. Paterson und D. Tinker, "Influence of type form on speed of reading," *Journal of Applied Psychology*,, Bd. 12, Nr. 4, p. 359–368, 1928..

[126] P. Isola, D. Parikh, A. Torralba und A. Oliva, "Understanding the intrincis memorability of images," in *25th Conference on Neural Information Processing Systems*, Granada, Spain, 12-17 December, 2011.

[127] A. Christiano und A. Neimand, "Stop Raising Awareness Already," Standfor Social Innovation Review, Stanford, CA , United States, 2017.

[128] C. C. Abt, Serious Games, New, York: The Viking Press, 1970.

[129] D. Parlett, The Oxford history of board games, Oxford University Press, USA, 1999.

[130] C. Franzwa, Y. Tang und A. Johnson, "Serious game design: Motivating students through a balance of fun and learning," in *2013 5th International conference on games and virtual worlds for serious applications (VS-GAMES)*, 2013.

[131] K. S. Tekinbas und E. Zimmerman, Rules of play: Game design fundamentals, MIT press, 2004.

[132] G. F. Tondello und L. E. Nacke, "Player Characteristics and Video Game Preferences," in *The Annual Symposium on Computer-Human Interaction in Play*, Barcelona, Spain, 22-25 October 2019.

[133] J. C. K. H. Riedel und J. B. Hauge, "State of the art of serious games for business and industry," in *2011 17th International Conference on Concurrent Enterprising*, 2011.

[134] J. Hamari, J. Koivisto und H. Sarsa, "Does gamification work?--a literature review of empirical studies on gamification," in *2014 47th Hawaii international conference on system sciences*, 2014.

[135] T. M. Connolly, E. A. Boyle, E. MacArthur, T. Hainey und J. M. Boyle, "A systematic literature review of empirical evidence on computer games and serious games," *Computers \& Education*, Bd. 59, pp. 661-686, 2012.

[136] J.-N. Tioh, M. Mina und D. W. Jacobson, "Cyber security training a survey of serious games in cyber security," in *Frontiers in Education Conference (FIE)*, 2017.

[137] W. A. IJsselsteijn, A. W. de Kort and Yvonne und K. Poels, "The game experience questionnaire," *Eindhoven: Technische Universiteit Eindhoven*, Bd. 46, 2013.

[138] R. M. Ryan, C. S. Rigby und A. Przybylski, "The motivational pull of video games: A self-determination theory approach," *Motivation and emotion*, Bd. 30, pp. 344-360, 2006.

[139] D. Johnson, M. J. Gardner und R. Perry, "Validation of two game experience scales: the player experience of need satisfaction (PENS) and game experience questionnaire (GEQ)," *International Journal of Human-Computer Studies*, Bd. 118, pp. 38-46, 2018.

[140] P. Sweetser und P. Wyeth, "GameFlow: a model for evaluating player enjoyment in games," *Computers in Entertainment (CIE)*, Bd. 3, pp. 3-3, 2005.

[141] M. Csikszentmihalyi und M. Csikzentmihaly, Flow: The psychology of optimal experience, Bd. 1990, Harper & Row New York, 1990.

[142] L. E. Nacke, "An introduction to physiological player metrics for evaluating games," in *Game analytics*, Springer, 2013, pp. 585-619.

[143] K. Beckers, S. Pape und V. Fries, "HATCH: Hack And Trick Capricious Humans -- A Serious Game on Social Engineering," in *Proceedings of the 2016 British {HCI} Conference, Bournemouth, United Kingdom, July 11-15, 2016*, 2016.

[144] V. Hazilov und S. Pape, "Systematic Scenario Creation for Serious Security-Awareness Games," in *Computer Security - {ESORICS 2020} International Workshops, {DETIPS}, {DeSECSys}, {MPS}, and {SPOSE}, Guildford, {UK}, September 17-18, 2020, Revised Selected Papers*, Cham, 2020.

[145] S. Faily und I. Flechais, "Persona cases: a technique for grounding personas," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011.

[146] P. Schaab, K. Beckers und S. Pape, "A systematic Gap Analysis of Social Engineering Defence Mechanisms considering Social Psychology," in *10th International Symposium on Human Aspects of Information Security {\&} Assurance, {HAISA} 2016, Frankfurt, Germany, July 19-21, 2016, Proceedings.*, 2016.

[147] P. Schaab, K. Beckers und S. Pape, "Social engineering defence mechanisms and counteracting training strategies," *Information and Computer Security*, Bd. 25, pp. 206-222, 2017.

[148] K. Beckers und S. Pape, "A Serious Game for Eliciting Social Engineering Security Requirements," in *Proceedings of the 24th IEEE International Conference on Requirements Engineering*, 2016.

[149] S. Pape, *Requirements Engineering and Tool-Support for Security and Privacy*, 2020.

[150] S. Pape, L. Goeke, A. Quintanar und K. Beckers, "Conceptualization of a CyberSecurity Awareness Quiz," in *Computer Security - {ESORICS} 2020 International Workshops MSTEC*, Cham, 2020.

[151] L. Goeke, A. Quintanar, K. Beckers und S. Pape, "PROTECT - An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks," in *Computer Security - {ESORICS} 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26-27, 2019, Revised Selected Papers*, Cham, 2019.

[152] D.-K. Kipker, S. Pape, S. Wojak und K. Beckers, "Juristische Bewertung eines Social-Engineering-Abwehr Trainings," in *State of the Art: IT-Sicherheit für Kritische Infrastrukturen*, S. Rudel und U. Lechner, Hrsg., Neubiberg, : Universität der Bundeswehr, 2018, pp. 112-115.

[153] S. Pape und D.-K. Kipker, "Case Study: Checking a Serious Security-Awareness Game for its Legal Adequacy," *Datenschutz und Datensicherheit*, Bd. 45, pp. 310-314, 05 2021.

[154] M. R. Lopes und C. Vogel, "The Influence of Personas' Gender in Design," in *14th Biannual Conference of the Italian SIGCHI Chapter*, Bolzano, Italy, 11 - 13 July 2021.

[155] S. Pape, "Challenges for Designing Serious Games on Security and Privacy Awareness," in *Privacy and Identity Management. "It's complicated": Exploring the relationship between cybersecurity and privacy, and improving training and awareness. 16th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School. Revised Selected Papers*, Springer, 2022, p. (to appear).

[156] A. Shostack, *Website: Security Games & Resources*, 2018.

[157] T. Denning, A. Lerner, A. Shostack und T. Kohno, "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education," in *2013 {ACM} {SIGSAC} Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*, 2013.

[158] T. Denning, A. Shostack und T. Kohno, "Practical Lessons from Creating the Control-Alt-Hack Card Game and Research Challenges for Games In Education and Research," in *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education, 3GSE '14, San Diego, CA, USA, August 18, 2014.*, 2014.

[159] OWASP, *OWASP Cornucopia Homepage.*

[160] M. Kyle, *Gamecrafter Homepage for Data Breach.*

[161] M. Gondree und Z. N. J. Peterson, "Valuing Security by Getting [d0x3d!]: Experiences with a Network Security Board Game," in *6th Workshop on Cyber Security Experimentation and Test, {CSET} '13, Washington, D.C., USA, August 12, 2013*, 2013.

[162] M. Gondree, Z. N. J. Peterson und T. Denning, "Security through Play," *{IEEE} Security {\&} Privacy*, Bd. 11, pp. 64-67, 2013.

[163] U. a. G. B. C. S. Bristol, *Decisions and Disruptions Homepage*, Available online: https://www.decisions-disruptions.org/ (14 January 2022, last accessed).

[164] A. Cetto, M. Netter, G. Pernul, C. Richthammer, M. Riesner, C. Roth und J. Sänger, "Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks," *CoRR*, Bd. abs/1402.5878, 2014.

[165] T. Romand-Latapie, "The NeoSens Training Method: Computer Security Awareness for a Neophyte Audience," in *Blackhat 2016*, 2016.

[166] A. Rieb und U. Lechner, "Operation Digital Chameleon -- Towards an Open Cybersecurity Method," in *Proceedings of the 12th International Symposium on Open Collaboration (OpenSym 2016)*, Berlin, 2016.

[167] A. Rieb, *KMA Homepage Article about Operation Digital Snake Game.*

[168] D. Aladawy, K. Beckers und S. Pape, "PERSUADED: Fighting Social Engineering Attacks with a Serious Game," in *{Trust, Privacy and Security in Digital Business - 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5-6, 2018, Proceedings}*, 2018.

[169] M. Newbould und S. Furnell, "Playing Safe: A prototype game for raising awareness of social engineering," *Australian Information Security Management {\ldots}*, pp. 24-30, 2009.

[170] H. Enriquez, Y. Kadobayashi und D. Fall, "Project config. Play a Turn-Based Strategy Security Board Game," in *ECGBL 2018 12th European Conference on Game-Based Learning*, 2018.

[171] L. Williams, A. Meneely und G. Shipley, "Protection Poker: The New Software Security "Game"," *Security Privacy, IEEE*, Bd. 8, pp. 14-20, May 2010.

[172] A. Yasin, L. Liu, T. Li, J. Wang und D. Zowghi, "Design and Preliminary Evaluation of a Cyber Security Requirements Education Game (SREG)," *Information and Software Technology* , pp. - , 2017.

[173] F. Osses, G. Márquez, C. Orellana und H. Astudillo, "Towards the selection of security tactics based on non-functional requirements: Security tactic planning poker," in *2017 36th International Conference of the Chilean Computer Science Society (SCCC)*, 2017.

[174] OWASP, *OWASP Snakes and Ladders Homepage.*

[175] C. Weit, *The Agile App Security Game*, 2018.

[176] Z. A. Wen, Y. Li, R. Wade, J. Huang und A. Wang, "What.Hack: Learn Phishing Email Defence the Fun Way," in *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 2017.

Annex A: CSA Frameworks

Vroom & von Solms [23] provide the elements for a successful security awareness program in an organization. The elements have been obtained by asking and satisfactorily getting answers to the following four questions:

- Who establishes the need for information security awareness in general in the organization?
- What sources should be applied in the execution of the program?
- Who develops the program?
- How should the program be structured?

Moreover, the proposed model for information security awareness comprises of the following components that essentially answer the aforementioned four questions. In Figure 6, each level represents a component.

- *Establishing the need for information security awareness*: Accentuates the need for awareness to management and users. (1 and 2 in Figure)
- *Sources used for the information security awareness program*: Specifies the foundation on which to build an awareness program, for example, international information security standards and security policies. (3 and 4 in Figure)
- *Responsibility of developing the information security awareness program*: Sets up a dedicated individual or team to oversees, coordinates, and manages an awareness program. (5 in Figure)
- *Construction of the information security awareness program*: Structures an awareness program for different users. For example, a general CSA for all employees and specialized ones for employees with certain roles in the organization. (6 and 7 in Figure)

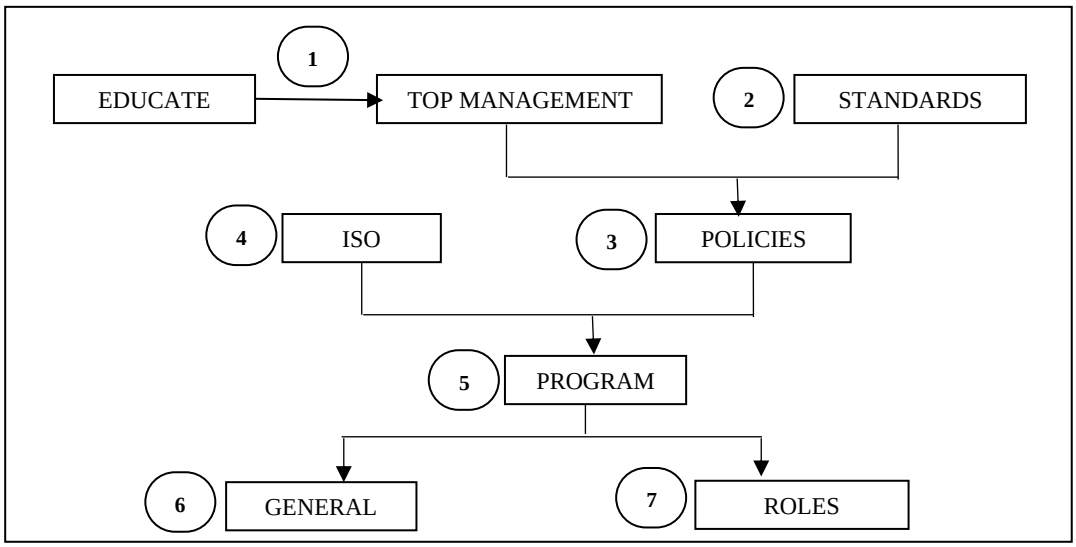

Figure 6: Information security awareness model [23]

The NIST report provides guidelines towards a comprehensive security awareness and training program on IT infrastructures [9]. The proposed approach particularly focuses on the following phases of a security awareness and training program:

i. *Designing phase*: In this phase, the awareness program is designed, the necessary awareness and training materials are developed, and ultimately the awareness program is implemented. This phase provides an overall structure of the awareness and training program. The NIST approach proposes three models to facilitate the management of the overall process: a) centralized program management, b) partially decentralized program management, and c) fully decentralized program management.
ii. *Development phase*: This phase describes the process of developing awareness materials considering specific security awareness topics and sources. Additionally, the development of training materials is described with a particular focus on security awareness courses.
iii. *Implementation phase*: This phase describes the process of the program's implementation. Namely, communicating the plan to the organization is described to be important for achieving support for the program's implementation and commitment of necessary resources. In addition, the techniques for delivering awareness and training materials are described (e.g., posters, newsletters, etc.).
iv. The NIST framework provides an iterative process where the result of each phase can be monitored and validated via the *post-implementation phase* (i.e., program success indicators, evaluation, and feedback).

The four phases and their respective processes are shown in Figure 7.

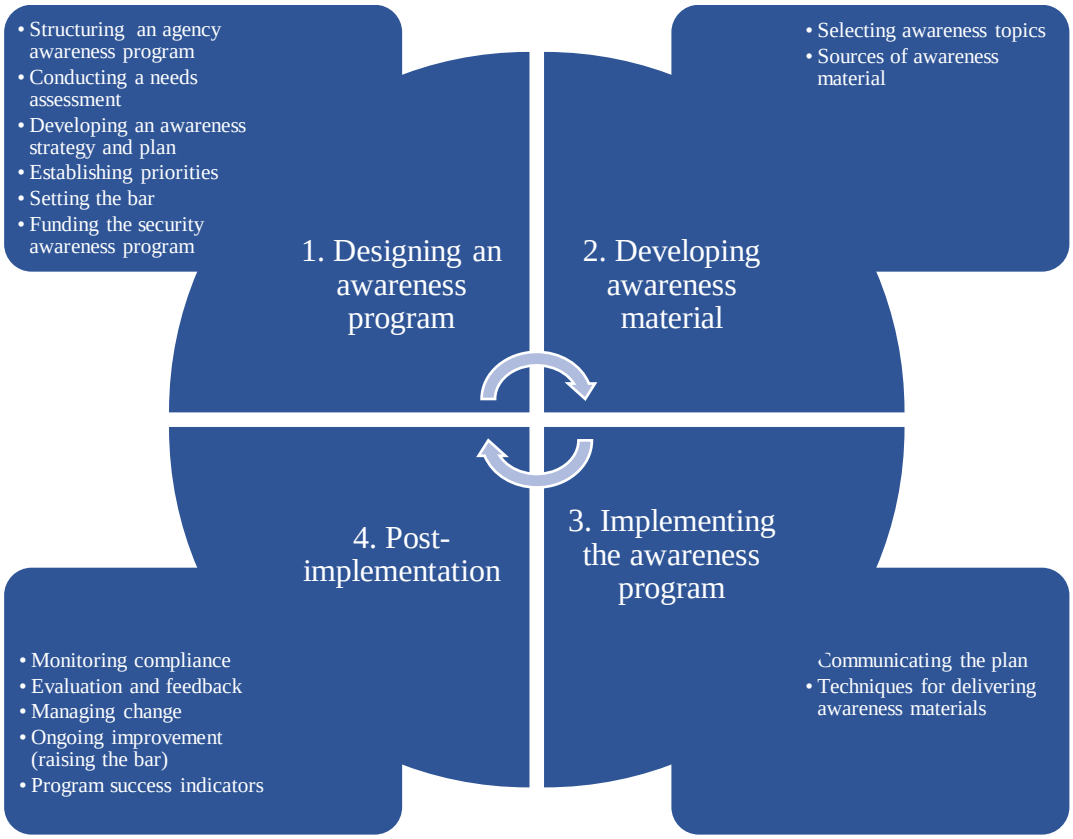

Figure 7: NIST CSA framework

The ENISA [10] proposes a general framework that provides guidelines for the public and private organizations towards an effective CSA program. Particularly, the guidelines are focused on analyzing awareness topics, developing business cases and communication frameworks, implementing the awareness program, and evaluating and improving the awareness program. Further, ENISA proposes three main processes towards the development of an effective information security awareness program, which are:

i. *Plan, assess, and design*: This phase includes identification of the organizational needs, development planning based on the needs, and establishing priorities (i.e., defines goal and objectives, the team set up, clarify the target group, identify needful personnel and materials, determine communication methods, define success criteria, establish a baseline for evaluation, etc.).
ii. *Execute and manage*: In this phase, analysis of the organizational needs, development of the accordant strategy, an association of the program and strategy, and development of the necessary materials are performed (i.e., program team confirmation, work plan review/revision, program implementation, communicating awareness contents, document lessons learned, etc.).
iii. *Evaluate and adjust*: This phase appraises the establishment of the requirements of the awareness program, as well as the design and implementation of feedback strategy and accordant mechanisms (i.e., conduct evaluation, gather data and feedback, review objectives, implement lessons learned, adjust the program, etc.).

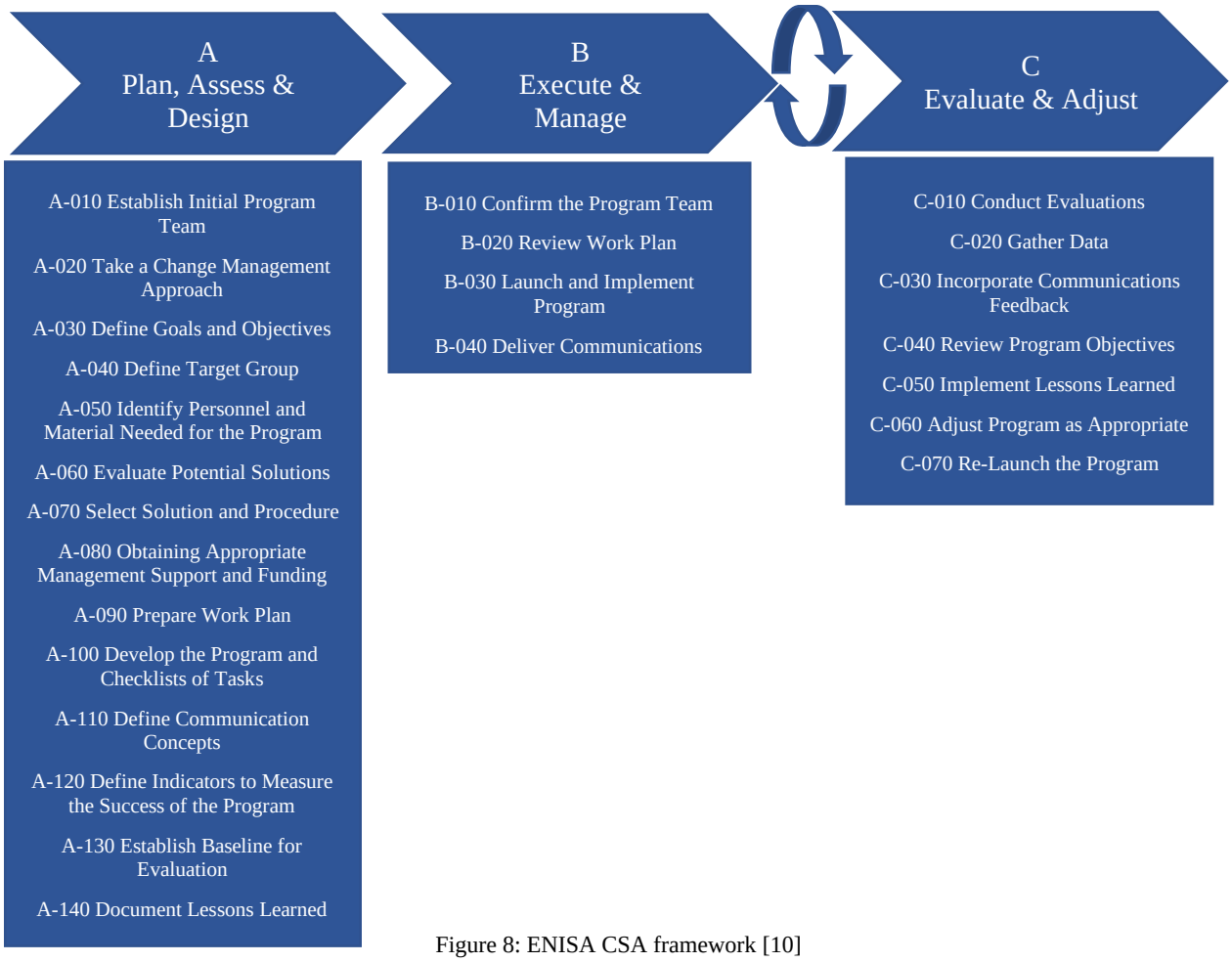

Figure 8: ENISA CSA framework [10]

The guidelines provide a comprehensive representation of a CSA program. The proposed framework consists of three levels: i) processes, ii) sub-processes, and iii) activities. The three processes and related sub-processes are illustrated in Figure 8.

Kortjan et al. [11] propose a CSA and education framework that would assist in nurturing a cybersecurity culture in the Internet users in South Africa. Building upon the result of a literature review, a five-layer framework is proposed shown in Figure 9. The proposed framework is based on specific key factors derived from the literature review.

The five layers of the proposed framework are listed below:

i. *Strategic layer:* Represents the organization/government view regarding cybersecurity aspects (legislations, regulations, etc.) [*overall vision*].
ii. *Tactical layer*: Represents the schemes/methods that are needed to achieve the national goals and enhance CSA and education [*national cybersecurity campaign*].
iii. *Preparation layer:* Describes the contents of the schemes/methods identified above [*topics, content, medium, and tools*].
iv. *Delivery layer:* Represents the involved stakeholders and, more importantly, the recipients of the content of the previous layer [*target audience*].
v. *Monitoring layer:* Analyzes the progress considering the national strategy/goals [*monitoring and evaluation of the progress*].

The framework aims to enhance CSA in South Africa by leveraging existing good practices, legislation, and regulation from the papers reviewed. However, the targeted audience is the citizens of a specific country. The adoption of the proposed framework in different countries where different guidelines, and regulations exist is not discussed.

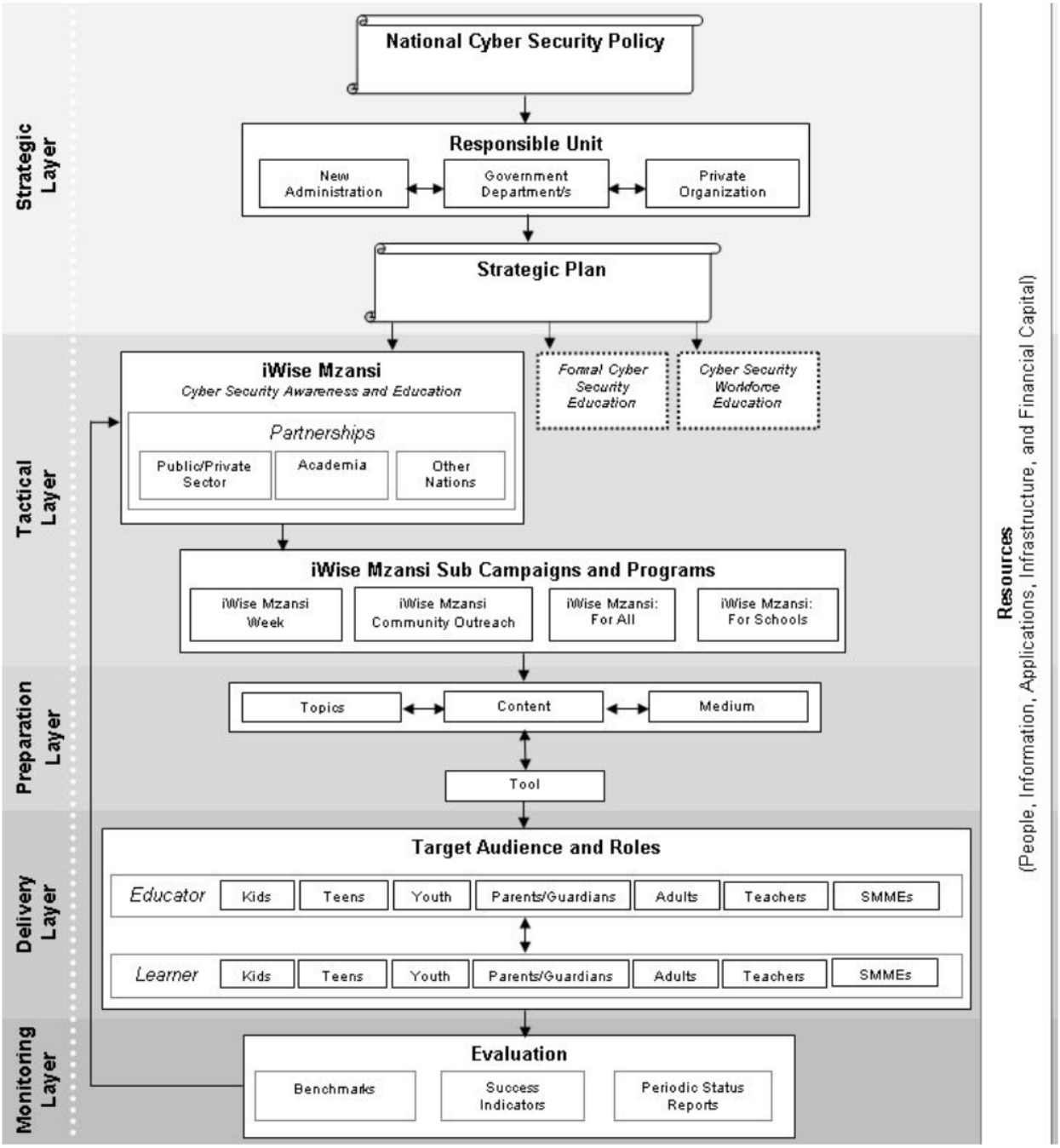

Figure 9: Cyber security awareness and education framework [11]

Beyer et al. [24] propose a progressive engagement framework for the lifecycle of awareness activities. The framework presents awareness to a continuous process that needs to be implemented and revisited over time. It consists of four steps shown in Figure 10 and explained next.

- *Awareness profiling*: This phase is about assessing and measuring different relevant factors in the organization to identify its security awareness needs. This also helps to realize the gaps (deviation between the current and desired) in or obstacles to the existing awareness efforts of the organization. In other words, this is about establishing the needs and scope of the awareness campaign. It utilizes various quantitative and qualitative methods depending on the needs.
- *Awareness planning*: This phase is about defining the goals and objectives of the security awareness campaigns, and roles and responsibilities of the team, and planning the overall steps needed for the campaigns. This also includes the relevant improvements in the existing awareness efforts.
- *Transformation*: In this phase, security awareness activities are implemented or put into practice according to the plan.
- *Optimization*: This phase involves revisiting the existing awareness efforts and make necessary improvements if the desired state or level of awareness has not been achieved. However, the optimization efforts or improvements could have unforeseen implications.

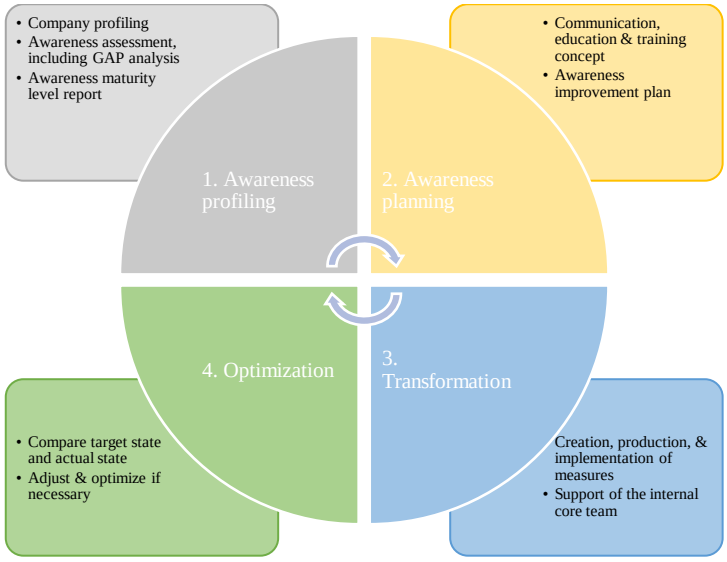

Figure 10: Progressive engagement Framework

Ki-Aries et al. [25] propose a persona driven information security awareness process. The process's activities are organized in a cyclic order similar to the NIST framework for information security [9]; however, it also considers the input and output recommendations Beyer et al. [24] that include on-going awareness, with a range of relevant topics that are targeted, actionable, doable, and provides feedback to help sustain peoples' willingness to change [4].

The six steps or activities shown in Figure 11 are explained next.

- *Needs & goals*: Identifies business needs, goals, and chosen awareness theme based on a risk analysis.
- *Personas*: Develops personas based on empirical data collected through observations and interviews, which is transcribed, refined, and modelled to produce personas tailored to the business.
- *Analysis*: Analyze personas against the findings of step 1, leading to recommendations towards an awareness approach suited to the target organization.

- *Design and development*: Apply selected recommendations for design and development, which considers the resource, budget, and communication methods available.
- *Implement*: begins the implementation of the program, where metrics may be applied.
- *Review*: concludes by reviewing the cycle's effectiveness towards raising awareness and considers improvements and the integration of new information or technology ensuring the process remains up to date, then continues on to repeat the cycle of activities and the chosen awareness theme.

Figure 11: Persona-driven information security awareness process [25]

Ghazvini et al. [26] propose a security awareness framework focusing on training programs shown in Figure 12. The scope of this work is threefold:

i. to develop a framework that provides guidelines for the healthcare sector,
ii. to develop a security awareness training program, and
iii. to propose a game for security training in the healthcare domain.

The framework suggests the following towards the development of a security awareness training program:

i. *Common information security issues within the healthcare organization*: the common cybersecurity issues in healthcare are identified based on the literature review.
ii. *Suggest/update the security policies following legislation and standards*: review the existing policies and regulations, and update when it is necessary based on international standards and legislation.
iii. *Create a targeted audience profile to facilitate the learning process*: e.g., beginners, professionals, and experts.
iv. *Organize the delivery process of the training program*: e.g., paper-based, online, game-based, etc.
v. *Continuous enhancement of the training program*: the training program addresses the employees' needs and preferences.

The framework focuses on the healthcare domain with a game-based delivery method. Contemporary organizations strive for a holistic security awareness approach to capture several aspects of awareness programs such as the implementation, training, and evaluation.

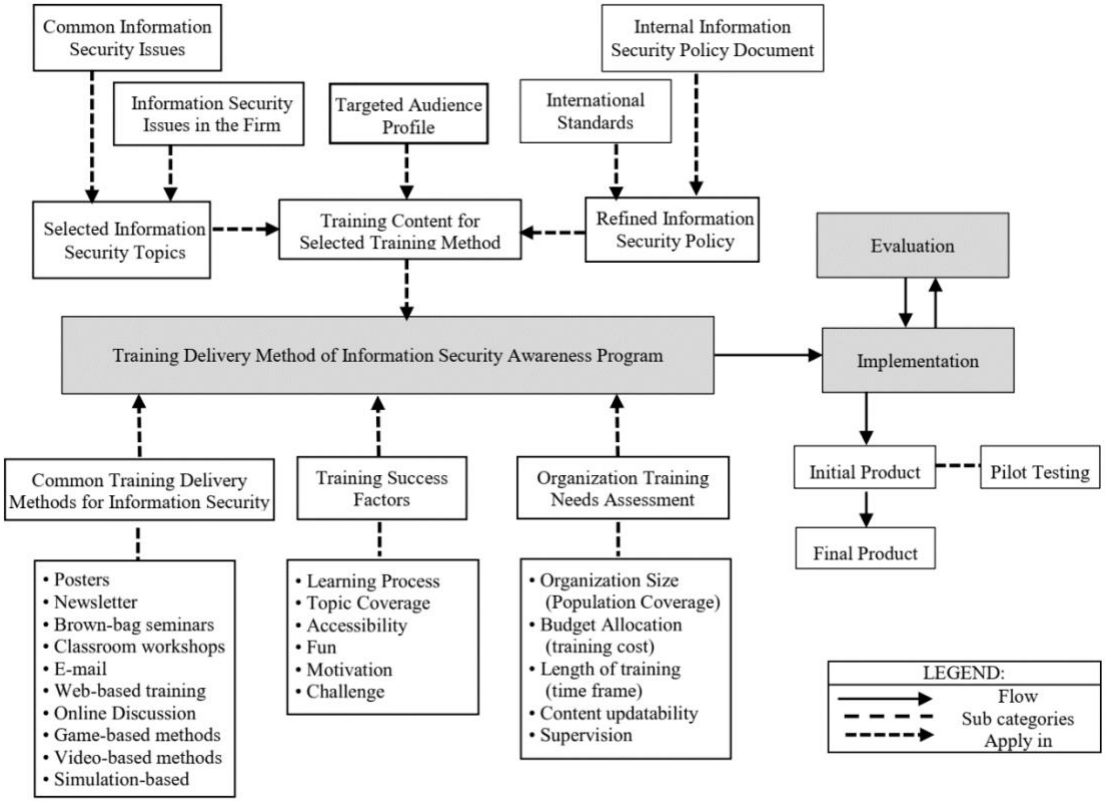

Figure 12: Training method selection framework [26]

Wang et al. [27] propose a CSA framework shown in Figure 13. They propose a platform to facilitate the raising of CSA using standards and guidelines from both academia and industry. The proposed framework is based on perception, protection, and behavior theory. The core of the proposed framework are the three levels listed below:

i. *Cognition/testing:* Provides a comprehensive understanding of the threat landscape and the relevant risks.
ii. *Knowledge and skills/evaluation:* Enables the analysis of the people's CSA in a specific situation.
iii. *Training/training:* Represents the necessary technical and theoretical means to increase CSA considering the two previous levels.

Overall, the framework is based on statistical models and aims to quantify the CSA levels focusing on the effectiveness of persons, evaluation, and training. Further, a CSA -raising platform is developed that consists of the knowledge classification and attribute index of the targeted audience. The main elements of the platform are:

i. *Knowledge & skills assessment system:* Represents the opinion of the cybersecurity expert.

ii. *Cognitive ability testing system*: Represents the objective measurement and scientific evaluation of the targeted audience.
iii. *Personnel risk assessment system:* Refers to the risk assessment of the targeted audience to acquire a comprehensive picture of CSA.
iv. *Training system:* Represents the required cybersecurity activities and resources towards an effective CSA program.

The applicability of the framework is illustrated with two experiments involving 600 and 400 participants. The proposed framework is based on testing, training, and evaluation. However, the description of each phase is only partially analyzed (possible ways for training or evaluation). Further, the stakeholders' involvement is only partially mentioned, and the role and responsibilities are not fully clarified. Further, the connection between the proposed framework and the proposed platform is not fully elaborated.

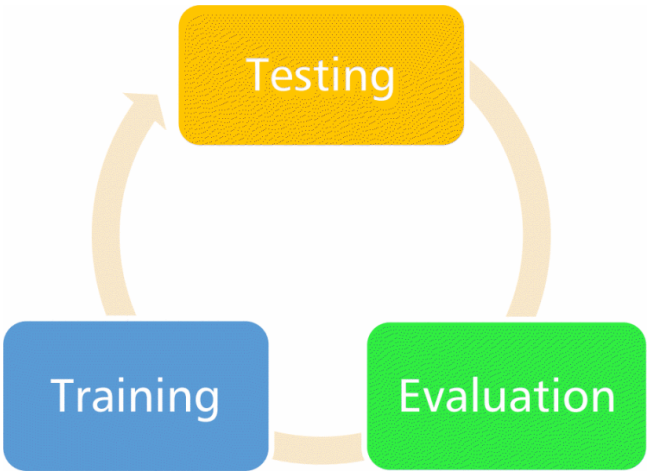

Figure 13: Testing, evaluation, and training (TET) CSA raising framework [27]

Bada & Nurse [2] propose a framework for the CSA program for SMEs. In order to craft this framework, the authors initially performed a systematic literature review of the past cybersecurity awareness, education, and training initiatives. This is followed by a case study of the UK's London Digital Security Center that offers cybersecurity awareness, education, and guidance primarily to SMEs based in London. In the case study, a survey is used to collect quantitative and qualitative data from member SMEs. Finally, by utilizing the best practices in research and industry (identified from the literature review) and findings from the case study, the authors crafted their proposition. The framework comprises the following five primary areas, also shown in Figure 14.

- *Initial engagement with SMEs*: It mainly emphasizes reaching out to SMEs. This can be done by visiting SMEs with trusted parties; making a presence at events, workshops, and conferences attended by SMEs; conducting SME-focused seminars, events, and workshops; and building relationships with industry and trade bodies that target SMEs.
- *Improving security practices & culture*: This includes conducting CSA programs in SMEs. This is done by establishing the needs of CSA in SMEs followed by planning, implementing, and reviewing necessary CSA programs.
- *Program resources*: This is related to identifying and preparing appropriate CSA resources and services that are freely available.

- *Trusted third-party resources/services*: This recommends partnering with vetted third parties who can offer CSA services and resources at reduced costs.
- *Communication strategy*: This emphasizes the importance of appropriate communication channels so that relevant security information can be delivered to SMEs in a timely manner.

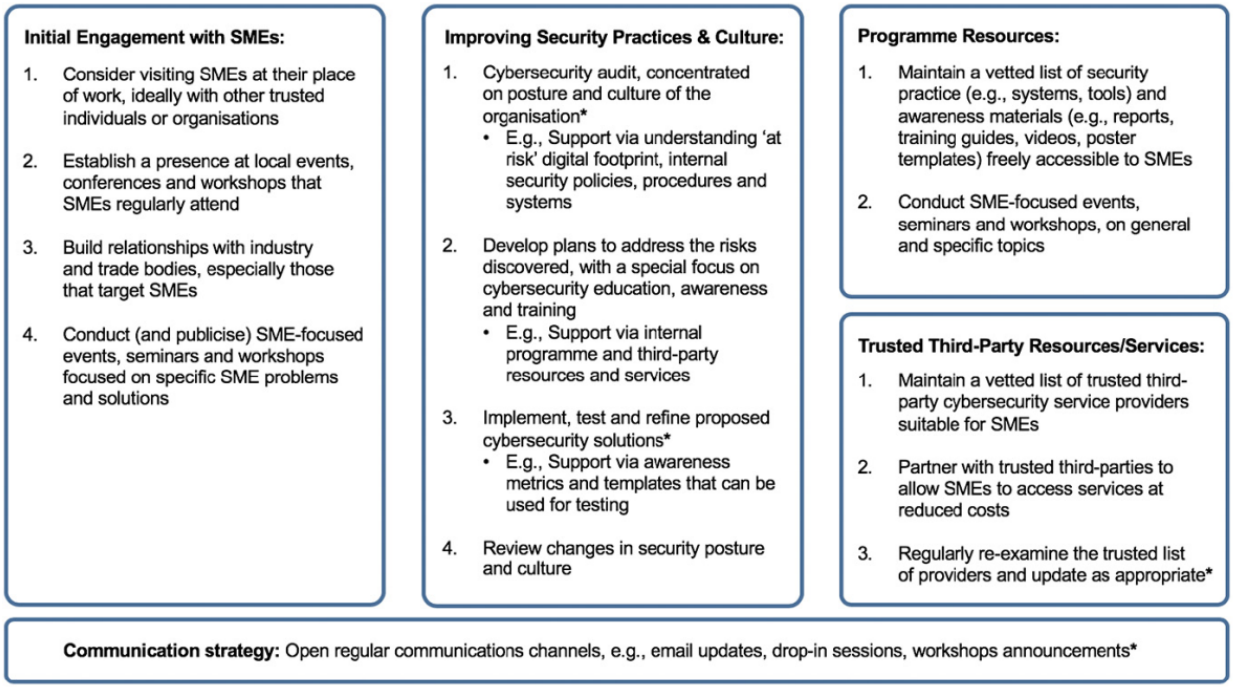

Figure 14: A CSA program for SMEs/SMBs [2]