Carnegie Mellon University
Software Engineering Institute

Building a Cybersecurity Awareness Program

Angel Hueca
Brittany Manley
Larry Rogers

Contents

Introduction

Awareness of Internet security issues is a benefit to all, from the seasoned systems administrator, to the home user paying a bill online or streaming a movie, to users just now learning about computers and the Internet. Managing the security of our personal information, and maintaining ownership of the goods and services we've purchased are universal challenges. The Internet community knows few geographical bounds, and foundational cybersecurity awareness is critical to the safety of the general public.

Users, defined as those who use an organization's resources, are often an organization's weakest link. Intruders focus on taking advantage of users[1] to gain access to an organization's networks and its sensitive information. Through techniques such as phishing, masquerading, or social engineering, intruders attempt to manipulate human emotions. Users may have access to critical data, login credentials, and other information that, if improperly used, could cause harm to an organization. While many organizations have put technical solutions in place to mitigate these malicious activities, security solutions require an *embedded culture of cybersecurity awareness to be truly effective.*

In this document we present a top-level collection of commonly accepted best practices and guidance to help you build a successful cybersecurity awareness program for your organization. This guidance was derived from the experiences of the Software Engineering Institute (SEI) and leverages resources from the National Institute of Standards and Technology (NIST),[2] and the Forum of Incident Response and Security Teams (FIRST).[3] We intend to leave you with:

- best practices for the development and design of cybersecurity awareness programs
- a consideration of roles and responsibilities in cybersecurity awareness programs
- a discussion of how to design and implement an awareness program
- ideas for running a cybersecurity awareness campaign at your organization or for your constituency
- a look ahead—considering cybersecurity awareness as a service

While cybersecurity awareness can be described in many different ways depending on the organization and organizational need, *awareness* is not equivalent to *training.* The purpose of awareness, as defined by NIST Special Publication (SP) 800–16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* "is simply to focus attention on security." Awareness is "intended to allow individuals to recognize IT security concerns and respond accordingly." In addition, FIRST describes the purpose of awareness as a service to "increase the overall security posture of the constituency and help its members to detect, and recover from incidents; ensure that constituents are better prepared and educated." Both of these descriptions center around the notion of enhancing an employee or user's awareness of how to properly recognize and respond to some type of questionable online activity, or an anomaly to their daily computing practices. This is important because the user is the first line of defense for an organization's cybersecurity posture.

Audience

We have written this guide primarily for the following groups:

- organizational leaders and managers
- organizational cybersecurity stakeholders
- information technology and cybersecurity managers
- Cybersecurity Center, Security Operations Center (SOC), or Computer Security Incident Response Team (CSIRT) staff
- CSIRTs of National Responsibility
- Sector-based CSIRTs

1 Employee and User are not always the same thing. An employee is a person who works for your organization, and could be an internal user of your information systems. Users may be individuals outside of your organization who are authorized to have or to use some aspect of the organizational information system.

2 NIST, a non-regulated federal agency in the United States, is responsible for the promotion of U.S. innovation, advancing measurement science, standards, and technology.

3 FIRST aims to enable incident response teams to effectively respond to security incidents by providing best practices, tools, and trusted communication mechanisms with other member security teams.

A successful cybersecurity awareness program is designed to change user behavior and reinforce good computer usage and security practices.

Scope

This document provides organizations with best practices for approaching, designing, and implementing cybersecurity awareness programs for users, as well as guidance that can be incorporated into an existing IT security program or developed for a cybersecurity awareness campaign. While the primary objective of a cybersecurity awareness program is to educate users on safe computing and their responsibility in protecting their organization's information and assets, different audiences require different levels of engagement, different types of training, and different levels of security controls. When considering the scope of a cybersecurity awareness program, all users of an organization's IT resources should be included—from end users to supervisors to executive level managers. Additional considerations should be given to the audience, the goals of the awareness building program, and the scope of the effort. Note that specific cybersecurity training techniques are outside the scope of this document; instead, this document will primarily focus on the considerations for and design of an organizational cybersecurity awareness program or campaign rather than specific cybersecurity training needs.

PROGRAM OR CAMPAIGN: WHAT'S WHAT?

Cybersecurity awareness programs and cybersecurity awareness campaigns

Organizations and teams referencing this document may be interested in developing a comprehensive cybersecurity awareness program, a cybersecurity awareness campaign, or both. While a campaign implies a difference in scope (campaigns may be more dedicated to a particular focus or topic area), much of the design and components of a cybersecurity awareness program will also apply to a campaign.

How to Use this Document

This document should be used by individuals and teams who are responsible for cybersecurity awareness programs or campaigns, or any organizational entity tasked with designing a program to enhance user awareness. The document highlights key considerations and provides process-based applications for you to leverage in your own organizations, sectors, economies, or countries. Readers must continue to keep in the mind the following considerations, as the application and implementation of this guidance should always be aligned with

- your constituents
- your audience
- the goals and objectives of awareness building
- the scope of your awareness effort

There are many activities included within the design and development of an awareness program or campaign. It is important to understand that the program should be tailored to meet the needs of your organization. While there is not a one-size-fits-all approach, this document provides some commonalities and considerations that can be applied across various awareness programs.

Cybersecurity Awareness Programs: Purpose and Best Practices

An awareness program's primary focus is informing users of cyber risks in an effort to influence user behavior, and assisting the user in making the right decisions when interacting with computers and the Internet as they perform their daily responsibilities. Users *must* be aware of common fraud and phishing schemes as well as basic techniques malicious actors use to trick unsuspecting users into performing an unintended act. A well-designed cybersecurity awareness program should foster organizational learning and support the overall organizational mission from the perspective of security. Without organizational learning, users will lack the background or skills to identify common threats to the information systems they work on.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program,* outlines three components seen in successful cybersecurity awareness programs. These are

1. Establishing an information technology security policy that reflects business needs and addresses known risks
2. Informing users of their responsibilities
3. Identifying reoccurring processes for monitoring and reviewing the program

In addition, industry experts outline the following components as best practice, some of which have already been mentioned:

- Leadership involvement: Senior leadership should support the awareness program; users will be aware of senior leadership involvement and will react accordingly.
- Persistence: For an awareness program, best practice is to build a year-long plan with specific learning milestones throughout the year.
- Relevance: Cybersecurity awareness programs should be relevant to the users and their day-to-day tasks.
- Immediate feedback: Providing hands-on training reinforces awareness activities covered in the campaign or program.
- Assessments: To determine any required adjustments, you need to understand where the program started and how it is progressing. Using identified metrics will help determine adjustments that needs to be made.

Taking all of this into consideration, a cybersecurity awareness program should be applicable to all users of your organization, with management taking the lead and setting an example for all users. The cybersecurity awareness program functions as a vehicle for information dissemination within the organization and is kept current, with adjustments made according to current threats and changes in how the organization responds to threats.

Effective cybersecurity awareness programs should also inform and educate users of security policy expectations and updates to security policies and procedures for compliance purposes. Ultimately, users need to be made aware of what is expected of them, and any non-compliance will justify accountability. A cybersecurity awareness program that develops a well-informed workforce—keenly aware of expectations, risks, and threats—will lead to increased security for the organization as a whole.

Learning Continuum

To set the context for designing an awareness program, it is important to understand the foundational components of the *learning continuum.* Both NIST SP 800-16 and NIST SP 800-50 describe levels of learning along a continuum. The continuum begins with awareness, builds into training, and develops into education. An organization can apply these categorizations to determine a user's proficiency at any of these levels within the learning continuum. This type of model is role-based and assumes users will have different roles within the organization, along with different responsibilities and relationships to IT resources.

Along the learning continuum, learning progresses as a user's security responsibilities expand within the organization. At the very bottom layer, all employees or users need cybersecu*rity awareness.* The training layer is comprised of "security basics and literacy" along with "roles and responsibilities relative to IT systems." This stage of the continuum represents training requirements for all individuals in a role which requires specialized knowledge involving security threats, vulnerabilities, mitigation strategies, and safeguards. The education layer, "education and experience," is applicable to individuals within the organization who have made information security their profession.

The learning continuum allows organizations to evaluate individuals against the learning continuum, determine their cybersecurity awareness needs, and identify and adequately scope awareness activities at the appropriate level depending on the audience. Note that within this document, we are primarily focused on the awareness level of the learning continuum.

LEARNING CONTINUUM LAYERS

AWARENESS

Design your cybersecurity awareness efforts to change employee behaviors and reinforce good security practices. NIST Special Publication 800-16 asserts that "awareness is not training," but rather awareness is focused on helping individuals to recognize cybersecurity concerns. With awareness, the individual is the recipient of information, whereas in training, the participant has an active role in learning activities.

TRAINING

Train people to produce relevant and needed security skills and competencies. In comparison to awareness, training aims to teach skills which allow a person to perform a specific function. In contrast, awareness focuses on the individual's attention to an issue or a set of issues.

EDUCATION

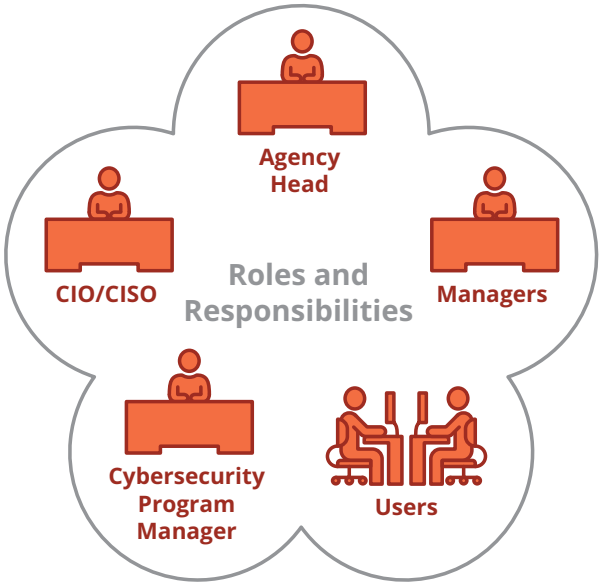
This body of knowledge strives to produce cybersecurity professionals capable of proactive cybersecurity response.

Understanding Your Environment

Before your organization or team can begin designing an awareness program or campaign, it is important to first understand the environment that you operate within. There are many factors to consider, but the primary considerations should be understanding your

- roles and responsibilities
- external or ancillary stakeholders
- existing policy, regulation, or legislation
- cybersecurity culture
- the business case
- budget

All of these factors must be considered as you design and implement an effective awareness program or campaign. These considerations, at the very least, will help determine how to move forward in the design of a program, who will be responsible for the program, and how it will be affected by existing constraints and challenges. These primary considerations will also help you determine the audience and goals and objectives of an awareness program or campaign.



Roles and Responsibilities

Teams function and coordinate more efficiently when there is a common understanding of individuals' roles and responsibilities within the organizational or team architecture. Often, this clear understanding can be lacking; people may not understand how these roles and responsibilities work together in order to accomplish the organizational mission. While understanding directives and guidance outlined in specific policies is important when starting a cybersecurity awareness program, it is of utmost importance that organizations understand who the responsible parties are in the design, development, and implementation of cybersecurity awareness programs.

Table 1 identifies example parties as outlined by NIST SP 800-50. Depending on the organization, agency, or team, one person may be fulfilling the duties of multiple roles. The following table provides a high level example of possible responsible parties.

Table 1

AGENCY OR ORGANIZATIONAL HEAD	Assign responsibility for IT and cybersecurity.
	Ensure cybersecurity program is implemented.
CHIEF INFORMATION OFFICER (CIO) OR CHIEF INFORMATION SECURITY OFFICER (CISO)	Establish overall cybersecurity awareness program strategy.
	Ensure that all senior managers and data owners understand the concepts and strategy of the cybersecurity awareness program, and are informed of the program progress and implementation.
CYBERSECURITY PROGRAM MANAGER	Ensure awareness and training materials developed are appropriate and timely for the intended audience.
	Depending on your organization, this may be an IT Security Program Manager or other designee, or the role may be assumed by an incident response team of a parent organization.
MANAGERS	Work with organizational leaders to meet shared responsibilities.
	Ensure all users are appropriately trained to fulfill the cybersecurity responsibilities for the systems they access.
USERS	Understand and comply with agency cybersecurity policies and procedures.
	Be appropriately trained in the rules of behavior for the systems and applications that they have access to.
ANCILLARY STAKEHOLDERS	Participate or be involved in the design and implementation of cybersecurity awareness programs in an ancillary role.
	Examples may include, but are not limited to, Human Resources, Talent Management, Training Departments, and Communications/Public Relations.

Responsible Parties in a Cybersecurity Awareness Program (adapted from NIST SP 800-50)

Additional Stakeholders

When developing cybersecurity awareness programs or campaigns for entities outside of your organization, there may be additional groups to involve throughout the design and implementation phases of a program. This is particularly applicable to Cybersecurity Centers, SOCs, or CSIRTs interested in developing cybersecurity awareness programs or campaigns for a wider constituency or community. Table 2 identifies the additional groups to consider.

Table 2

STAKEHOLDER	Any organization or entity which has an interest or some other value-related concern with your organization/team.
	May not be directly served by the organization/team, but may receive significant secondary benefits.
	Organizations or entities that may be called upon to provide inputs such as funding, staffing, policy advice and guidance, or legal authorities.
CONSTITUENT	A subset of the stakeholders.
	Organizations or entities which will be served by your organization/team (for example, those that have cybersecurity and incident response services provided to them).
COMMUNITY	Broader set of tangential and related organizations which have some relationship with your organization/team, but may not fit the definition of stakeholders or constituents.
	Examples may include, but are not limited to, local, regional, or international incident response organizations, CSIRTs of National responsibility, international communities of CSIRTs, CSIRTs in neighboring countries, or sector CSIRTs.

Additional Stakeholder Groups

Regulation or Legislation

As we noted earlier, cybersecurity awareness is intended to shape user behavior in support of information security. This includes awareness of organizational rules, policies, and requirements. These requirements are often defined and communicated within an information security policy (ISP). The ISP outlines user information security behavior and computer usage that the organization considers compliant, as well as organizational expectations of the users. The ISP may also align with specific policy or regulatory requirements that must be met to be aligned with an obligation outlined by a governing body. These regulatory requirements may be provided to the organization at the national, state, local, and/or organizational level. A user who does not take appropriate actions, or behaves in a way that is not acceptable based upon the established measures, is not only out of compliance, but also causes the organization to be out of compliance.

Typically, regulatory compliance pertains to specific industries or sectors. It is important to consider and incorporate existing and applicable regulation when designing and implementing a cybersecurity awareness program. Here are a few examples of regulations that may pertain to specific countries, regions, and sectors.

- The European Union (EU) General Data Protection Regulation (GDPR) defines personal data, security program, and breach notification requirements for companies that process data of EU citizens and subjects who are in the EU/European Economic Area (EEA).

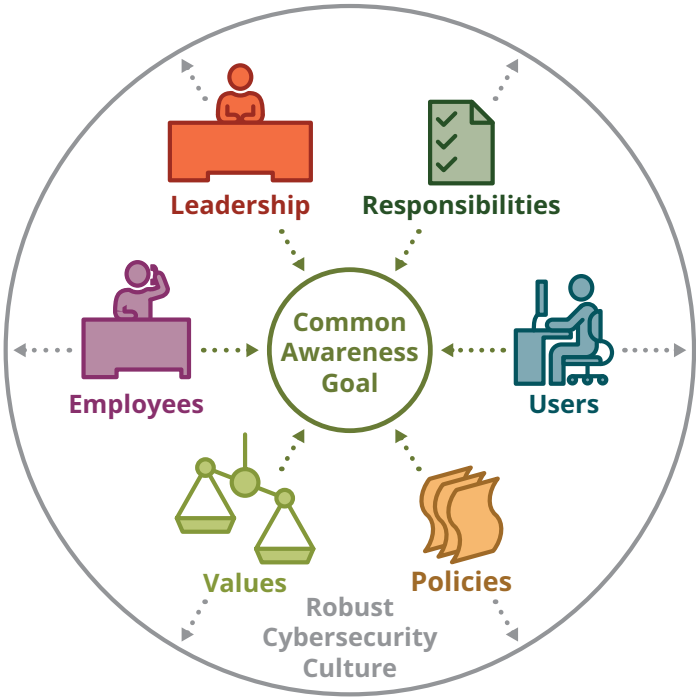
- The EU Directive on Security of Network and Information Systems (NIS Directive) requires a national strategy on network and information systems security, designation of a CSIRT, and cooperation at a national level.
- Health Insurance Portability and Accountability Act (HIPAA), addresses personal medical information protection.
- The Sarbanes Oxley (SOX) Public Company Accounting Reform and Investor Protection Act, addresses transparency and record retention of public corporations.
- The Gramm-Leach-Bliley Act (GLBA) requires financial institutions or companies that offer financial services to disclose their information sharing practices and how they safeguard consumer information.

CONSIDER LEGAL AND REGULATORY OBLIGATIONS

One of the main functions of a CSIRT is to contain and mitigate an incident as efficiently as possible, while ensuring the incident caused the least amount disruption to normal business operations. For CSIRTs and/or National CSIRTs specifically, the steps conducted during a security event or incident should consider any legal or regulatory obligations and must be within the scope of applicable laws and regulations. Therefore, the creation of an awareness program must take these into consideration; awareness program activities may focus on raising constituency awareness of the laws and regulations and/or how constituents should operate within the confines of these laws and regulations.

Cybersecurity Culture

Cybersecurity awareness programs introduce users to safe online practices and help them develop skills they will use both at work and in their personal lives. Successful awareness programs unite organizational leaders around a common awareness goal—protect the organization's information technology related assets and resources. By "buying in" to the security goals of the organization (and building an organizational culture with all employees and users responsible for cybersecurity) organizational leaders increase cybersecurity awareness and create a robust security culture. An organizational cybersecurity culture can be characterized as a facet of the broader organizational culture, which encourages employees and users to fulfill their responsibilities in alignment with the organization security policies.



The Business Case

Leadership buy-in is often a challenge. This may stem from budget constraints, lack of resources, lack of knowledge of basic cybersecurity principles, or other business priorities. For senior leadership to truly understand the value security brings to an organization and promote an effective cybersecurity culture, they must understand the role that security plays within the organization and on the continuity of its business. You may need a dedicated effort focused on educating senior leadership and presenting the business case for cybersecurity awareness. The business case may differ, depending on your organization, its mission, and its constituency. One common argument entails comparing the cost of recovering from a cybersecurity incident against the cost to develop a cybersecurity awareness program. Responding to and recovering from a cybersecurity incident can be extremely costly—which could divert significant funding, resources, and effort away from other priority tasks and mission sets. The business case might also include less quantitative metrics, such as harm to reputation or loss of trust by the constituency.

Budget

This consideration is a subset of the business case. It is important to understand funding and resources from the very beginning of any awareness program or campaign efforts. That enables you to adequately scope the program and determine how many activities (and what level) will be offered. Understanding and managing the budget may be challenging, but it is essential to ensuring the scope and success of a cybersecurity awareness program or campaign.

Designing a Cybersecurity Awareness Program

When designing an awareness program or campaign, it is important that the program supports the business needs of the organization and complements the organizational culture and IT infrastructure. These programs must be designed with the intention of supporting the organizational mission in alignment with the security needs of the organization or constituency. Furthermore, users should find the program relevant to their daily activities. As the cybersecurity awareness program is designed, it must complement the organization's or constituency's awareness, needs, and goals.

Identify Awareness Program Model

Responsibility for administering various aspects of a cybersecurity awareness program can be either centralized or distributed, depending on organizational structure and resources available. NIST SP 800-50 identifies three common approaches to designing, developing, and implementing a cybersecurity awareness program, as listed below:

Model 1 Centralized policy, strategy, and implementation

Model 2 Centralized policy and strategy, distributed implementation

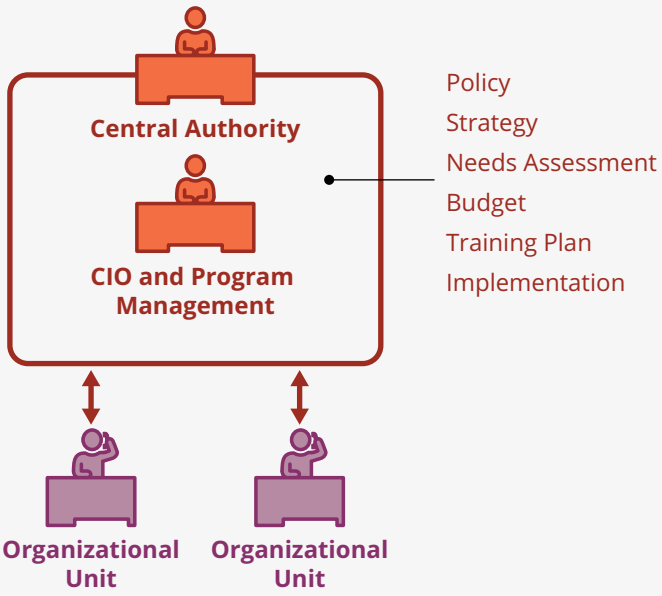
Model 3 Centralized policy, distributed strategy and implementation

All three models show a centralized policy. Responsibility on strategy and program implementation may be handed to subordinate entities depending on funding and resource availability, as summarized in the following models described in NIST 800-50.

PROGRAM OWNERSHIP

It is important for you to think through who will own the cybersecurity awareness program, how it will be promulgated throughout your organization, and who is the governing body. In some organizations, this responsibility may fall to the office of the CIO, the Compliance Office, or a Cybersecurity Program Management Office. By NIST guidelines, this governing body is called the "central authority." However, for all intents and purposes it is the governing body of any awareness program. In addition, NIST guidelines identify subordinate entities as "organizational units." These organizational units report to the governing body. For standardization purposes, we use the terms identified by NIST in the following models.

Centralized Program Management Model



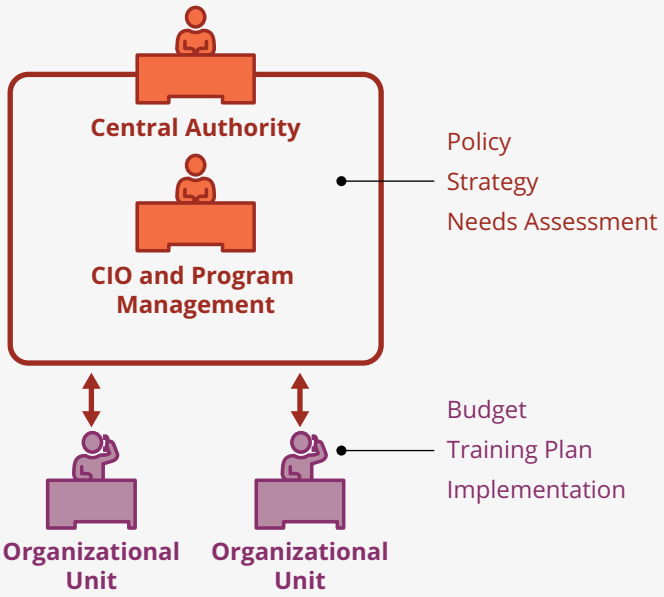
In the centralized program management model, the cybersecurity awareness policy, strategy, and implementation plans are centralized and managed by the central authority. This means that all directives regarding cybersecurity awareness strategy development, model planning, scheduling/implementation, and any coordination are conducted by the central authority.

Since the central authority is responsible for the development of the awareness and training strategy, it must conduct an awareness and training needs assessment. This needs assessment will assist in identifying existing gaps and deficiencies in training and specific needs of the organizational unit. Based on the findings from the needs assessment, the central authority will develop the strategy, plan, and any awareness materials needed for the awareness program.

In this model, the central authority communicates and guides the organizational units with (1) the parent organization's policies and directives regarding cybersecurity awareness and training, (2) the cybersecurity awareness strategy, materials, and (3) methods of implementing the cybersecurity awareness program. The central authority may request feedback from the organizational unit on the effectiveness of the awareness materials, the delivery methods, or the training itself. This feedback will allow the central authority to update materials as necessary in order to improve upon the cybersecurity awareness program.

PROS	CONS
A central authority governs all aspects of the cybersecurity awareness program.	Organizational unit input may be lacking.
It works well with structured and central management of IT functions.	Modifications to awareness program materials may be delayed due to central authority constraints.
Organizational units assist as necessary.	Modifications to awareness program materials are conducted by the central authority and may not reflect the accurate state, priorities, or issues at the organizational unit.

Partially Decentralized Program Management Model



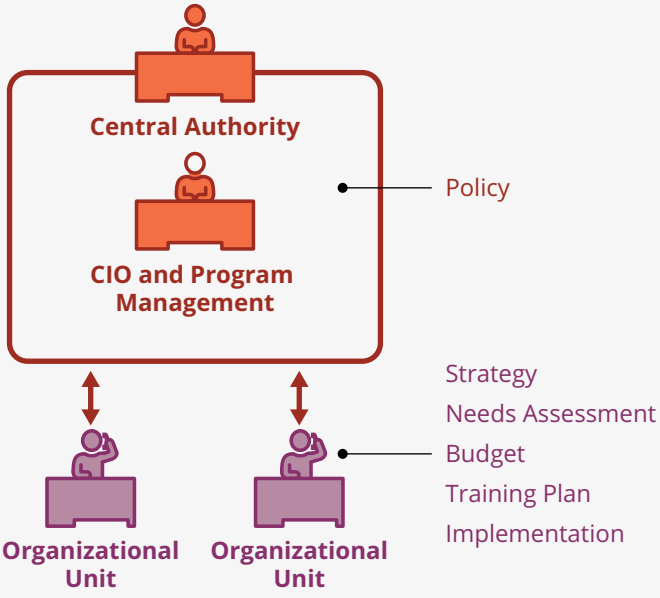
In a partially decentralized program model, both the cybersecurity awareness policy and the cybersecurity awareness strategy are prescribed by the central authority. However, awareness program implementation, material development, and scheduling are the responsibility of the organizational units.

In this model, the central authority communicates the cybersecurity awareness policy, the cybersecurity awareness program implementation strategy, and the overall budget allocation for each organizational unit. The central authority also conducts a needs assessment of the organizational unit, since this assessment helps guide the strategy for the awareness program. The central authority may provide guidance to the organizational unit in creating a cybersecurity awareness implementation plan; however, managing the budget and implementation are the responsibilities of the organizational unit. The implementation plan will also outline the best delivery method for the organizational unit's users or constituency.

In an oversight role, the central authority may request regular updates from the organizational units for items such as status of awareness program development, updates on implementation progress and material development, and financial expenditures. Once the cybersecurity awareness program has been implemented, the central authority may also request metrics as to the number of attendees at awareness training sessions, the number of people trained on specific topics, and the number of people who have yet to participate in the awareness activities. These metrics can assist the organization in determining the level of compliance and effectiveness of the organizational unit's awareness program implementation.

PROS	CONS
Split responsibilities between the central authority.	A lack of resources may impact awareness program creation.
It can be spread over wide geographical areas.	Resource constraints at the organizational unit may affect cybersecurity awareness material creation.
It is suited for organizations with diverse missions.	With the organizational unit responsible for implementation, this may require input from several teams, delaying implementation.

Fully Decentralized Program Management Model



In the fully decentralized program model, the central authority communicates the organization's overarching cybersecurity awareness policy, and expectations regarding program implementation and management. In this model, it is the organizational unit's responsibility to budget for, create, implement, and manage the cybersecurity awareness program. Directives and expectations are provided by the central authority to the organizational units.

In this model, the needs assessment is conducted by each organizational unit, as the organizational units themselves determine the best strategy for the cybersecurity awareness program. Based on the assessment findings, the organizational units then develop the appropriate training plans, awareness materials, and delivery methods best suited for their needs. The central authority may request regular updates on the status of awareness program expenses, needs assessment outcomes, program implementation, and the results of trainings conducted to date.

PROS	CONS
The organizational unit has complete control of the cybersecurity awareness campaign.	Awareness program development is the responsibility of the organizational unit.
It is ideal for large organizations.	Resource constraints may impact awareness program development and implementation.
It allows organizational unit autonomy.	It may cause a lack of standardization across distributed organizational units.

Conduct a Needs Assessment to Determine the Baseline
Establish a baseline of current status before implementing an awareness program. This will help you fully understand the security needs of your organization or constituency. This baseline will help determine the focus areas or particular topics to be addressed throughout an awareness program or campaign.

A baseline will assist in determining key metrics which can be later used to measure the performance of an awareness program or campaign. It is necessary to evaluate a program or campaign so that the organization can understand the effectiveness of the awareness program overall and make changes where necessary—leading to program success. Metrics should be relevant to the target audience and program, thus all metrics cannot be universally applied to all groups as needs will vary. See the Post-Implementation section for more on metrics.

Regardless of the model selected, a needs assessment must be conducted in order to determine this baseline. The needs assessment is a process that can assist in determining where your organization stands with cybersecurity awareness, identify gaps in training and understanding, and as a result determine your organization's cybersecurity awareness needs. It is important to address the specific needs of different roles within the organization and how they may differ. Likewise, it is important to address the needs of a particular constituency or subset of the general public, if you are developing an awareness campaign for them. See Table 3 for an example of training needs.

Table 3

EXECUTIVE MANAGEMENT	Requires a clear understanding of the operating environment, including policy, legislation, regulatory and security requirements, as well as their roles in promoting a culture of cybersecurity and achieving compliance with mandated requirements.
SECURITY PERSONNEL	Act as subject matter experts (SMEs) and must have clear understanding of security policies and accepted best practices.
SYSTEMS OWNERS	Require an understanding of the systems they own, and the policies that impact how security controls are implemented on the systems they manage.
SYSTEMS ADMINISTRATORS	Require a high level of technical knowledge and authority over systems support operations.
MANAGERS AND USERS	Require a high degree of cybersecurity awareness, to include organizational security controls, acceptable use policy, and rules of behavior for the systems on which they conduct business operations.

Training Needs Throughout an Organization (adapted from: **https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf***–pp16.)*

Determine Sources and Methods of a Needs Assessment
There are many sources within the organization that can be leveraged to aid in the identification of the cybersecurity awareness needs. Additionally, NIST 800-50 provides various methods that can be used to collect this information, to include, but not limited to the following:

- interviews with key groups within the organization
- organizational surveys
- review of assessment materials and methods, and current training materials
- review of security plans for general support systems
- review of findings from any governing and oversight bodies
- analysis of security incidents and events
- review of any technical and infrastructure changes
- study of current events and trends identified across the security landscape
- any metrics obtained from previous cybersecurity awareness activities

Develop Awareness Program Strategy
The needs assessment results can be used to develop a strategy for the development, implementation, and maintenance of a cybersecurity awareness program. The strategy should address the foundational items discussed thus far, as well as others provided by NIST 800-50, such as

- any national, regulatory, or local policy requiring cybersecurity awareness activities to be completed
- the scope of the cybersecurity awareness program
- roles and responsibilities of those who should design, develop, and implement the cybersecurity awareness program
- the goals to be accomplished for each aspect of the program
  - Learning objectives
  - topics to be addressed
  - material updates and evaluation of material frequency
  - cybersecurity awareness activity frequency
- Target audiences and the applicability of the program to specific audiences
  - C-level, management, staff contractors, training coordinators, etc.
  - the general public
    - further categorize, as required (i.e., at-risk audiences such as children or the elderly)

Develop Awareness Program Plan and Identify/Prioritize Awareness Program Components

When the cybersecurity awareness strategy is complete and agreed on, establishing the awareness program plan and implementation schedule will help set the program in motion. This plan lays out how the strategy will be executed. Program implementation may need to be phased if there are budget or resource availability constraints. It is then important to decide what factors need to be taken into consideration when determining which initiatives to schedule first and any particular sequence that should be applied, depending on scope, timeframe, audience and/or budget. Some key factors to consider include

- availability of materials and resources
- role and organizational impact
- status of current compliance/baseline
- critical project dependencies
- funding, if required

Develop Awareness Program Materials

Before developing tailored awareness material, it is critical that you determine the audience and the topics that will resonate with that particular group. While some material may be well-suited for the general population, there are particular categories, such as age, education, and technical skills, that must be considered when developing content. The key to effective user awareness is understanding the demographics of your constituency and tailoring the most useful of these resources to your audience. The message should be *relatable, realistic, and memorable* for that particular demographic and topic. Keep your message *simple, direct, and engaging.*

Once you determine the audience, topics, and goals for an awareness building program or campaign, you can collect resources and solicit ideas for content. Maintaining a repository of reputable sources for material development may also aid in the amount of effort, time, and resources required to develop awareness and training material. Cybersecurity awareness transcends borders, sectors, and organizations—there is a significant amount of publicly available materials that can be referenced, used, and tailored to different organizations and audiences. See the Supplemental Materials section for a list of publicly available awareness building resources.

After collecting relevant materials and engaging in brainstorming exercises, you can begin to organize and tailor the information for specific needs. Always remember your desired audience and messaging when developing content. You should also consider the scale of various awareness building mechanisms and needs—whether that is a fully developed awareness building program, an awareness week or month, or a simple and fun awareness building poster.

Identify Best Delivery Methods

Cybersecurity awareness programs are implemented to make users aware of security issues and concepts. The success of the cybersecurity awareness program relies on how it is delivered to the user. Cybersecurity awareness program implementers have various delivery techniques at their disposal. Delivery methods do not necessarily have to be, and should not always be, in a classroom or formal setting. Delivery methods, like many other components of the program, should be determined by the scope, audience, and intended goals of the program. In all cases, delivery methods should be engaging, eliciting participation and encouraging an effective learning environment.

CONVENTIONAL METHODS: ELECTRONIC OR PAPER-BASED PRODUCTS	Prepare attention-grabbing emails or paper-based products such as handouts and leaflets with cybersecurity awareness tips and tricks, including reminders on password complexity or other security related topics relevant to the organization.
	Display posters showcasing security-related messages in public areas (use to remind users of time-sensitive issues such as completing mandatory training or upcoming changes to security procedures). Note, though, that users may walk by and overlook the message, or become desensitized to this method.
	Paper and electronic newsletters are periodic; use them to reinforce the cybersecurity awareness program; one advantage of newsletters: they can convey several messages at the same time. However, though newsletters may appeal to a specific group, there is no guarantee that a user has read the newsletter.
INSTRUCTOR-LED DELIVERY	These can be formal or informal classroom or seminar type of workshops facilitated by internal or external security experts. The advantage of instructor-led delivery is that the instructor is able to perceive non-verbal cues from the participants and determine how best to modify the instruction.

ONLINE DELIVERY METHODS	This method is well suited to communicating with users in different geographical areas. Online delivery can include email broadcasting, real-time and asynchronous discussion, content uploading, blogs, video, multimedia content distribution, and other techniques.
VIDEO-BASED DELIVERY METHODS	Many organizations use video-based content delivery as part of their cybersecurity awareness program. There is no need for an instructor and users set their own pace. Video-based delivery methods can be coupled with reading exercises and quizzes to give the user a more effective experience.
GAME-BASED DELIVERY METHODS	Game delivery methods are interactive and offer an effective alternative to more traditional methods of content delivery. These games are typically computer based and combine graphics with training concepts to create interactive learning environments.
SIMULATION-BASED DELIVERY METHODS	Simulation-based delivery methods are highly interactive and are presented as legitimate activity. This type of delivery is often used in phishing exercises to test users' vulnerabilities to phishing techniques, and is often followed up by training, should a user fall victim to the simulated phishing email. Simulated phishing emails often reflect current events, or claim to involve the user at a personal level to entice the user into performing a specific action.

(Adapted from: **https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf** *– pp34.)*

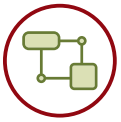
Conducting Your Cybersecurity Awareness Program

Once the strategy and key components of a cybersecurity awareness program or campaign have been finalized (for example, the needs assessment has been conducted, the awareness campaign strategy is developed, the security awareness program plan is completed, and the materials have been designed), you can begin implementing your cybersecurity awareness program or campaign. Considerations for implementation include communication and socialization of the program, delivering cybersecurity awareness materials and activities, developing and tracking measures of success, and continually revisiting the effectiveness of the program. Below is a summary of components and steps for the development of a cybersecurity awareness program.

Cybersecurity Awareness Program Components

Understand policy/regulatory constraints/ considerations.

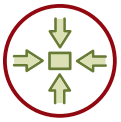
Determine roles and responsibilities.



Determine model.

Conduct a needs assessment.

Develop and document strategy.



Design awareness program plan based upon the models, needs assessment gaps, and strategy

Determine metrics

Develop awareness material for the program.

Communicate the program.

Conduct/execute awareness program.

Conduct post-implementation activities.

Communicate the Awareness Program

To gain support from the users and necessary resources, the cybersecurity awareness program or campaign must be socialized. The components of the program also must be clearly communicated. These communications will outline the *expectations* as well as the expected *results* of the program and the value provided to users and/or the constituency.

Conduct Awareness Activities and Execute Awareness Program

Cybersecurity awareness program implementers use various techniques to disseminate information across the organization. The choice is based on organizational culture and needs. How the message gets out depends on the available resources, topics, and the complexity of the message. In all cases, ensure ease of access to awareness program materials; for example, an intranet page with access to awareness materials, training links, and other activities can serve as one-stop shopping for all program updates and information.

Developing Metrics and Monitoring Compliance

Using metrics and objective measurement is important for monitoring performance, considering that the cybersecurity threat landscape is constantly changing. By implementing a comprehensive cybersecurity metrics program, organizations can achieve several goals—including decision making, visibility, and the ability to evaluate your cybersecurity awareness program against industry and regulatory benchmarks. Metrics can be adapted to suit the needs of any target audience, and can be used to improve on cybersecurity policies and cyber security awareness programs.

When implementing metrics as part of an awareness program, a key task is to identify what metrics to measure, along with where and how to obtain the raw data. Defining metrics can be difficult, and when developing metrics, organizational considerations should be applied as to what information is collected, how it is collected, and how it is stored. Metrics collected and reported should follow something similar to the *SMART* goal objectives:

- **Specific—**Targeted to the area being measured, not a result or an assumption.
- **Measurable—**Data collected is accurate, complete, and reliable.
- **Actionable—**Data is easy to understand and actionable.
- **Relevant—**Measure what is important in the data.
- **Timely—**Data is available when needed.

When measuring specific security areas, organizations may want to address:

- Vulnerability data, such as internal or external vulnerabilities, or vulnerabilities by criticality, severity or priority
- Cybersecurity policy and compliance adherence, such as exception, configuration, and regulatory compliance tracking
- Training and awareness, such as training completion and tracking
- Monitoring and response, such as number of events/alerts collected and number of events/incidents being reported by constituents

For broader metrics associated with an awareness program or campaign, tracked metrics may also include, but are not limited to

- website traffic
- downloads of available cybersecurity materials or information provided for constituents
- media coverage
- social media activity

Post Program Activities

To remain relevant, the cybersecurity awareness program should remain current with advancements in technology, changes to the organization or IT infrastructure, shifts in the organizational mission, changes to cybersecurity policies, and most importantly, be continually updated to reflect the changing threat and cyber landscape. The cybersecurity awareness strategy should include mechanisms to ensure the program continues to be not only relevant to the organization but also remains compliant. In the post-implementation phase as described by NIST 800-50, the cybersecurity awareness program should aim at continuous improvement and offering users the latest and most current information available.

Lessons Learned

Feedback from participants and lessons learned from the roll out of an awareness program can help improve the quality of the program. By incorporating feedback, findings, and lessons learned, the program can improve long term. In larger organizations where organizational units are responsible for implementing their own cybersecurity awareness programs, sharing lessons learned, experiences, ideas, and processes that work would benefit the organization as a whole.

Regular Audit and Program Maintenance

You must determine how often to review and audit your cybersecurity awareness program, as well as identify who will conduct a regular audit. At a minimum, annual reviews are preferred. They will incorporate lessons learned, activities to be adjusted based upon the evolving threat environment, and any changes or adjustments to roles and responsibilities of the program.

Additionally, an organization may choose to conduct an audit or assessment following certain awareness program activities. There are many different types of audits or assessments that can be provided, including a review of security policies, scanning, penetration testing, and others. Depending on the type of audit or assessment, it could also be outsourced to a third-party contractor or managed security service provider with the appropriate expertise in conducting audits and assessments. Audits and assessments are outside of the scope of this document. However, it is important to continue

to think about the various methods and mechanisms for program audit and maintenance in order to maximize long-term program effectiveness.

Monitoring compliance will also play a role in the measurement of a cybersecurity awareness program's success. Cybersecurity awareness compliance will not only be necessary at the organizational level but may also be required by government mandate or regulation based on industry or sector. A tool should be in place to monitor compliance and program effectiveness. NIST 800-50 suggests an automated tracking system should be implemented and designed to capture program activity information to include awareness activities, dates, audience, size, and sources, to name a few. This data should be captured, analyzed, and reported at regular intervals in order to ensure compliance is monitored and awareness program goals and objectives are continually being met.

MEASURING THE SUCCESS OF PHISHING AWARENESS CAMPAIGNS

Many organizations implement phishing awareness campaigns in order to give users the tools necessary to recognize phishing scams. There are many factors to be considered when determining the effectiveness of a phishing awareness campaign, and it is very common for organizations to highlight their "click rate." However, when determining metrics, a baseline of understanding must be established to identify where individuals score under current working conditions. After a campaign is conducted, individuals can then be reassessed to determine the effectiveness of the campaign. Possible metrics that organizations can utilize to determine effectiveness of phishing awareness campaigns include the following:

1. **Successful phishing attempts—**The amount received by a user in six months to a year
   Are users getting closer to or further from becoming knowledgeable in identifying phishing techniques? An effective phishing awareness campaign would yield results of decreased successful phishing attempts.
2. **Phishing emails reported—**The amount received by the security team in six months to a year
   An effective phishing awareness campaign may yield an increase in phishing emails reported.
3. **Results of a simulated phishing campaign**
   How well did users avoid becoming victims?

Cybersecurity Awareness Campaign Considerations

While a cybersecurity awareness campaign implies a different scope than a cybersecurity awareness program, much of the design and components of a cybersecurity awareness program also apply to a campaign. It is important to refer back to the How to Use this Document section, and continue to answer the following questions when developing an awareness campaign:

- Who are your constituents?
- Who is your audience?
- What are the specific goals and objectives of awareness building?
- What is the scope of this specific awareness building effort?

The questions must be answered before starting effective and meaningful awareness campaigns. Developing an awareness campaign is very similar to developing an awareness building program. Since campaigns may be broader in scope (i.e., for the general public) or potentially narrower in focus (developed around a particular topic or focus area), it may not be feasible to conduct an awareness needs assessment. However, awareness campaign topics should be driven by the audience and any available knowledge or data regarding common cybersecurity *challenges.*

For example, national CSIRTs are in a unique position to collect data on common cybersecurity incidents and threats, and this information should be used to identify challenge areas that may determine particular campaign topics or focus areas. A campaign strategy should also be developed in a similar fashion as an awareness building program. The audience, scope, and roles and responsibilities should be determined in advance of the planning stages.

Communication and Marketing

Careful consideration should be given to the communication and marketing of the campaign. An awareness campaign can be more effective with

- a single, unified message
- fun, engaging, and interactive material
- real-world applicability and relatability
- content tailored to specific audiences

Advertise the campaign before it begins; expand to maximum reach and interest by all possible constituents and audiences. Coordinate with the communications or public relations department, if applicable; it can aid in the messaging, branding, and reach of a campaign, and allow the cybersecurity team to focus on the content and implementation of the campaign itself.

EXAMPLES OF CYBERSECURITY AWARENESS CAMPAIGNS

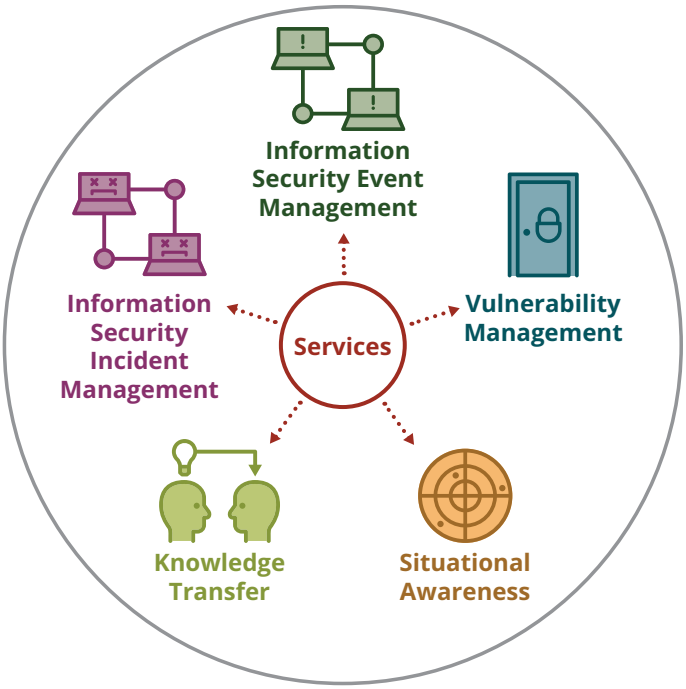
For national CSIRTs or other CSIRTs, cybersecurity awareness campaigns are often conducted during National Cybersecurity Awareness Month. This effort is typically a dedicated campaign focused on particular topics and audiences, including child online safety, data protection and privacy, user awareness, or other similar subjects. Effective campaigns are relatable, applicable, and easy to understand. Not only do they raise cybersecurity awareness, but they should also raise awareness of the CSIRTs themselves and their missions and purposes. The Organization of American States (OAS) compiled a comprehensive *Cybersecurity Awareness Campaign Toolkit* that can be leveraged by any CSIRT interested in developing a campaign (see the Supplemental Materials and Resources sections).

Awareness as a Service

Cybersecurity centers, SOCs, or CSIRTs may be more focused on cybersecurity awareness campaigns, or awareness as a service to its constituents, rather than on building organizational awareness building programs. While incident response teams can perform many different services, awareness may or may not be one of these core services.

The FIRST CSIRT Services Framework describes services and functions of incident response teams within a high-level framework to assist in community-wide standardization and the selection and establishment of a team's services portfolio. It is important to note that teams are not expected to provide all services; you should select your services based on your mission, constituents, resources, and capacity. The structure of the framework is based on four elements: service areas, services, functions, and sub-functions. When you develop an awareness program or support service, refer to the CSIRT Services Framework to help your organization with goal setting, understanding desired outcomes, and implementation planning.

The FIRST CSIRT Services Framework identifies five service areas, as outlined in the image to the right. The Knowledge Transfer service area specifically addresses awareness building. We will summarize the Knowledge Transfer service area in order to highlight key purposes and outcomes that should be considered when building out these services. If these services are not a critical part of your mission, the information may still assist in designing particular pieces of an awareness program or campaign.



FIRST CSIRT Services Framework Service Areas

Service Area: Knowledge Transfer

Incident response teams are in a unique position to create best practices that help users and constituents detect, prevent, and respond to security incidents. By transferring this knowledge to constituencies, incident response teams have the capability to improve overall cybersecurity posture. The following categories are considered services of the Knowledge Transfer service area and are excerpted from the FIRST CSIRT Services Framework for reference.

Awareness Building

Functions within the Awareness Building Service build on communication with your constituency, experts, trusted partners, and other stakeholders to raise the collective understanding and awareness of identified threats and the actions that can be taken to mitigate the vulnerabilities and risks posed by these threats.

Purpose Increase the security posture of the constituency and help its members to detect, prevent, and recover from incidents; ensure that constituents are better prepared and educated.

Description This service includes working with the constituency, experts, and trusted partners to raise the collective understanding of threats and actions that can be taken to prevent or mitigate the risks posed by these threats.

Outcome The constituency is provided with the necessary awareness of security and operational best practices and steps to take to detect, prevent and mitigate threats and malicious activity.

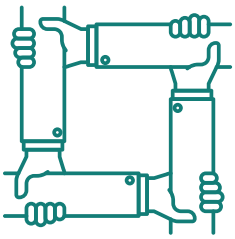
Training and Education Service

By establishing a training and education program, you can establish relationships and improve the overall cybersecurity landscape for all its constituents and stakeholders, to include the ability to prevent future incidents from happening.

Purpose Provide training and education to a constituency (which may include organizational staff) on topics related to cybersecurity, information assurance and incident management.

Description A training and education program can help the team establish relationships and improve the overall cybersecurity posture of its constituency, including the ability to prevent future incidents from happening. Such a program can help maintain user awareness, constituency understanding of the changing landscape and threats, facilitation of information exchanges, and training on tools, processes and procedures related to security and incident management.

Outcome A consistent training and education program is provided that enables your constituency to appropriately acquire methods to detect, prevent or respond to threats, tools and practices to help protect critical assets, and understand incident management processes and how to get assistance.



Exercises Service

By conducting exercises in collaboration with the constituency and teams, you can better assess the effectiveness and efficiency of existing cybersecurity and functions. This service can be offered to constituents and teams that support the design, execution, and evaluation of cybersecurity exercises used to train or evaluate constituent capabilities and the overall stakeholder community.

Purpose Conduct exercises to assess and improve the effectiveness and efficiency of cybersecurity services and functions.

Description Services are offered by the organization to constituents that support the design, execution, and evaluation of cyber exercises intended to train and/or evaluate the capabilities of individual constituents and the stakeholder community as a whole, including communications capabilities.

Outcome The effectiveness and efficiency of cybersecurity services and functions is improved and opportunities for further improvements are identified. Requirements analysis, format and environment development, scenario development, exercise execution, and exercise outcome reviews are parts of the implementation of this service.

Technical and Policy Advisory Service

By providing this service, you can ensure that constituents' policies and procedures include incident management considerations. This service can be provided to your constituencies and key stakeholders. Formalizing and accepting policies and procedures further legitimizes the services you can offer.

Purpose Ensure the constituency's policies and procedures include incident management considerations and enable the constituency to better manage risks and threats.

Description Support the constituency and key stakeholders in activities related to risk management and business continuity, providing technical advice as needed and contributing to the creation and implementation of the constituency's policies. Policies are also important in legitimizing the services of a team.

Outcome A constituency is enabled to make organizational decisions based on operational security best practices, while also understanding the need of including incident management teams as trusted advisors in business decisions where appropriate.

Supplemental Materials

FIRST CSIRT Services Framework

Resources for Building Cybersecurity Awareness brochure

Your feedback is welcome.

If you have feedback you'd like to give on this publication, we would love to hear it. Please send an email to **security-operations@cert.org**

Resources

FIRST CSIRT Services Framework v2.1

first.org/standards/frameworks/csirts/csirt_ services_ framework_v2.1

NIST Special Publication 800-50: *Building an Information Technology Security Awareness and Training Program*

csrc.nist.gov/publications/detail/sp/800-50/final

NIST Special Publication 800-16: *Information Technology Security Training Requirements: A Role-and Performance-Based Model*

csrc.nist.gov/publications/detail/sp/800-16/final

OAS Cyber Security Awareness Campaign Toolkit

sites.oas.org/cyber/Documents/2015%20OAS%20-%20 Cyber%20Security%20Awareness%20Campaign%20 Toolkit%20(English).pdf

Measuring An Information Security Awareness Program

clutejournals.com/index.php/RBIS/article/view/5398/5483

Persona-Centred Information Security Awareness

sciencedirect.com/science/article/pii/S0167404817301566

From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization

dl.acm.org/doi/abs/10.1145/3130515.3130519

7 Elements of a Successful Security Awareness Program

csoonline.com/article/2133408/networksecurity-the-7-elements-of-a-successful-securityawareness-program.html

User Preference of Cyber Security Awareness Delivery Methods

tandfonline.com/doi/full/10.1080/0144929x.2012.708787

Digital Guardian "Security and Analytics Experts Share the Most Important Cybersecurity Metrics and KPIs"

digitalguardian.com/blog/what-are-the-most-important-cybersecurity-metrics-kpis

For More Information on Implementing a Cybersecurity Awareness Program

SANS Security Awareness Planning Toolkit and Resources

sans.org/security-awareness-training/resources/ securityawareness-planning-toolkit

sans.org/security-awareness-training/resources

Center for Internet Security (CIS) Implement a Security Awareness and Training Program

cisecurity.org/controls/implement-a-security-awarenessand-training-program/

PCI Security Standards Council Best Practices for Implementing a Security Awareness Program

pcisecuritystandards.org/documents/PCI_DSS_V1.0_ Best_Practices_for_Implementing_Security_Awareness_ Program.pdf

About the CERT Division

The CERT® Division of Carnegie Mellon University's Software Engineering Institute studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu