Table of Contents

[README 1](#_Toc69828527)

[PROJECT PLAN 3](#_Toc69828528)

[Executive Summary 3](#_Toc69828529)

[Engagement/Training Strategies 4](#_Toc69828530)

[Overall Strategy 4](#_Toc69828531)

[Cultivating an Effective Awareness Culture 4](#_Toc69828532)

[Network Assurance Department 5](#_Toc69828533)

[Information Technology (IT) Department 5](#_Toc69828534)

[Infrastructure Operations Department 5](#_Toc69828535)

[Personnel Administration Department 5](#_Toc69828536)

[Ambassador Engagement 5](#_Toc69828537)

[Training Methods and Modalities 6](#_Toc69828538)

[Mandated Annual Training 6](#_Toc69828539)

[Reinforcement via Quarterly Brown-Bag Sessions 6](#_Toc69828540)

[Phishing and Physical Security Assessments 6](#_Toc69828541)

[Branding 7](#_Toc69828542)

[Newsletters 7](#_Toc69828543)

[Metrics 7](#_Toc69828544)

[Phishing Click Rate 7](#_Toc69828545)

[Unauthorized Media Usage 8](#_Toc69828546)

[Physical Security 8](#_Toc69828547)

[APPENDIX 9](#_Toc69828548)

[Learning Objectives 9](#_Toc69828549)

[Target Audience 9](#_Toc69828550)

[Goal / Outcome 9](#_Toc69828551)

[Background 9](#_Toc69828552)

[Learning Objectives 9](#_Toc69828553)

# Executive Summary

A core aspect of ACME Central’s mission is to defend the Department of Defense (DOD) Information Network in the Central Region area of responsibility (AOR). This defense ensures the security of sensitive information that has a direct impact on the lives of warfighters overseas. To secure this information we must train the staff at ACME Central to understand the risks and to be aware of the steps they must take to protect our information networks from both malicious and non-malicious cyber threats. The DOD invests hundreds of millions of dollars every year on the most advanced cyber security systems to defend our networks. However, many of these systems can be beaten by targeting the weakest link in the chain ---the human. To ensure the integrity of our nation’s most sensitive information and to protect the lives of the men and women overseas, a security awareness program must ensure ACME Central’s staff is aware of the human risk and the steps they can take to mitigate this risk. While ACME Central has an existing security awareness plan, it is broad in scope and is designed for quick completion rather than lasting impact on the security awareness culture.

COVID-19 has seen ACME Central transition to a 75% remote workforce. This dramatic change has contributed to a significant rise in security incidents involving employees working from home. This negative trend can partly be attributed to complacency and lack of understanding of secure practices. ACME Central’s current security awareness program meets the mandated requirements and allows staff to quickly confirm they completed their training without any real measure of understanding or impact. The intent of this improved security awareness plan is to create a program the staff want to be a part of by focusing on positive emotional engagement.

This awareness program will address these issues by delivering training tailored to the mission at ACME Central. Metrics will be tracked to ensure the program is delivering positive change and to identify key areas that must be addressed. A security awareness program should not only meet the mandated requirements but should effectively regulate human risk by promoting appropriate workforce behaviors through emotional engagement and regular reinforcement. To improve our existing program the Cyber Security Fusion Team will administer quarterly brown-bag training to reinforce important security awareness topics. Training completion and understanding will be confirmed via multiple choice tests and interactive simulations. Metrics of security incidents and training results will be tracked and reinforcement training will be adjusted based on trending data. ACME Central’s Physical Security and Cyber Security Teams will conduct regular assessments to test the effectiveness of the awareness program.

The overall goal of the improved security awareness program is to limit human risk by positively changing the organization’s culture to be more mindful of secure practices. Learning objectives will be reinforced and tested to ensure staff are aware of proper procedures and aren’t becoming complacent. This program may ultimately save ACME Central money and lives by investing in the “human sensor” rather than relying on reactionary incident response as a result of poor security practices and cyber hygiene.

# Engagement/Training Strategies

## Overall Strategy

ACME Central’s current security awareness program meets the mandated requirements and provides the staff with a resource that offers some awareness of information security. However, with an AOR containing one of the largest numbers of deployed U.S. warfighters worldwide, ACME Central must not only meet the minimum security requirements, but rather strive to set the highest standard of security awareness. The following training and engagement strategies are the methods in which this security awareness program will evolve the workplace culture to be more security minded. The goal is for the staff to become emotionally invested in security by connecting them with the real life impact information security has on the warfighter they are responsible for supporting. It is important to note that this training and engagement strategy will supplement the existing security program, not replace it. Both training strategies will be combined to ensure positive cultural change is made and mandated requirements are still being met.

## Cultivating an Effective Awareness Culture

ACME Central is primarily made up of active duty service members and prior service civilians, both contractors and government employees. This makeup of veteran staff members provides the organization with a sense of camaraderie even among new hires. The organization is very process driven and values direct human interaction making it primarily a conservative workplace culture. While ACME Central may have a pre-dominantly conservative culture there are several sub-cultures. These sub-cultures are different for those who are deployed overseas as well as from department to department (e.g., Network Assurance, Infrastructure Operations). The goal of this security program is not to change the workplace culture within ACME Central but to embed security into its existing culture and sub-cultures.

Each sub-culture within ACME Central will benefit from having a variety of delivery methods to choose from to reach the individuals within each department or work location. ACME Central is an international organization but the overseas personnel are primarily made up of temporarily deployed U.S. citizens that were once service members. This means they share a similar cultural makeup as the stateside employees. Some departments are made up of mixed demographics while others are primarily made up of one demographic. The security awareness program will take a mostly conservative approach but will offer alternate forms of communication that may be selected by each department’s Security Awareness Ambassador.

Below are each of the major departments within ACME Central along with their majority demographic and a short description of their sub-culture. Each department will require unique methods of engagement to better embed security awareness into their sub-culture.

### Network Assurance Department

Primarily made up of contractors, members of this department are mostly among the millennial generation. They’ve typically been in the cyber security field for 5 or more years. Described as introverted skeptics, this department is likely to include the most individuals with the “Curse of Knowledge” as they are required to be experts in the cyber security field. These individuals value training opportunities that offer some sort of technical skill development. They likely prefer media-centric online training or in-person training but only if the presenter is regarded as having strong technical knowledge.

### Information Technology (IT) Department

Trendy and media savvy, members of this department are a mixture of Gen Z or millennials and have typically been in their respective work field for 5 or less years. Many individuals in this department value security and want to learn more to advance their careers. Like the Network Assurance department, the IT department prefers media-centric online training or in-person training by a presenter with strong technical knowledge.

### Infrastructure Operations Department

Hierarchy-oriented and extroverted, members of this department are mostly Baby Boomers with a small number of Gen X and make up a majority of the ACME Central workforce. Average time in their work field is 15 or more years. This is the most conservative sub-culture that prefer in-person training by one of their peers with written material as a supplement. This department responds well to competition among their peers making them very responsive to the trends of their department’s security awareness metrics.

### Personnel Administration Department

Mostly made up of Gen X and millennials, the Personnel Administration department consists of diverse multitaskers who have a wide variety of job experience from new-hire to 10+ years in the field. They likely prefer media-centric online training or in-person training. This is the smallest department with the least technical staff but are typically very enthusiastic and curious about other departments’ job roles.

## Ambassador Engagement

Department Chiefs within ACME Central will each appoint a Security Ambassador. The Ambassador role is established to provide each department a representative that understands their sub-culture and may best select the most effective communication method for their team. Ambassadors will relay security related questions to the appropriate authority and pass relevant and timely information on security related issues and events to their local security office. Ambassadors will be each department’s familiar face that will deliver reminders and track security awareness training for their own department. As a liaison between the cyber security team and their respective department, Ambassadors must have an interest in information security but are not required to be technical.

## Training Methods and Modalities

### Mandated Annual Training

ACME Central’s existing security awareness program offers an interactive training platform that is accessible online. This existing program fulfills the DOD mandated annual and new hire training requirements. Although this training meets the minimum requirements of the DOD, this single training platform does not meet the cultural and operational requirements of each unique department within ACME Central. The mandated program also does not test the user on their understanding of the main learning objectives or include any refresher training. Under our new security awareness program, this interactive training will continue to be taken annually with an added quiz and simulation exercise. In addition to this, the new program will add quarterly brown-bag sessions, newsletters, and security assessments.

### Reinforcement via Quarterly Brown-Bag Sessions

Results from the annual training and feedback from the phishing and physical security assessments will be used to determine the topics for the quarterly brown-bag sessions. These sessions will be delivered by a local Senior Cyber Security Fusion Analyst with the assistance of the local department Security Ambassador. These sessions will be delivered in-person, recorded for later playback, and streamed live over video conferencing for remote workers to attend. Meeting notes and the presentations will be saved as video and text files for distribution to the department and for later reference. The chosen topics for these brown-bag sessions will include examples from recent cyber security news and understanding of how the highlighted security awareness topics relates to it. Emphasis will also be made on any positive impacts information security has had on the organization and the supported warfighters by providing overviews of performance and security related metrics. Each department will host their own brown-bag sessions tailored to their unique user group and sub-culture listed above.

### Phishing and Physical Security Assessments

The ACME Central Cyber Security Team will begin conducting routine phishing simulations to help track the effectiveness of the program. ACME Central Physical Security Team will also conduct regular assessments. These assessments have little to no cost and can be conducted regularly to assess the staff. Phishing simulations are quantifiable and actionable. Clicks on phishing links will be tracked and prompt the user to undergo supplemental security awareness training that will consist of the phishing email modules found in the existing online DOD interactive training platform. Consistent clicks by staff can identify vulnerable users or departments and help fine tune training as well as other security measures. Physical security will be assessed by having someone sit outside of the facility at a time of heavy foot traffic (e.g. early morning, lunch, end of day) and record the number of personnel that do not conceal their access badge or allow tailgating into the secure facility. Staff members caught doing this will be tracked and given feedback. Repeat offenders will undergo remedial training.

### Branding

The branding of the training materials and newsletters will follow ACME’s mandated guidelines. The main theme of the program will be supporting the warfighter to help defend against a common adversary. This theme reinforces the emotional tie staff will build with information security and the lives of U.S. citizens overseas. The importance of network integrity will be expressed through real life examples of actions and consequences of privileged individuals’ failure to follow the processes and procedures outlined in the security awareness program. The overall tone of the training and newsletters will be serious and conservative as to follow the military-based culture of the DOD.

### Newsletters

Currently, the Cyber Security Fusion Team at ACME Central creates a weekly newsletter aimed at informing the intelligence and cyber security communities of new cyber security relevant events in the news as they relate to ACME Central. This new security program would include a version of this product that is non-technical and aimed at informing the broader ACME Central workforce. This weekly security awareness newsletter would be a short, one page email that includes security awareness reminders and updates of recent events and how they relate to security awareness in the ACME Central AOR. As a similar product is already being produced, it would be low impact to create an additional simplified version to distribute to the remainder of ACME Central.

# Metrics

Metrics are key to ensuring our security awareness program is effectively embedding security awareness into ACME Central’s culture. The best way to measure the change in human behavior is to track various impact metrics. These metrics can then be used to improve the program’s training and learning objectives by focusing in on areas that need improvement and reducing time spent on areas where the organization is doing well. Three impact metrics have been selected initially based on historical data. These metrics will be reevaluated annually to ensure we are getting a complete picture of the organization’s behavior change.

## Phishing Click Rate

Phishing emails are one of the most popular attack vectors for both nation state actors and cyber criminals. The Cyber Security Team at ACME Central will conduct monthly phishing assessments on a randomly selected group of users and record whether users report, delete, ignore, or interact with links or attachments within these emails. Repeat victims of these phishing emails will be put on a watch list and assessed more often. Clicks on these phishing links will require the user to undergo supplemental security awareness training. This metric can identify vulnerable users or departments and help fine tune training as well as other security measures. Over time this metric should decrease as behaviors change. Metrics will be measured monthly by the Cyber Security Team and presented quarterly to an advisory committee.

## Unauthorized Media Usage

The ACME Central Cyber Security Team will use the existing host based intrusion prevention software every month to measure the number of times users are being locked out of their systems due to the insertion of an unauthorized device. USB storage devices are the number one contributor of these lockouts. Unauthorized mass storage devices are used by insider threats to exfiltrate sensitive information. USB drop attacks are also used to trick curious users into downloading malware onto their systems via a USB stick that may have been intentionally dropped outside of their secure facility. Users should practice good situational awareness and cyber hygiene when working from home or in the office to avoid accidentally inserting any unauthorized devices into their work computer. This metric will be measured and recorded to identify user awareness and behavior change. This metric will be measured monthly by the Cyber Security Team and presented quarterly to an advisory committee.

## Physical Security

One day a week picked at random, the ACME Central Physical Security Team will have someone sit outside of the facility at a time of heavy foot traffic (e.g. early morning, lunch, end of day) and record the number of personnel that do not conceal their access badge or allow tailgating into the secure facility. For the DOD, physical security is a major control in reducing risk. Unauthorized access to facilities by tailgating with a counterfeit badge could allow for sensitive information to be stolen. This metric will measure the staff’s understanding and enforcement of ACME Central’s policies and procedures on physical security. This metric will be measured weekly by the ACME Central Physical Security Team and presented monthly to an advisory committee.

# Learning Objectives

**Title** Phishing Detection and Reporting

## Target Audience

All military, civilian, and contractor personnel assigned to ACME Central Field Command that utilize DOD email services on their work or personal computers.

## Goal / Outcome

Course participants will be aware of the most common signs of a phishing email and the email characteristics they can use to help identify them. Participants will understand how to determine the steps to take if targeted and the appropriate reporting procedures. The decisions ACME Central personnel will make as a result of this course will lower the risk of successful phishing attacks against ACME Central Field Command personnel.

## Background

Phishing is the number one method of social engineering and is the most common vector of initial access used by adversaries targeting the DOD. There are two main types of phishing: targeted attacks (also known as “spear-phishing” or “Whaling”) and broad-based opportunistic phishing. These malicious emails use a number of methods to exploit users including but not limited to, malware embedded in attachments, links to malicious websites, and social engineering attempts designed to steal sensitive information such as passwords or financial data. ACME Central and the DOD have multiple measures in place that can help users more easily identify potential phishing attempts but it is up to the user to understand how these can be used.

## Learning Objectives

1. Email users can identify and explain the different ways phishing attacks can be delivered and executed.

a. Individual Metric: User correctly answers at least 80% of questions on a 30 question multiple choice phishing quiz, which includes a section on types of phishing attack methods. User completes interactive session that will be repeated until completed with at least 80% accuracy. The session presents various example emails, some of which are phishing and some are not. Users must extract the suspicious indicators from the emails and match them up to the appropriate phishing term.

b. Organizational Metric: Monthly phishing assessments will record which types of simulated phishing emails were successfully reported, deleted, or executed by users. Initially aim for less than 20% click rate on phishing simulations with a click percentage reduction of 5% quarterly until the click percentage stays below 5% after the 1st year.

2. Email users are able to identify and explain the various parts of a DOD email such as email encryption, digital signatures, and external or internal source.

a. Individual Metric: User correctly answers at least 80% of questions on a 30-question multiple choice phishing quiz, which includes a section on DOD email properties. User completes interactive session that will be repeated until completed with at least 90% accuracy. The session presents various example emails where users must identify the location of certain email properties (e.g., email encryption, digital signature, source).

b. Organizational Metric: The ACME Central Cyber Security Team sees a steady reduction in security violations involving improperly handled emails. Emails that are not appropriately portion marked, signed or encrypted based on the contents of the email are flagged when passing through the security stack. Flagged emails and phishing email assessment click rates should drop to below 5% after the 1st year.

3. Email users understand the correct reporting procedures that must be followed when a potential phishing email has been identified.

a. Individual Metric: User correctly answers at least 80% of questions on a 30 question multiple choice phishing quiz which includes a section on reporting procedures. User also completes interactive session that will be repeated until completed with at least 80% accuracy. The session presents various example emails, some of which are phishing and some are not. Users must correctly follow the reporting procedures for the emails they identify as phishing.

b. Organizational Metric: The ACME Central Cyber Security Team sees an increase in reported phishing emails and a reduction in security incidents involving user interaction with phishing emails after the 1st year. The ratio of deleted to reported phishing assessment emails is increased in favor of reported emails. After the 1st year 90% of phishing assessment emails are successfully reported rather than deleted or ignored.