ACME Security Awareness Plan

For ISE 5300 Managing Human Risk

2021

## Table of Contents

[Table of Contents 1](#_Toc90401893)

[README 2](#_Toc90401894)

[1.0 Executive Summary 3](#_Toc90401895)

[2.0 Engagement Strategy 4](#_Toc90401896)

[2.1 Organizational Culture 4](#_Toc90401897)

[2.2 Communication and Modalities 5](#_Toc90401898)

[2.3 Reinforcement 6](#_Toc90401899)

[2.4 Branding 6](#_Toc90401900)

[3.0 Metrics 7](#_Toc90401901)

[3.1 Phishing Click Rates 7](#_Toc90401902)

[3.2 Social Engineering Test 7](#_Toc90401903)

[3.3 Removable Media Usage 8](#_Toc90401904)

[4.0 Appendicies 9](#_Toc90401905)

## README

I developed a new security awareness plan for my current employer ACME Networked Solutions. ACME is a Global Digital Services and Solutions Provider with roughly 2,500 employees. The company mainly consists of consultants who live across the US and provide technology services for clients. ACME has a startup-like culture and prides itself on keeping up with the latest technology. Since ACME mainly consists of information technology professionals that inherently need access to sensitive data and credentials, the human risk is much higher. Our workforce has access to highly sensitive and, in some cases, classified client data. This puts ACME in a unique position to access sensitive data on many businesses that aren’t our own. This heightens the need for our employees to understand human risk. If one of our employees were to fall victim to a social engineering or phishing attempt, the data that could be exposed would affect ACME and our clients and client relationships. Our employees need to understand human risk and account for it in situations that don’t apply in standard enterprises.

## 1.0 Executive Summary

At ACME, we pride ourselves on being a Global Digital Services and Solutions Provider that delivers secure on-prem and cloud environments that form the backbone of digital transformation. Our service experts guide clients by performing initial assessments, strategy consultation, and implementation services to help clients make the most of the technology investments that drive their businesses forward. We excel at providing the technology services needed by our clients in both on-prem and cloud environments while ensuring those environments are secure.

Ensuring that we are building secure environments for our customers directly depends on our ability to secure the underlying information systems supporting our customers’ mission and business outcomes. Disruption of our systems directly affects our customers and can lead to brand degradation. Since security is a focus at ACME, we are constantly evolving how we secure our client’s technology stacks against modern threats. We have highly trained security professionals and consultants dedicated to improving our information security program.

Given the vast technical security talent and resources at our disposal, we are still exposed to a wide range of risks that our technology and security expertise can’t address. These risks are known as human risks. Human risks exploit human nature to manipulate our employees by convincing them to act detrimentally to the organization. Given our employee’s inherent requirements to have access to sensitive data of our organization and our clients, this risk is one of the most serious threats we face. A single targeted individual could compromise ACME and every client that individual services. As we continually see human risk being exploited as part of more significant data breaches and attacks, we must prioritize our efforts to train our workforce to protect themselves against this type of threat. Prioritizing our efforts to mitigate human risk will vastly lower our susceptibility to the threat of our workforce’s human nature being exploited.

To manage human risk, we must change the behavior of our workforce in ways that will directly mitigate the threats that target our organization. We can accomplish this by implementing a program to train our workforce to spot these threats before acting. This program, formally known in most organizations as security awareness training, can help by educating our staff on adversaries’ techniques to exploit human nature. With the program’s focus being the human risks that are most likely to affect the organization, we should see a dramatic reduction in our employee’s susceptibility to the risks that would significantly affect ACME. This will lead to a more robust overall security culture within ACME and, over time, lead to a better security culture within our clients.

## 2.0 Engagement Strategy

The goal of the security awareness program is to manage and mitigate threats that exploit human nature. These threats are known as human risks. Mitigation of human risk is ultimately done by changing the behavior exhibited by our employees when the exploitation of human risk is occurring. An example of changing behavior would be teaching a user how to identify and not click on a phishing email.

Changing behavior is no easy task and doesn’t occur without the employee gaining a new understanding of the methods adversaries will use to exploit them. Changing behavior requires consideration of corporate culture, employee motivation, communication, and person-to-person interaction. We must consider how these aspects will affect our chances of changing behavior to mitigate human risk. The list below will help maximize engagement when communicating security awareness messages. All awareness program communication should adhere to the following:

Maximizing Engagement

* Understand ACME’s culture of technology to make sure the message is engaging
* Use small incentives where possible to increase motivation
* Clearly communicate what outcomes are expected
* Ensure that a focus of “Why” is communicated
* The message should be positive in nature and written in a positive voice

### 2.1 Organizational Culture

ACME has over 7000 employees, with the overwhelming majority being information technology engineers. Our engineers perform consulting services for clients in many different industry verticals throughout the continental US. Technology drives the culture at ACME, and understanding new technologies as they are released is built into the culture of ACME’s workforce.

The tech industry has influenced the company culture at ACME. This has driven it to be more outgoing than many other organizations. The company accepts change and new ideas, which is ingrained in many technology/start-up style companies. This means that influencing change is easy, but making changes consistent can be more challenging.

The organization fosters an open environment where teams collaborate to get the best outcome for clients. This is so ingrained in the culture it has been given the title of “One ACME.” Given that most teams are remote workers, collaboration technologies have become the primary way groups communicate and interact with one another. This has fostered internet culture to be very present within the company.

### 2.2 Communication and Modalities

The primary method for delivering content will be annual computer-based training (CBT). This training style will give our employees the most flexibility to use their computers or personal devices and complete the activity on their schedule. This will allow for the flexible nature of work ingrained in ACME culture. Any existing training with our Compliance and Human Resources departments will be reviewed. Training will be updated to ensure that all learning objectives cover any necessary compliance or human resource-related requirements.

Training will consist of several CBT modules that apply to all employees. This will be delivered to employees via ACME’s Learning Management System (LMS). Users will be asked to complete a 20-question quiz at the end of training to ensure they understand the topics presented.

The topics for CBT training will include the following for most employees:

* Compliance training will be targeted to each employee situation as some employees will be working with clients with differing requirements. Employees will only be trained on compliance that applies to their job role. Examples of the compliance standards that users will be trained on are the following:
  + Payment Card Industry Data Security Standard (PCI-DSS)
  + Health Insurance Portability and Accountability Act (HIPAA)
  + General Data Protection Regulation (GDPR)
  + Federal Information Security Management Act (FISMA)
  + California Consumer Privacy Act (CCPA)
* Protection of Personally Identifiable Information (PII), these topics will cover the following:
  + Protecting and masking of Social Security Numbers (SSN)
  + Protecting sensitive Personally Identifiable Information (PII)
* General computer security topics will also be presented:
  + Password and authentication best practices (multifactor authentication)
  + Phishing procedures and reporting
  + Social Engineering and verification procedures
  + Using VPN on public networks
  + Removable media security best practices

### 2.3 Reinforcement

The security team understands that using CBTs isn’t sufficient for sustaining security awareness. Reinforcement training will be offered throughout the year. This will focus on enhancing the curriculum covered during the annual training by illustrating how the areas covered can protect the organization. The reinforcement training will not be mandatory but encouraged, and some small incentives will be offered to those who attend reinforcement training. Training will be provided utilizing different techniques to cater to our mixed generation workforce and their respective preferences.

The primary method of reinforcement training will consist of monthly tech talks. Each month the security team can host a tech talk to cover a current topic in security. Tech talks will focus each month on a current issue in cybersecurity. These lunch-n-learn type presentations will show how following what is learned in a primary training learning objective can protect the organization or the employee from a modern security threat. An example of this is inviting a member of the penetration-testing team to present how using multi-factor authentication can defeat credential attacks.

Gamification will also be part of the lunch and learn tech talk series. There will be a secret word that is presented at each tech talk. If you attend all the tech talks, you will be able to make the “Phrase that Pays.” Each employee who submits the correct phrase and has signed up for all the tech talk sessions will be able to get a challenge coin and a small prize such as a gift card. The “Phrase that Pays” will also reinforce the themes in primary training as it will be something memorable to ensure that the employees remember the primary training.

The secondary reinforcement training method will be a monthly newsletter sent to all employees. This will help the more conservative ACME staff members who expect a more traditional medium of engagement. The newsletters will be very concise and designed to be a shorter read. These will have a theme to help engagement, such as holidays during the month or other current events to ensure better engagement.

### 2.4 Branding

The ACME Adaptive Security logo will be used initially for all the Security Awareness Program branding. This logo is well known throughout the company and represents that the security awareness program will be an initiative that is part of the cybersecurity team. As the program moves forward, we will be coordinating with members of our marketing team and select cybersecurity team leaders to create a specific Security Awareness Program logo derived from the adaptive security badging. This new logo will then be used in all presentation materials that refer to the awareness program. The new logo and presentation materials created using the new logo will eventually signify security awareness to the greater ACME population.

## 3.0 Metrics

Metrics are the best method of ensuring that we are effectively changing behavior to reduce human risk. Measuring the Security Awareness Program will show its intended effect of educating users about the risks that exploit human behavior. These metrics can verify that the learning objectives effectively target the human risks we want to mitigate. If the metrics aren’t improving over time, the learning objectives need to be tuned to ensure that they engage the user. Three metrics have been selected based on historical analysis and the calculated areas of highest human risk. Metrics will be re-evaluated annually to ensure the program’s efficacy. If any metrics trend in the wrong direction, then the affected area’s learning objectives will be reevaluated before primary training at the beginning of the year.

### 3.1 Phishing Click Rates

Phishing is one of the most significant threats to the organization, as successful phishing can result in compromised credentials or the compromise of ACME assets. While we have strong phishing protection at the network edge, phishing emails still slip through even the best phishing protection. This means it’s best to educate our employees on how to spot and report a phishing email.

**Metric**We will conduct phishing tests and report the success rate back to the organization. Metrics will be compared between departments, and an internal dashboard will be created. This will allow better measurement based on job role and create internal competition amongst departments.

**Frequency**Phishing tests will be conducted monthly. We will test 1000 users at a time and spread them among departments until all users have been tested. This will ensure effective testing as most users will either click immediately or not at all. This will also prevent users from informing other users of the phishing test.

**Metric Goal**Reducing the rate of users clicking on Phishing emails to prevent the risk of compromised credentials or compromise of ACME assets.

### 3.2 Social Engineering Test

Social Engineering is a technique used to trick a user into taking an action. Since Social Engineering has been a problem in the past for ACME, we will conduct social engineering testing to see if enticing users into action is possible. Our workforce should follow verification procedures before taking any steps that would be detrimental to the organization.

**Metric**We will conduct Social Engineering tests to ensure that employees follow required verification procedures. We will report the rate of users not following verification procedures. The security team will choose one process requiring verification and convince the employee not to follow the procedure. This will ensure that ACME is protected against threats from users not following verification procedures.

**Frequency**Social Engineering tests will be conducted annually at least once per department. These tests will be tested in order of risk based on the area where the risk is highest, then working through each department. Each year, the risks will be different to ensure that all verification procedures within ACME are tested.

**Metric Goal**To lower the percentage of employees who don’t follow verification procedures, thus reducing the risk of employees conducting actions that could be detrimental to ACME.

### 3.3 Removable Media Usage

The risk of using unencrypted media for sharing files could result in the loss of ACME’s proprietary information, intellectual property, or data belonging to ACME clients. Since ACME has a long-standing policy of not allowing the usage of unencrypted removable media, we will measure employee behavior around using unencrypted media in ACME-owned devices.

**Metric**We will conduct a removable media drop or direct mailing of a removable media drive to select employees. We will detect when the removable media devices are plugged into ACME assets and are not reported to the security team. This will ensure that employees follow the removable media best practices learning objective. We will also create a dashboard to measure the success of this metric for presentation to management.

**Frequency**We will conduct the USB drop or direct mailing annually at least once per department. We will note the time and date of the removable media usage and report this back to departmental management.

**Metric Goal**Ensure that ACME employees follow the guidelines on secure usage of removable media to prevent the risks of losing intellectual property, proprietary data, and malware infection.

## 4.0 Appendicies

#### 4.1 Learning Objectives

Learning objectives give the security awareness program a method to measure changes in employee behavior by categorizing human risks into a set of required knowledge. Learning objectives allow ACME to reduce specific risks by measuring employee knowledge around the correct behaviors to minimize the threats most likely to affect the company.

**Title:** Password and Authentication Best Practices

**Target Audience:** All employees with a particular focus on employee groups who access sensitive data such as HR, Finance, and Information Technology.

**Goal:** Course participants will learn good password practices. Learners should be able to create secure passwords and recognize a strong versus weak password when presented. Learners should understand the benefits of multifactor authentication and what type of data should require multifactor authentication before being accessible.

**Background:** ACME employees must authenticate as part of initial access to all corporate systems. This fundamental identity boundary prevents unauthorized access to systems if strong passwords or multifactor authentication are used. Identity boundaries can be easily defeated if a single employee with privileged access uses a weak or easily guessable password. This puts a tremendous amount of trust in our employee’s judgment on using strong passwords for authentication. Usage of weak passwords dramatically increases the risk of system compromise, especially when compensating controls are weak or not present.

**Learning Objectives:**

1. Learners can explain the need to use strong passwords.
2. Individual Metric: The learner correctly identifies why strong passwords are needed in a test question.
3. Learners can explain why a single dictionary word is a poor choice for a password.
4. Individual Metric: The learner correctly identifies why dictionary-based passwords are a poor choice in a test question.
5. Organizational Metric: A user can assess a good password from a sample list of passwords.
6. Learners can create a passphrase and determine why they are necessary.
   1. Individual Metric: The learner can correctly identify strong passphrases in a test question.
7. Learners can explain why you need to use a unique password for every account.
   1. Individual Metric: The learner correctly identifies reasons passwords should not be reused in a test question.
   2. Organizational Metric: A password assessment against a list of user passwords from differing systems to see if password reuse occurs.
8. Learners can explain the reasons to be careful when choosing questions for password resets.
   1. Individual Metric: The learner can correctly identify the risk of choosing password reset questions and answers that can be easily guessed in a test question.
   2. Organizational Metric: Assess a sampling of user password questions and answers.
9. Learners can identify the benefits of using multi-factor authentication
   1. Individual Metric: The learner can correctly identify various types of multi-factor authentication methods and determine which are the most secure in a test question.
10. Learners can demonstrate how password managers work and the benefits of using them.
    1. Individual Metric: The learner correctly identifies what password managers are used for and the benefits of their usage in a test question.