**Commonwealth Energy**

**Security Awareness Program Project Plan**

**ISE 5300**

**Note:** This document is not a complete security awareness plan. It is limited to the subsections required by the ISE 5300 course offered as part of the SANS Technology Institute’s Master of Science in Information Security Engineering as of January 2021.

**Table of Contents**

**Read Me 3**

**1 – Executive Summary 4**

**2 – Engagement and Training 5**

**2.1 – Overall Engagement Strategy 5**

**2.2 – Company Culture 5**

**2.3 – Localization Requirements 5**

**2.4 – Training 5**

**2.5 – Branding and Imagery 6**

**3 – Metrics 7**

**3.1 – Impact Metrics 8**

**4 – Appendices 9**

**4.1 – Appendix A – Learning Objectives 9**

**READ ME**

The name of the organization I have chosen to write a security awareness plan for is Commonwealth Energy. It is a fictional organization based on my current employer. I have chosen to anonymize the organization for security reasons. I picked this type of organization because this is where I currently work. This company is in the energy vertical with over twenty thousand employees. It is located solely in the United States of America. I chose to create an awareness plan from scratch.

**1 – Executive Summary**

Our mission at Commonwealth Energy is to serve our customers safely and reliably by keeping the lights on while strengthening our communities, minimizing environmental impacts, and rewarding our shareholders. Our customers rely on us to provide them a critical component of everyday life. Energy is considered a uniquely important sector of critical infrastructure. It fuels the economy and is an enabler for all critical infrastructure sectors. Energy is so vital to our country that its loss would be considered a threat to national security, the economy, and public health. As such, our company’s risk tolerance is very low.

Given our company’s mission and risk tolerance, our organization employs best-in-class security technologies and practices as security controls to reduce the risk of unauthorized access, modification, or destruction of our data or systems. Despite this regimen, incidents and breaches across our vertical and others are tied to a risk that cannot be mitigated with technology-based technical controls alone. According to the 2020 Verizon Data Breach Investigations Report (DBIR), human risk remains one of the highest preferred risks for attackers to target. This risk category includes phishing, credentials, and errors such as misdelivery of emails or misconfiguration of systems.

A security awareness program (SAP) is a control utilized to mitigate human risk. Human risk mitigation is accomplished through engagement and training of the workforce, which positively alters workforce behavior. This control is considered a compensating control in addition to our technical controls to help reduce residual risk to a level commensurate with our organization’s low-risk tolerance. Adopting this program will further ensure our company’s ultimate goal of keeping the lights on to enable our customers.

There is no finish line in security. Accordingly, this program will operate in a perennial capacity with core training for all employees and role-specific training for employees in specific functions with unique risks. To ensure the highest return-on-investment (ROI), the program will focus its efforts on the most critical human risks. These prioritized risks will be identified by conducting a qualitative risk assessment. Annual updates will help ensure this program safeguards continued risk mitigation. The Human Risk Officer (HRO) will lead this program, report to the Chief Information Security Officer (CISO), and utilize an advisory board consisting of key players throughout the organization to assist in planning and maintaining the program.

**2 – Engagement and Training**

**2.1 – Overall Engagement Strategy**

For this program to be effective, our workforce must have the motivation and the ability to change their behavior. This program will inspire motivation by communicating the importance of our company’s mission in supporting our customers, communities, and country and how security helps safeguard the completion of that mission. We will ensure our employees can explain why our service is considered critical infrastructure and how cyber human risk plays a large role in the continuity of that service. To reinforce the notion that each employee’s behavior matters, we will promote the following slogan: “You are the key to cybersecurity.” Through our training, the workforce will obtain the ability to make the right decisions at the right times.

**2.2 – Company Culture**

Our company is mostly conservative, with a healthy mix of employees from different generations. The leadership team strives to be transparent and create a safe, diverse, and inclusive working environment. There is a focus on providing clean renewable energy to help protect the planet and support the communities we serve through volunteering and charitable contributions. Work-life balance is important to leadership, which speaks to the company’s family values. Commensurate with those family values, our training will be constructive and encouraging while striving to protect our employees both on and off the job.

**2.3 – Localization Requirements**

Being centrally located in the United States, our program will communicate in American English.

**2.4 – Training**

Prior to the release of any training, Corporate Communications will send an email on behalf of the leadership team. This will introduce the workforce to the training and communicate the importance of its message as well as its learning outcomes.

**2.4.1 – Primary Training**

Computer Based Training (CBT) will be the main technique used for training. CBT will be delivered and tracked through our Learning Management System (LMS). This training will be mandatory, conducted annually, and available on-demand. This delivery method will allow employees to take the training at their own pace and schedule. Automated quizzes will be utilized throughout the training to engage the employee as well as to measure comprehension continually. This training will ensure the company satisfies compliance requirements.

LMS will notify employees via email that they have been enrolled in training and remind them if they are approaching completion deadlines. When training is completed, LMS will send a training completion email for employee record keeping. Accessibility features will be utilized to enable successful training for all employees.

**2.4.2 – Reinforcement Training**

The SAP team understands that annual primary training is not sufficient to change employee behaviors. Accordingly, SAP will offer reinforcement training focusing on strengthening employee comprehension of the material covered during the annual training. This training will not be mandatory but will be encouraged. Training will be offered utilizing different techniques to cater to our mixed generation workforce and their respective preferences.

One of the primary methods for reinforcement training will be newsletters to accommodate the more conservative crowd. Newsletters were chosen since the conservative demographic prefers a more traditional medium for content. These will be sent monthly with the objective of being concise and pointed. The SAP team will also take advantage of seasonal themes that help protect our employees away from work, such as holidays, vacations, and annual taxes. The other primary technique will be geared towards gamification to cater to the younger millennial demographic. A virtual scavenger hunt will be hosted quarterly, which will have interested employees compete for points in a question and answer capture-the-flag style event. This technique was chosen since the younger generations prefer to make learning fun and interactive. Corporate Communications will announce the top ten employees while the top three employees will win SAP challenge coins.

**2.5 – Branding and Imagery**

Our organization has a powerful brand, which we have chosen to embrace. The advisory board, which includes members from Corporate Communications and Branding, thought that utilizing the brand colors would make the content seem familiar to our employees. Our logo involves a padlock and key, which compliments our tagline, “You are the key to cybersecurity.” Corporate Communications is responsible for all internal communications and is also available ad hoc to answer employees’ questions. Corporate Communications will coordinate with the SAP team as needed to answer these questions promptly.

**3 – Metrics**

Since our program has no finish line, metrics become crucial in determining what our program is doing well and what needs improvement. Metrics will also communicate to leadership the value our program provides to the organization. Our program will track and measure two types of metrics: compliance metrics and impact metrics. Compliance metrics will measure our activities and ensure compliance with all applicable requirements. Impact metrics will measure the change created by our program. Commensurate with leadership’s belief, as mentioned earlier, in transparency, the program will be honest and open about the metrics it employs while protecting its employees’ identities. Our program will practice positive reinforcement and highlight employees exercising desired behaviors.

**3.1 – Impact Metrics**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Metric  Name | Measure  What? | Measured  How? | Measured  When? | Measured  By? | Measured  Why? |
| Phishing Click Rate | The number of people that fall victim to phishing simulation by clicking on a link or opening an attachment. | Phishing Assessment | Monthly | SAP Team | By measuring victims who fall victim to simulated phishing emails, SAP can determine if awareness increases (click rate decreases over time). |
| Phishing Reporting | The number of people that report phishing emails. | Phishing Assessment | Monthly | SAP Team | By measuring employees who report phishing emails, SAP can determine if awareness increases (report rate increases over time). |
| Phishing Repeat Offenders | The number of people that repeatedly fall victim to phishing simulations. | Phishing Assessment | Monthly | SAP Team | By measuring employees that consistently fail simulated phishing emails, SAP can determine employees that are considered high risk.  These employees would require additional training and potentially escalations with their manager and Human Resources. |

**4 – Appendices**

**4.1 – Appendix A – Learning Objectives**

**4.1.1 - Title**

Phishing Security Learning Objectives

**4.1.2 – Target Audience**

All employees and contractors that use email as part of their job duties.

**4.1.3 – Goal**

Employees and contractors will learn why knowledge of phishing is essential. They will obtain the capability to explain what phishing is and how to identify it. The change in behavior that participants exhibit after this training will reduce the organization’s risk.

**4.1.4 – Background**

Email is one of the primary methods of communication in the world today. Due to its popularity, it has become a favorite for attackers to penetrate the perimeter and gain an initial foothold inside victim networks. This presents a substantial risk to every organization. This training will teach participants how to use email safely.

**4.1.5 – Learning Objectives**

1. Participants can explain what phishing is, the different phishing types, and demonstrate how to identify it.
   1. Individual metric – Participant correctly identifies what a phishing email is in a training session.
   2. Organizational metric – Send simulated phishing emails enticing participants to click on malicious content.
2. Participants can identify various indicators of a phishing email.
   1. Individual metric – Participant correctly identifies phishing email indicators in a training session.
   2. Organizational metric – Less than a certain percentage of participants fall victim to a simulated phishing email.
3. Participants can demonstrate how to report a phishing email.
   1. Individual metric – Participant correctly identifies the proper reporting method in a training session.
   2. Organizational metric – More than a certain percentage of participants accurately report a simulated phishing email.