**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 May 2021.

ABC PETROLEUM

Security Awareness Program Project Plan

ISE 5300

JAmes Cheng

2021

**README**

The organization that I have picked to write a security awareness plan on is ABC PETROLEUM. ABC PETROLEUM is a fictitious organization based on my current employer. I have chosen to anonymize the organization for security and compliance reasons. The reason I chose to write the security awareness plan for my company is so as to maximize the relevance and benefit of this assignment to my current organization. My company is a global multinational exploration and production diversified resources company with a Petroleum division. The company has approx. over fifty thousand employees and contractors operating across multiple countries.

The awareness plan that I will be building will be a new security awareness program plan that is focused on addressing human risk within our production operations space at our production assets and will be separate from the security awareness plan that already exist at the global level which is more generic and mainly focused on the broader enterprise IT security.

Table of Contents

[Executive Summary 3](#_Toc73956611)

[Engagement and Training Strategies 4](#_Toc73956612)

[Organizational Culture 4](#_Toc73956613)

[Communication and Modalities 4](#_Toc73956614)

[Awareness Campaign: 4](#_Toc73956615)

[Primary Training: 5](#_Toc73956616)

[Reinforcement Training: 5](#_Toc73956617)

[Enrollment & Notification: 7](#_Toc73956618)

[Localization Requirements 7](#_Toc73956619)

[Branding and Imagery 7](#_Toc73956620)

[Metrics 8](#_Toc73956621)

[Impact Metrics 9](#_Toc73956622)

[Appendix - Learning Objectives 11](#_Toc73956623)

[Title : 11](#_Toc73956624)

[Learning Pathway : 11](#_Toc73956625)

[Target Audience : 11](#_Toc73956626)

[Goal : 11](#_Toc73956627)

[Background : 11](#_Toc73956628)

[Applicable Human Risk : 11](#_Toc73956629)

[Learning Objective 1 : 12](#_Toc73956630)

[Learning Objective 2 : 12](#_Toc73956631)

[Learning Objective 3 : 12](#_Toc73956632)

[Appendix - Learning Pathways Catalog of Modules 13](#_Toc73956633)

Executive Summary

At ABC Petroleum our mission is to operate the best assets in the world productively and securely. Safety and sustainability come first in everything we do. Today, at all of our operations, we are increasingly leveraging technology, data and automation to help us in operating as efficiently and safely as possible. The use of technology, despite all of its benefits both to productivity and operational safety, exposes us to new kinds of risk within the cyber security space.

Cyber criminals, hacktivists, and nation state threat actors often seek to compromise and attack the technology systems at industrial or critical infrastructure for various malicious intent. The physical safety and productivity of our people and infrastructure at our production facility strongly depends on our ability to effectively secure our information technology (IT) and operational technology (OT) systems at our sites. This is not only a fundamental obligation we have to our workforce and their families, but a compromise to safety due to a cybersecurity incident can have material financial, environmental, legal, regulatory, and reputational impacts including a risk to our license to operate.

In order to effectively secure our IT and OT system, ABC Petroleum’s Cybersecurity team has increasingly over the recent years invested in and applied many of the latest cybersecurity technologies in a defense-in-depth strategy. Technical and process related controls form just a portion of our overall cybersecurity preventative and mitigative control, but the people aspect is just as important. There has been a growing number of critical incidents in recent years in our industry due to people and specifically human risk. A recent and closely relevant example to our company is the ransomware attack on Colonial Pipeline IT systems which led to the shutdown of all of their IT and OT systems at the site resulting in huge financial, operational and societal impacts. Although the exact cause of the ransomware has not been officially announced yet, these types of attacks are usually introduced through targeting humans. Human risk within our production operations environment and at our operational facilities is one of the areas for us that is under-addressed, and with an increased frequency of attacks and risks to industrial and critical infrastructure, this is an area we should focus on through the introduction of a focused security awareness program for our production facilities.

A security awareness program (SAP) is one of the types of security control and is specifically designed to manage human risk through the training and engagement of our workforce. The SAP will be targeted at our workforce that operates the critical IT and OT systems at our production sites. This program is not meant to replace existing technical controls, but instead helps further strengthen our overall cybersecurity posture through the securing of the human element.

The SAP will be a long-term ongoing effort involving people at all levels that directly or indirectly support our production sites. The SAP will involve awareness campaigns, general and targeted training, as well as the integration of a cyber safe culture as part of the overall safety culture that already exist at our sites. This will be done through training of our onsite safety champions on cybersecurity related risks and best practices. The SAP will identify and prioritize the addressing of our top human risks and implement metrics and ongoing measurements and will be reviewed and updated annually to ensure ongoing effectiveness and relevancy. The SAP will be administered by our Cybersecurity Team led by the CISO and will be guided by a dedicated advisory board comprising representatives both from our Technology Team as well as our Asset Operations Team.

Engagement and Training Strategies

This Security Awareness Program’s objective is to equip the workforce that supports the IT and OT systems at our production sites to be able to detect and respond to cybersecurity risk swiftly and appropriately. Many of the IT and OT systems that our workforce uses at our production sites are getting increasingly more complex and with the changing cyber threat landscape, a compromise can lead to severe safety, financial, environmental, legal, and regulatory impacts if not managed safely and effectively. Effective and continuous training and preparedness of the workforce can effectively reduce the risk of any incident due to human risk or a minimization of impact if any incident were to occur.

## Organizational Culture

The culture at ABC Petroleum production sites is already one that is heavily focused on safety. Effective management of risk and reducing it to as low as practicable is already one of the principles that is deeply embedded into the culture.

The operations leadership team and workforce continuously and diligently strives to manage a safe operation including ensuring all maintenance activities are religiously carried out to maintain asset integrity. As such, with the pre-existing deep focus on safety and asset integrity, the program will seek to ensure that the workforce grows to understand that cyber risk is one of the many different risks that they are already managing so well, and that effective management of cyber risk will allow them to maintain a safe and productive operation and ensuring everyone goes home safely to their families.

The workforce that directly supports the production sites are mostly not technologically savvy and mostly conservative with a healthy mix of employees and contractors from different generations. The workforce operates 24x7 on a rotating roster and most are involved in maintenance activities out in the process area and do not sit in front of a computer all day. Most of these production sites are also remote and not easy to get to.

## Communication and Modalities

The implementation of the SAP will be conducted through 3 channels.

* Awareness Campaign
* Primary Training
* Reinforcement Training

### Awareness Campaign:

The awareness campaign will be the initial channel in which the introduction of the topic on cybersecurity risks that exists to industrial and critical infrastructure, the implication to safety, and good cybersecurity behaviors will be introduced to the workforce.

The awareness campaign will be conducted through means of quick 1-page newsletters distributed in digital format, infographics that will be shared through the corporate computer screen-lock wallpaper, and posters that will be placed in common areas around the production facility.

This will be introduced over the initial weeks of the program to build and create awareness prior to introducing the formal primary training requirements so as to first create awareness and generate interest to build up momentum prior to the launch of the mandatory training program.

The awareness campaign will continue to run throughout the year continually as a means of keeping cybersecurity risks and good behaviors front and center of the workforce minds.

Once a general awareness and familiarity has been built within the workforce, this will be measured through conducting of a quick 5 minute survey, then the SAP will begin to introduce the primary role-based training plan that will include training and goals relevant to the roles that each individual play at site.

|  |  |
| --- | --- |
| **Role** | **Training Learning Pathways** |
| Short Term Contractors, Visitors, New Hires | Fundamentals of Cybersecurity Training CBT |
| Mechanical | Basic Cybersecurity Training CBT |
| Control Room Operator | Intermediate Cybersecurity Training CBT  Incident Response and Recovery CBT |
| Electrical, Instrumentation, Automation, Technology | Advanced Cybersecurity Training CBT  Incident Response and Recovery CBT |
| Management and Leadership | Management Cybersecurity Training CBT |

\*A List of the CBT modules that are contained as part of each learning pathway is presented in the appendix of this SAP as part of a catalog of learning objectives.

### Primary Training:

Since most of the workforce will not be able to sit in front of a computer all day or take time off for extended training programs due to the nature of their roles and rosters they work to, and also the production sites are remote and difficult to get to, most of the training and awareness content will be delivered through short mandatory role-based computer-based training (CBT).

This will allow the workforce to have flexibility around when they take their training as their schedule or shifts allows. This also avoid the need for trying to get trainers to site for instructor led training or the long-extended time commitment from virtual live training sessions.

All training content will be developed under the guidance of the Cybersecurity team and reviewed by legal and Human Resources prior to publishing into ABC Petroleum’s Learning Management System (LMS).

Each role-based training program can comprise of multiple CBT modules, with each CBT module being no longer than 30mins. There will be a series of interactive quizzes and questions throughout the CBT to keep the learner engaged whilst testing comprehension of each module.

All CBT modules will also be developed with closed caption (CC) and text transcripts for all audio parts to allow accessibility to anyone with hearing impairment. For anyone suffering from loss of sight, CBTs can also be conducted with a nominated facilitator to aid in the completion of any parts of the CBT that cannot be easily expressed in audio recordings.

All training will be repeated annually and will be specific to each role type.

### Reinforcement Training:

Although training is repeated annually, it is recognized that this may not be enough in changing their behaviors. Therefore, for a few of the key behaviors around a few of our highest cybersecurity risks, we will be utilizing a variety of reinforcement methods throughout the year to target and train those desired behaviors.

Reinforcement training will not be introducing something new but will cover materials that are already covered in the primary training. In terms of timing, Reinforcement training will be launched a quarter after the roll-out of the primary training.

* **Monthly Campaigns**

These campaigns will be based on a particular high-risk topic (i.e. phishing campaign) for that month, and will be conducted in a way that can be measured. This will provide a mechanism to communicate actual statistics back to the workforce and organization, as well as introduce a way to reward good behavior.

**Example (Phishing Campaign):**

One of the highest risk areas to our operations is through the means of a phishing attack targeted at our workforce who have access to the critical OT systems at site. A phishing attack is an email crafted to look like a legitimate email and usually tries to convince the recipient to either click a link, download a file or attachment, or review some sensitive information.

Through the CBT training as mandated through the SAP, all employees, contractors and visitors will have been trained on how to spot suspicious phishing emails and the right behaviors around how to respond to these types of email, which is to click on the “report phishing button” located within the email client.

Through such a campaign, the practical real-life experience around remaining vigilant can be reinforced and reporting on the click rate can help the organization measure the effectiveness of specific areas of the program and also further tailor training to areas of highest risk. The measured results can be used to create friendly competition between sites and reward good behavior.

Any employees found to have clicked on the phishing email will immediately be notified through the email client phishing plug-in, as well as an automatic email that will be sent to them with quick refresher tips on aspects of that email that could be tell-tale signs that this was a phishing attempt and the appropriate actions and behaviors that should follow. Subsequent repeat click violations will result in an email to their line manager as well as automatic enrollment into refresher training in the LMS.

|  |  |  |
| --- | --- | --- |
| **Monthly Campaign Schedule** | **Schedule** | **Target Group** |
| Phishing – Level 1 | 2021 – Q1M1,M2,M3,M4 | All Employees |
| Social Engineering Test Call – Level 1 | 2021 – Q1M2 | All Employees |
| Update Your Device Drive | 2021 – Q1M1,M2,M3,M4 | All Employees |
| Phishing – Level 2 | 2021 – Q2M1,M2,M3,M4 | All Employees |
| Social Engineering Test Call – Level 2 | 2021 – Q2M2 | All Employees |
| Update Your Device Drive | 2021 – Q2M1,M2,M3,M4 | All Employees |
| Phishing – Level 3 | 2021 – Q3M1,M2,M3,M4 | All Employees |
| Social Engineering Test Call – Level 3 | 2021 – Q3M2 | All Employees |
| Update Your Device Drive | 2021 – Q3M1,M2,M3,M4 | All Employees |
| Phishing – Holiday Season Special | 2021 – Q4M1,M2,M3,M4 | All Employees |
| Social Engineering Test Call – Holiday Season Special | 2021 – Q4M2 | All Employees |
| Update Your Device Drive | 2021 – Q4M1,M2,M3,M4 | All Employees |

* **Seasonal and Event based content**

Post any public breaches, events or news that has a cybersecurity risk implication to ABC Petroleum, special training and awareness newsletters or infographics will be developed to provide targeted reinforcement of certain key behaviors. This content will be produced and published as required and will aid in providing a real and tangible connection to the cybersecurity safety culture that is being developed to real world examples.

* **Monthly Safety Stand-Down**

At ABC Petroleum production sites, the operational teams perform weekly safety stand-down meetings where the majority of the team will stop work and spend a couple of hours discussing topics relating to personnel and process safety. Our cybersecurity SAP will leverage these sessions on a monthly basis and use this to further embed the culture and behaviors around cyber safety into part of the existing strong safety culture that already exist. The site’s safety champions will also be trained and provided with material to help champion good cybersecurity behaviors to the broader workforce at site.

### Enrollment & Notification:

An email will be sent out to all core workforce member with the respective training requirements based on their role. For non-core workforce members (i.e., short-term contractors or visitors) the enrollment for the visitor’s cybersecurity CBT will be automatic as part of their site visit induction requirements.

On enrollment, an email notification will be sent to each individual including their line manager, and automatic reminders will be sent also to the individual and their line manager if they are past due.

On completion of each module, an automatic certificate will be sent to the individual. Once an entire learning pathway has been completed, a final certificate will be automatically sent to each individual and their line manager and a message congratulating and certifying them for their respective track. All employees can voluntarily enroll for a more advanced cyber security training CBT learning pathway if they so desire to do so via the LMS.

### Localization Requirements

ABC Petroleum has operating production assets located all around the world, specifically in USA, Canada, Mexico, Trinidad & Tobago, Singapore, and Australia. Although generally all our organization speaks and operates in English, some of the operational workforce in Canada are predominantly Canadian French speaking, in Mexico are Mexican Spanish speaking, and in Singapore and Australia are British English speaking with variation in certain terminology and spelling. As such, our program will be tailored accordingly to maximize impact and relevance to the local audience.

### Branding and Imagery

ABC Petroleum has global corporate branding around color theme, but generally not prescriptive around style and imagery. The SAP will adhere to the corporate branding around use of the corporate color theme as required by our global standards. However, to connect better with our workforce who mainly understands process safety and risks in the oil & gas industry, we will capitalize on that already strong safety culture and make use of imagery, situations, and contextual case studies that the work force already understands but connected with Cyber security risk. For example when explaining the impacts of certain cyber events or compromises, instead of focusing on things such as loss of financial information or personally identifiable information that is commonly used in other industries, we will use events such as a potential Piper Alpha or BP Macondo event. Although those were not cyber related causes, the potential impact could be similar in a compromise of the facilities OT systems.

This will help the workforce understand and see the connection of how these new cybersecurity training and behaviors being taught are enhancing what they are already doing as part of their safety culture in keeping them safe and ensuring that everyone goes home safely to their families and not just another annoying corporate IT requirement.

The program will not be establishing any new cybersecurity engagement ambassadors. The program will leverage the safety champions already at each site and enlist the support of these safety champions to act as a focal point for the review of any new safety messages. The site safety champions will also act as a local escalation point if people have any security questions or security incident they want to report. This local escalation channel will be in addition to the official reporting channels that will be taught as part of the training.

Metrics

As part of the continuous SAP, compliance and impact metrics will be used to measure the effectiveness of the program as well as aid the program’s steering committee in further tailoring program activities to address areas of greatest risks and needs. Compliance Metrics will help the program’s steering committee track and measure the adoption and completion of the mandatory CBT modules by role.

## Impact Metrics

| Metric Name | What is Measured | How is it Measured | When is it Measured | Measured by | Why is it Measured |
| --- | --- | --- | --- | --- | --- |
| Phishing Click Rate | Number of people that fall victim to phishing simulation by clicking on a link or opening an attachment. | Phishing Assessment | Monthly | Cybersecurity Team | This indicates the current risk exposure within the workforce and provides a measure for additional training requirements. This number should decrease over time as behavior changes. |
| Phishing Reporting | Number of people who click on the PhishMe phishing report button (Regardless of whether it is part of a simulation or not) | Phishing Assessment | Monthly | Cybersecurity Team | This indicates the effectiveness of the SAP training and an increase in number over time will indicate progress in the maturity of the workforce in this area acting as Human Sensors. |
| Phishing Repeat Offenders | Number and names of people who repeatedly fall victim to phishing simulations | Phishing Assessment | Monthly | Security Awareness Program Team | Individuals who are not changing behavior represent a high risk to the organization and would be candidates for additional training. |
| Social Engineering | Number of people who can identify, stop and report a social engineering attack | Phone call assessments | Quarterly | Security Awareness Program Team | Another avenue in which attackers use to bypass technical security controls is through social engineering attacks trying to get employees to divulge sensitive information or pretending to be from internal or external technology support organizations and have victims download malicious payloads. Measurement of this will identify the effectiveness of the SAP training and the risk exposure our sites have to such attacks. |
| Updated Devices | Percentage of corporate IT and OT devices that are updated and current the meantime to being updated from when an update is available until when it is implemented. | Online update/patch assessments | Monthly | Cybersecurity Team | Often times within the operational environment, updates are not mandatorily started so as not to impact production activities. An update is presented by the workforce has the option to delay or reschedule the installation of the updates.  This metric helps measure the risk exposure of our systems and helps assess whether the workforce is improving in their understanding on the importance of keeping devices updated instead of continuously delay the installation of updates. |

# Appendix - Learning Objectives

## Title :

Use of Removable Storage Media

## Learning Pathway :

* Fundamentals of Cybersecurity Training CBT
* Basic Cybersecurity Training CBT
* Intermediate Cybersecurity Training CBT
* Advanced Cybersecurity Training CBT
* Management Cybersecurity Training CBT

## Target Audience :

The target audience for this training module is stated in the role-based learning pathway table as shown in the Engagement and Training Strategies section.

## Goal :

All employees and contractors should understand the risks around the use of and connection of removable storage media devices to the IT and OT systems at site. In this course, the learners will learn the processes around the safe and responsible use of removable storage media devices, how to gain approval, and be able to explain the risks and reasons behind the need to be vigilant and adhere to the process prior to connecting any device to the IT and OT systems and network.

## Background :

Removable storage media are used during certain operational and maintenance activities to store and transmit files between systems. This could either be logs, applications, control system project files or any other data that cannot be copied over the network either due to size or technical cybersecurity perimeter controls. However, as much as these devices are useful in moving of files, it presents a risk around allowing malware to bypass technical cybersecurity perimeter defense controls and can be a vector for the introduction of malware into the environment. This module will teach the steps individuals can take to use removable storage media devices responsibly and safely at our production sites.

## Applicable Human Risk :

Employees or Contractors who have a need to use and connect removable storage media devices to the IT and OT systems at a production site.

## Learning Objective 1 :

Learners can explain the risk around using of removable storage media devices especially ones that are obtained from unknown or untrusted sources.

* Individual Metric:

Learners correctly identifies the risks around using removable storage media devices as part of the CBT quiz.

* Organizational Metric:

Collection of a sampling of users that correctly identifying the risks around using removable storage media devices as part of the CBT quiz.

## Learning Objective 2 :

Learner can correctly explain the process that needs to be followed to gain first gain approval for the authorized use of removable storage media devices and this is logged within the request for approval system. The learner then correctly performs the checklist of self-assessment questions as part of the authorization process to assess the trust worthiness and risk of the device containing malware. The learner will then proceed to use the sand-box test system located at each site to scan and sanitize the device prior to connecting the removable storage media device to the IT or OT systems.

* Individual Metric:

Learners correctly identifies the steps and procedures around responsibly and safely using removable storage media devices as part of the interactive training section of the CBT.

* Organizational Metric:

Collection of a sampling of user declaration and authorization request from the system, and then matching that up with the test reports and logs from the sand-box test system located at each site.

## Learning Objective 3 :

Learners can correctly explain and identify the different indicators of compromise and necessary immediate actions to take if a malware breakout occurred as part of the use of removable storage media devices.

* Individual Metric:

Learners correctly identify some of the common indicators of compromise and a series of recommended immediate actions to be taken as part of the interactive training section or through a series of test questions as part of the CBT.

* Organizational Metric:

Number of reported incidents that occur from use of removable storage media devices that are reported proactively by users of removable storage media devices within a short period of the incident occurring and immediate mitigative actions have been taken, regardless of whether it is a false positive or true positive incident.

# Appendix - Learning Pathways Catalog of Modules

| Training Learning Pathways | Modules |
| --- | --- |
| Fundamentals of Cybersecurity Training CBT | * Secured Area Access Management * Phishing * Use of Removable Storage Media |
| Basic Cybersecurity Training CBT | * Secured Area Access Management * Phishing * Use of Removable Storage Media * Data Privacy and Safe Data Handling * Passwords * Safe Web-Browsing * Social Engineering Attack * Unauthorized Software Use |
| Intermediate Cybersecurity Training CBT | * Secured Area Access Management * Phishing * Use of Removable Storage Media * Data Privacy and Safe Data Handling * Passwords * Safe Web-Browsing * Social Engineering Attack * Unauthorized Software Use * IT vs OT Segregation of Networks * Ransomware * Email Security * OT System Acceptable Use Policy |
| Advanced Cybersecurity Training CBT | * Secured Area Access Management * Phishing * Use of Removable Storage Media * Data Privacy and Safe Data Handling * Passwords * Safe Web-Browsing * Social Engineering Attack * Unauthorized Software Use * IT vs OT Segregation of Networks * Ransomware * Email Security * OT System Acceptable Use Policy * Privilege Access Accounts * Secure use of Remote Access * Patch Management * Vulnerability Management * End-Point Protection |
| Incident Response and Recovery CBT | * Responding to Ransomware (Production Operations Team) * Responding to unauthorized system access |
| Management Cybersecurity Training CBT | * Secured Area Access Management * Phishing * Use of Removable Storage Media * Data Privacy and Safe Data Handling * Passwords * Safe Web-Browsing * Social Engineering Attack * Unauthorized Software Use * Reporting Requirements * Management of Cybersecurity Incident (Facility Management Team) |