Company: WestWorld - A Delos Destinations, Inc. Company
Author: Latoya Jamison

Security Awareness Program

Securing Our World

Table of Contents

Executive Summary

WestWorld is an industry leading vacation destination operated by Delos Destinations, Inc. The park is operated by majority artificial intelligent/android technology robots known as, “host”. The code and the advanced 3D printing technology used to create the host were created by Dr. Robert Ford and Arnold Weber. WestWorld provides a unique experience to all guests at every age. As all hosts are lifelike and provide guests the opportunity to experience a variety of unique storylines during their stay in the park. All hosts are unable to harm any guest it interacts with, and are preprogrammed to follow a set narratives(storylines) that play out daily, but are able to be interrupted by the park guest at their leisure. All hosts are reset every 24 hour period, and restart their preprogrammed narratives.

Westworld Intellectual Property and park guest data make it a target for insider/external threats, as well as data breach attempts. Therefore, a new security awareness program will help educate and ensure all employees have the proper tools and knowledge to help protect the organization. This includes but is not limited to proprietary data/intellectual property, park guest or employee applicable PII.

Currently, there is no standalone security awareness program within the organization, and security education is delivered primarily during employee orientation. The new security awareness program will not only help supplement security training taught during company orientation, but will also ensure continuous security awareness training in order to help promote security and assist the organization in reducing its human risk.

The new security awareness program will also ensure the organization maintains its PCI-DSS, SOX, ISO 2700 compliance requirements and standards.

The main goals of the WestWorld security awareness program is as follows:

- Educate employees on the importance of security of all data maintained by Westworld.
- Educate employees on the importance of physical/ cyber security in order to protect all intellectual property, company data, and physical safety of all employee and park guests.
- Reduce overall human risk and threat landscape of the organization.
- Ensure the company maintains compliance requirements.

Project Charter

Project Title:	Securing our World
Project Owner:	Will require co-ownership from member of the following teams: ● Cyber security operations ● Communication/Marketing team.
Estimated Cost:	● First year: $1,250,000 - Includes initial cost for starting the new security awareness program. - Approximately 35% will be for support with getting the new security modules developed by the LMS. - Approximately 20% will be for Phishme service. - Approximately 15% will be for promotional materials. - Approximately 30% will be for events, classes, speakers etc. ● Second year: $750,000- This will include the cost for implementation of appropriate LMS security modules for contractor employees, and the refresh of new/current employee LMS content. ● Third year: $500,000/yr - This will include refresh for content, security events, speakers, etc.
Human Resources:	2 full-time resources are required (1 cyber security ops + 1 Comm/Marketing team member) . - Consultation from members of the advisory board that represent the organization will be required on an as needed basis. - Volunteers from various teams may also be required for various security awareness events that may take place.
Finalize Plan Date:	TBD
Program Launch Date:	TBD
Project Scope	All company employees will be included. Contractors will be included in next year's project refresh.
Project Goals:	The main goal is to start an official security awareness program. By helping to change employees behavior, overall risk to the organization

	will be reduced.
Project Objectives:	- To maintain compliance standards PCI-DSS, SOX, ISO 2700. - To reduce malware infections due to phishing campaigns. - To increase security awareness for all employees in the organization. - To provide continuous security education and awareness to all employees.
Project Justification	Westworld Intellectual Property and park guest data make it a target for insider/external threats, as well as data breach attempts. Therefore, a new security awareness program will help educate and ensure all employees have the proper tools and knowledge to help protect the organization.
Key Milestones	- Attain a 95% completion of LMS Security Awareness training - Implement a mature simulated Phishing campaign with a goal of 15% susceptibility rate by Q4 of year 1. - Successfully maintain reinforcement training efforts. - Complete at least 83% (10/12 months) of executive briefings for the year. - Receive at least 80% average scores on LMS Security Awareness training.
Assumptions and Constraints:	Assumptions - Having executive level support to help drive the importance of cyber security awareness to the entire organization.This will help ultimately change the culture and behaviors. - Have full time support of project owners to have accountability on hitting all milestones. - Having support of all operation teams to provide metrics to help assess project status. Constraints - Employee time for training. - Budget for maintenance.
Critical Success Factors:	Executive level support.

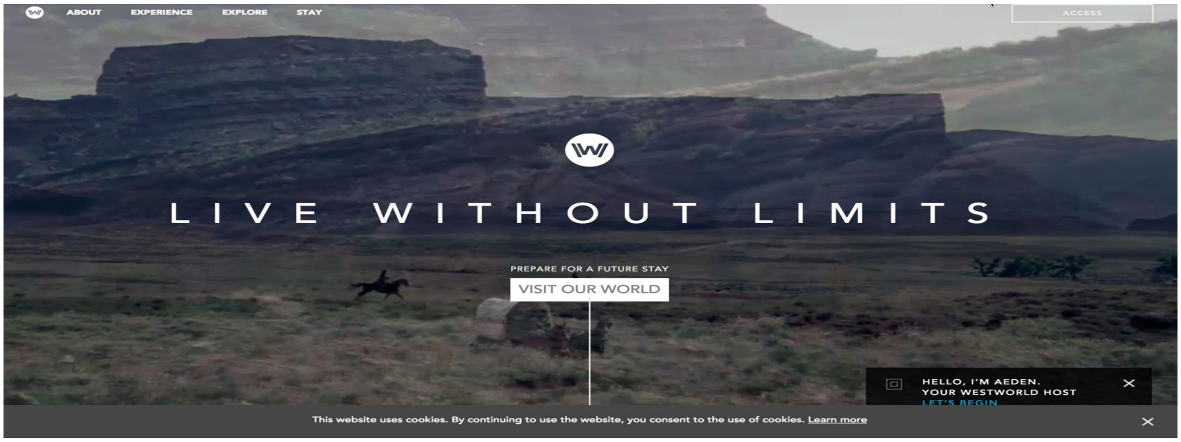
Company Information

Employee breakdown

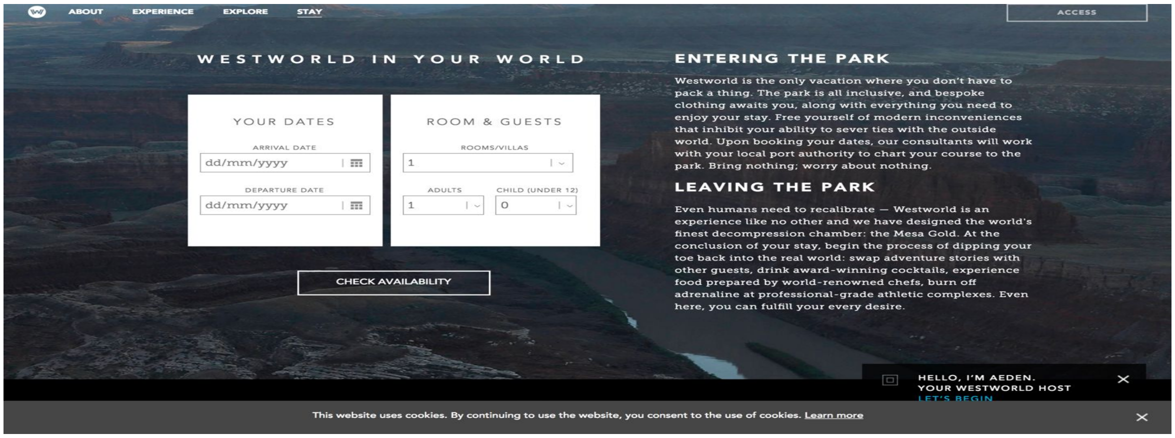
Total Employees	2,127
IT	1,037
Non- IT	850
Other (Contractors, Consultants, etc)	240

WestWorld Park Website Information:

Website: [Discover WestWorld]



This website uses cookies. By continuing to use the website, you consent to the use of cookies. Learn more



YOUR DATES

ARRIVAL DATE: dd/mm/yyyy

DEPARTURE DATE: dd/mm/yyyy

ROOM & GUESTS

ROOMS/VILLAS: 1

ADULTS: 1

CHILD (UNDER 12): 0

ENTERING THE PARK

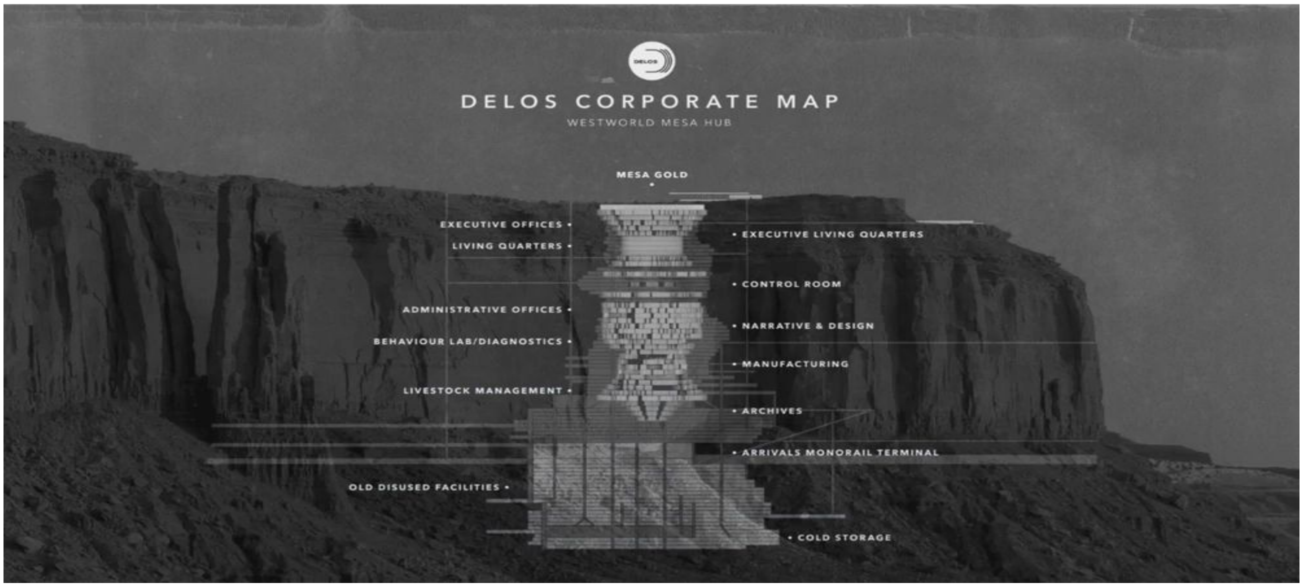
Westworld is the only vacation where you don't have to pack a thing. The park is all inclusive, and bespoke clothing awaits you, along with everything you need to enjoy your stay. Free yourself of modern inconveniences that inhibit your ability to sever ties with the outside world. Upon booking your dates, our consultants will work with your local port authority to chart your course to the park. Bring nothing; worry about nothing.

LEAVING THE PARK

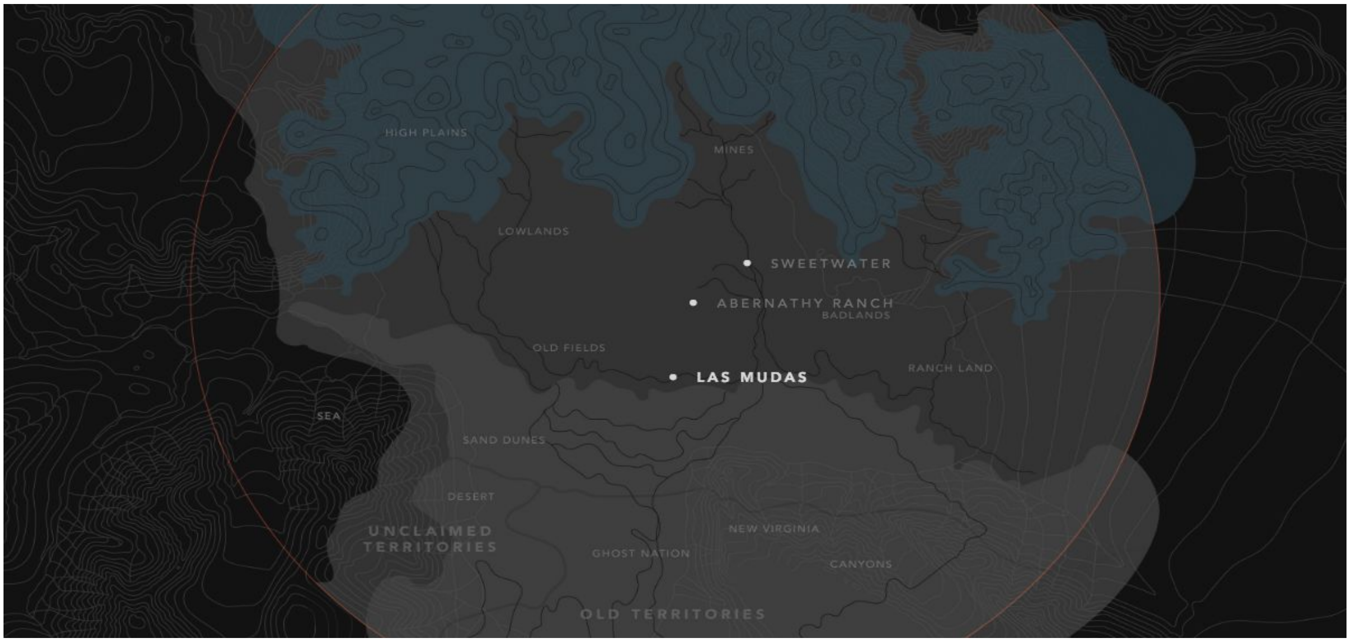
Even humans need to recalibrate — Westworld is an experience like no other and we have designed the world's finest decompression chamber: the Mesa Gold. At the conclusion of your stay, begin the process of dipping your toe back into the real world: swap adventure stories with other guests, drink award-winning cocktails, experience food prepared by world-renowned chefs, burn off adrenaline at professional-grade athletic complexes. Even here, you can fulfill your every desire.

This website uses cookies. By continuing to use the website, you consent to the use of cookies. Learn more

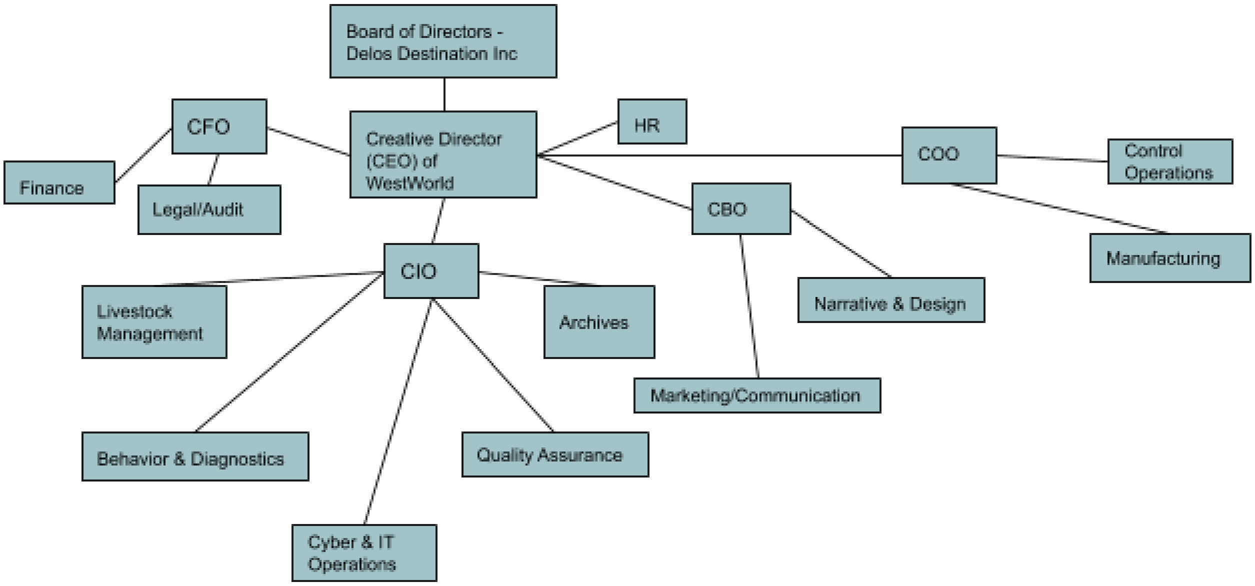
Delos Corporate HQ Map



WestWorld Park Map



Organizational Structure



Department/Role	Description
CEO- Creative Director	The highest ranked position within WestWorld. Responsible for the overall management within the organization. Position is currently held by a co-creator.
C-Level Suite (CFO,CIO,COO,CBO)	The most senior level executives within the organization in addition to the CEO. These executives lead a variety of initiatives such as Finance, Information Technology, Operations, and Branding.
Legal/Audit	This department works to maintain and prevent any legal issues that may arise for the organization.
Finance	The department is responsible for planning, organizing, auditing, and controlling the company's finances.

Quality Assurance	This department does final program testing to ensure that all hosts meet organizational requirements before being placed in park production.
Control Operations	The department that maintains physical security of both the corporate office and the park.
Cyber Security Operations	The department that maintains and oversees the cyber security of Westworld. They works to prevent, detect, and analyze a variety of security incidents
IT Operations	The department that maintains and oversees the overall health, and improvement opportunities for both physical and virtual systems within the organization.
HR	The department that establishes and maintains all employee resources.
Marketing/Communication	The department that drives the promotion and branding of the park. As well as all organization communication.
Narrative/Design	The department that creates the narratives and scripts that are used by the host within the park.
Behavior/Diagnostics	This department works to develop and maintain the code used in the AI host.
Manufacturing	The department that handles the building and production of the host.
Archives	The department that maintains proprietary sensitive data, and legacy hosts.
Livestock Management	The department that manages and maintains the host physical conditions.

Current Management Support Matrix

This section shows our current management support and target management support following project completion.

Name	Current Commitment Level	Target Commitment Level	Engagement Strategies
CEO	Medium	High	Provide executive level briefings to review program success and challenges. Keep briefings short.
CIO	High	High	Will be the executive sponsor of the project. Will assign a department to own project. Will need to show success with the program, and have adequate metrics.
Head of Behavior & Diagnostics Division	Medium	High	Will need to show the value of the program for security of intellectual property.
Head of Narrative & Design Division	Low	Medium	This group focuses on the storyline used within the company park. Engagement strategy will need to show the value of the program for security of their written work which is considered intellectual property.
Head of Cyber Operations	Medium	High	This group will be an important factor to the program and will be vital providing cyber security expertise. One of their team members will be a project co-owner to help drive the program.
Head of Legal	Medium	High	Will need to show the value of the program for compliance requirements.
Head of Control Operations	Blocker	Medium	This group's current commitment is in blocker status because they work in their physical security space. They believe the physical security of the organization is top notch and

			does not need to be included in the project. We will engage this team as experts in the physical security space.
Head of HR	Low	High	Will need to show the value of the program for educating employees on policies.
Head of Marketing/Communications	Medium	High	This group will be an important factor to the program and will be vital in helping identify the best way to reach the employees. One of their team members will be a project co-owner on this project.

Advisory Board

This advisory board is made of a variety of team members from several departments within the organization.

Name	Department	Email Address	Reason for Being on Steering Committee
Bernard Lowe	Head of Behavior and Diagnostics	Benard.Lowe@delos.com	Holds a leadership position within the organization and will be a cavelair for promoting the program. Provides executive level perspective.
Felix Luxe	Livestock Management	Felix.Luxe@delos.com	Will represent a portion of our technical department.
Mary Woodson	Human Resources	Mary.Woodson@delos.com	Will provide guidance on ensuring training follows policy.
Shannon Woodard	Behavior and Diagnostics	Shannon.Woodard@delos.com	Will represent a portion of our technical department.
Angela Donalds	Marketing/Comm.	Angela.Donalds@delos.com	Will help with the creative aspect of security awareness and how to best communicate to the entire company. Will be a co-owner of the project.
Sarah Davids	IT Operations	Sarah.Davids@delos.com	Represents a portion of our technical team specifically IT Operations. Will be vital in helping with getting new modules in the LMS system.
Perry Samuels	Legal	Perry.Sammuels@delos.com	Represents our legal and audit teams, and will provide guidance on how our security awareness program satisfies our legal and compliance standards and requirements.
Teressa Bacon	Security Operations	Teressa.Bacon@delos.com	Representative for our cyber security operations team. Will be a co-owner of the project.

Who: Defining our Security Awareness Targets

This section will list all target groups we have in the organization by employment group category. The new security awareness program will begin with an approach of creating a baseline security awareness education for everyone. The initial rollout of the project will not include contractors. The contractor employment group will be visited in year 2.

WestWorld has four employment group categories:

- Executive
- Full Time - Non Information Technology
- Full Time - Information Technology
- Full Time - Information Technology - Developers
- Contractors (This group is a mixture of Non-IT and IT team members)

The project will focus on the following target groups in Year 1:

- Executive level
- IT team members (all)
- Non IT team members

Department/Role	Type
CEO- Creative Director	Executive
C-Level Suite (CFO,CIO,COO,CBO)	Executive
Legal/Audit	Non- IT
Finance	Non-IT
Quality Assurance	IT (Developers)
Control Operations	Non-IT
Cyber Security Operations	IT
IT Operations	IT
HR	Non-IT
Marketing/Communication	Non-IT

Narrative/Design	Non-IT
Behavior/Diagnostics	IT
Manufacturing	IT
Archives	IT

Detailed Breakdown of Target Groups

Target: Main Employees

Description: This includes our Executives, Full-time staff IT/Non-IT.

Why: WestWorld innovative technology makes it a target for both internal, and external threats. Regardless of level, this will act as a baseline of security awareness education on understanding how to assist in the continuous security of the company.

Location: Delos, WestWorld Corporate HQ

Unique Requirements: Because of the wide variety of team members in this group. Training must be kept general and non-technical. Also must be kept short to ensure all team members can take value from the training.

Target: Executive

Description: Executive level team members hold the highest level of positions in the organization.

Why: The knowledge and access some of these leaders have made them a target for social engineering (Phishing, specifically whaling attacks).

Location: Delos, WestWorld Corporate HQ

Unique Requirements: Most members of the C-level suite are not extremely technical experts, and have very busy schedules .Training must be concise, yet effective at emphasizing how to protect the organization at the C-level.

Target: IT (All)

Description: The team members of IT build, operate, maintain, and secure the systems of the organization as a whole.

Why: IT members often have access to systems that contain very sensitive data. These team members are considered to have the “keys to the kingdom”.

Location: Delos, WestWorld Corporate HQ

Unique Requirements: IT team members are the most technical team members of the organization. Some IT may not think security awareness education for their systems is necessary because of their expert knowledge. Security awareness education must be presented to them in a way of partnering with them to help secure the organization rather than “teaching” them to secure the organization . Education must also be kept concise, yet effective because of their busy schedules.

What: Identifying Key Human Risk and Behaviors

This section identifies the organization's highest risk and threats to aid in the creation of a training program that will not only help reduce the organization's human risk, but will also help change behavior.

The following sources were used:

- Compliance regulations: PCI-DSS/SOX/ISO 2700
- Internal/External Vulnerability assessments
    - Risk:
        - Over 250 Physical security incidents reported last year.
        - Password audit detected 10% of employees used the same password on multiple accounts, or easily cracked passwords.
- Security Operations Incident reports
    - Risk:
        - Over 975 malware related incidents occurred last year.
        - 60% of malware was due to phishing. A great percentage of the phishing were whaling attempts of C-level leaders.
        - 2 Major security incidents occured last year that caused system availability issues due to DDOS and DOS attempts to park websites.
- Verizon Data Breach Investigation Report (2017)
    - Company Industry Category: Accommodation, Information, Other.
    - Risk: Hacking, DOS,Phishing, Malware
    - Attack type: 96% external, 4% Internal

Defining Risk

Probability

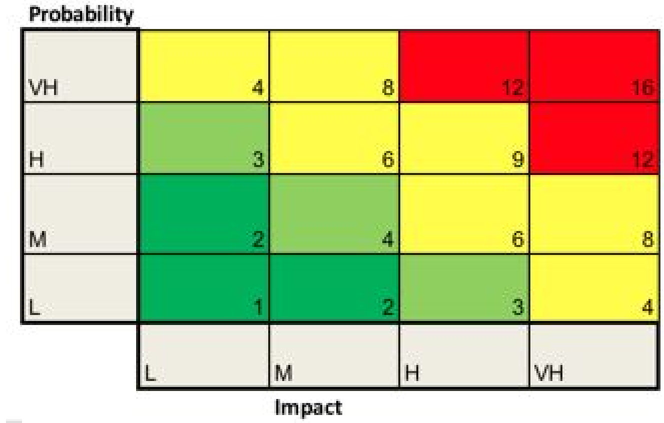
Level	Description
Very High (4)	70% or greater chance of happening in the next 1 months.
High (3)	50% - 70% Chance of happening the next 1 months
Medium (2)	20% - 50% Chance of happening in the next 1 months
Low (1)	20% Less chance of happening in the next 1 months

Impact

Level	Description
Very High (4)	- Loss of Life of park guest or corporate employee due to negligence or accident. - Proprietary data and/or PII data leakage/exposure - Park operation shutdown - Permanent negative reputational damage - Requiring public notification of a breach - Financial loss of $10 million or more
High (3)	- Critical Injury of park guests or corporate employees due to negligence or accident. Hospitalization required and incident report.If corporate employee, 1 week > month time lost from work. - Non proprietary data or PII data leakage/exposure - Financial loss of $1 million - $10 million - Park temporary evacuation < 1 day - Long-term negative reputational impact and public exposure
Medium (2)	- Injury of park guests or corporate employees due to negligence or accident. Requires visit to park clinic and incident report. If a corporate employee, 1 week or less time lost from work. - Financial loss $100k - $ 1 million - Serious negative reputational impact and public exposure - Localized park area evacuation < 1 day
Low (1)	- Minor injury of park guests or corporate employees due to negligence or accident. Requires visit to park clinic and incident report. If a corporate employee, no time lost from work. - Financial loss < $100K - Minimal to no negative reputational impact and public exposure - Localized or individual guest evacuations in a single day < 20

Risk Assessment

Risk Name	Score	Probability	Impact
Data Security	16	4	4
Targeted Attacks	16	4	4
Encryption	12	3	4
Social Engineering (Phishing)	12	4	3
Hacked	9	3	3
Physical Security	9	3	3
Passwords	9	2	4
Cloud	8	2	4



Probability				
VH	4	8	12	16
H	3	6	9	12
M	2	4	6	8
L	1	2	3	4
	L	M	H	VH
	Impact			

Security Awareness Education Modules

The purpose of this section is to specify the goal of each security awareness module.

Legend

E -	(Everyone)
IT -	(IT teams-all)
Exec	(Executives)

Learning Objective	Target Audience
Data Security	E
Targeted Attacks	IT, Exec
Encryption	IT
Social Engineering (Phishing)	E
Malware	IT
Physical Security	E
Passwords	E
Cloud	IT

Learning Objective - Data Security

Target Audience: All four employment groups are included in this training.

Goal:
The goal for this module will be for employees to gain an understanding of the importance of safeguarding company data.

Background: The sensitive data as well as IP the organization maintains has made it a target. All company data must be maintained with the highest precautions. Security incidents within the last year within the organization has proven that security of company data is extremely important.

Learning Objectives:

1. Employees will learn the importance of locking systems that they are no longer actively using.
    a. Individual Metric: Employees will successfully be able to answer multiple end module quiz questions regarding company system lock policy.
    b. Organizational Metric: % of employees who answered quiz questions correctly.
2. Employees will understand how to properly dispose of data no longer needed.
    a. Individual Metrics: Employees will successfully be able to answer end module quiz questions regarding locations within their team area to dispose of data.
    b. Organizational Metric: % of employees who answered quiz questions correctly.
3. Employees will be able to explain the different types of intellectual property (IP).
    a. Individual Metrics: Employees will be given several scenarios involving IP, and will be able to assign the scenario to a specific type of IP (Patent, copyright, trademarks).
    b. Organizational Metric: % of employees who answered quiz questions correctly.

Learning Objective - Targeted Attacks

Target Audience: This training is for all of IT, as well as the company C-level suite (Executives). This training will be slightly technical but is imperative for all employees assigned.

Goal: The goal of this module is for employees to explain, detect, and protect against targeted attacks. Employees will also know how to report suspicious system behavior.

Background: The sensitive data as well as IP the organization maintains has made it a target for APT organizations that seek value in its proprietary data. Multiple security incidents occured in the past year of threat actors attempting to take down and gain access to production systems.

Learning Objective:

1. Employees will be able to explain the definition of advanced persistent threat (APT).
    a. Individual Metrics: Employees will be able to successfully answer the end module quiz question of APT definition.
    b. Organizational Metrics: % of Employees that answer question correctly
2. Employees will be able to explain the definition of C-level fraud.
    a. Individual Metrics: Employees will be able to successfully answer the end module quiz question of C-level fraud definition.
    b. Organizational Metrics: % of Employees that answer question correctly
3. Employees will be able to explain the differences in ddos and dos style attacks.
    a. Individual Metrics: Employees will be able to successfully answer the end module quiz question of DDOS and DOS definition.
    b. Organizational Metrics: % of Employees that answer questions correctly.
4. Employees will know how to report suspicious system activity.
    a. Individual Metrics: Employees will be able to successfully answer the end module quiz question of reporting mechanism.
    b. Organizational Metrics: % of Employees that answer questions correctly. And % of reports received throughout the year for confirmed suspicious activity.

Learning Objective - Social Engineering (Phishing)

Target Audience: All four employment groups are included in this training.

Goal: The goal of this module is to help educate all employees on how to quickly identify emails with malicious intent. As well as ways to report suspicious emails they may receive.

Background: Phishing is one of the top attack vectors for an organization because every organization's biggest threat to security is the employees that have access to the systems. Employees also make an easy target for threat actors.The company has had a huge phishing problem with several incidents occurring confirmed as phishing being the initial threat vector.

Learning Objective

1. Employees will gain an increase in knowledge on how to spot malicious emails.
    a. Individual Metric: User will successfully answer questions on identifying malicious emails in end module quiz.
    b. Organizational Metric: % of employees who answered quiz questions correctly.
2. Employees will understand how to report suspicious emails to the security operations team for review.
    a. Individual Metric: User will successfully answer questions on reporting malicious emails in end module quiz.
    b. Organizational Metric: % of malicious emails reported vs a decrease in % of malware caused by phishing. % of employees who answered quiz questions correctly.
3. Employees will know how to identify the difference between phishing and spam.
    a. Individual metric: Users will successfully answer scenario based questions on phishing vs spam.
    b. Organizational Metric: % of employees who answered quiz questions correctly.

Learning Objective - Encryption

Target Audience: IT(all)

Goal: To explain the basics of what encryption is, and to be able to explain types of data that can be encrypted.

Background: The sensitive data as well as IP the organization maintains has to be encrypted at all times on systems that store it and while in transit.

Learning Objectives

1. Employees will be able to explain the basics of data encryption.
    a. Individual Metric: Employees will be able to successfully answer multiple end module quiz questions regarding what encryption is and why it's important.
    b. Organization Metric: % of employees who answered quiz questions correctly.
2. Employees will be able to identify types of data that can be encrypted.
    a. Individual Metric: Employees will be able to successfully answer multiple end module quiz questions regarding which data types can be encrypted.
    b. Organization Metric: % of employees who answered quiz questions correctly.
3. Employees will gain the knowledge to be able to encrypt data at rest or for transit.
    a. Individual Metric: Employees will be able to successfully answer multiple end module quiz questions regarding setting up PGP keys and encrypting data prior to transport.
    b. Organization Metric: % of employees who answered quiz questions correctly.

Learning Objective - Hacked

Target Audience: IT

Goal: For employees to understand the company security incident response reporting process. Understanding the different types of malware and how to report any suspicious activity.

Background: The sensitive data as well as IP the organization maintains has made it a target for threat actors that seek value in its proprietary data. Multiple security incidents occured in the past year of threat actors attempting to take down and gain access to production systems.

Learning Objectives

1. Employees will be able to define the different types of malware (trojan, worm, rootkit, ransomware etc.)
   a. Individual Metric: Employees will be able to successfully answer multiple end module quiz questions regarding malware types.
   b. Organization Metric: % of employees who answered quiz questions correctly.
2. Employees will know how to report any suspicious activity to the cyber security team.
   a. Individual Metric: Employees will be able to successfully answer end module quiz questions regarding communicating with their cyber security team.
   b. Organization Metric: % of employees who answered quiz questions correctly.

Learning Objective - Physical Security

Target Audience: Everyone

Goal: To explain how physical security is an important first step in protecting company data, networks, facilities, personnel, and guests.

Background: There have been several instances in the company past where employees were in restricted areas without proper approval. The company is working to implement additional badged accessed turnstyles to prevent tailgating. This training will be supplemental to the physical security measures already taken by the company.

Learning Objectives

1. Employees will be able to identify items that help maintain physical security.
   a. Individual Metric: Employees will be able to successfully answer multiple end module quiz questions regarding common physical security items (CCTV, RFID tags, physical access, etc)
   b. Organization Metric: % of employees who answered quiz questions correctly.
2. Employees will know the process and policy of accompanying guests.
   a. Individual Metric: Employees will be able to successfully answer multiple end module quiz questions regarding the process of having visitors.
   b. Organization Metric: % of employees who answered quiz questions correctly.
3. Employees will be able to explain the importance of physical security
   a. Individual Metric: Employees will be able to successfully answer multiple end module quiz questions regarding the importance of physical security.
   b. Organization Metric: % of employees who answered quiz questions correctly.
4. Employees will know how to properly identify badge colors and area access.
   a. Individual Metric: Employees will be able to successfully answer multiple end module quiz questions regarding badge and access types according to company policy.
   b. Organization Metric: % of employees who answered quiz questions correctly.

Learning Objective - Passwords

Target Audience: All four employment groups are included in this training.

Background: Passwords are often the first line of defense for any organization. The company shows history through vulnerability testing a high use of easy to guess passwords.

Goal: The goal of this module is to educate users on how to create complex passwords but also tips on how to remember them. Putting emphasis on passphrases, rather than standard passwords with mixed characters, numbers, and symbols.

Learning Objectives

1. Employees will learn how to create passphrases that are hard for attackers to guess.
    a. Individual Metric: In CBT training, the employee will be asked to create a couple of mock passwords to pass policy not using common password tactics.
    b. Organizational Metric: External pentest will be conducted every 6 months, and will attempt to password crap a sample of employee credentials.
2. Employees will be able to explain what defines two-factor authentication.
    a. Individual Metric: The employee will be able to answer CBT training quiz questions on the different types of authentication (Something you know, something you have, something you are -biometrics).
    b. Organizational Metric: Assesses the amount of systems utilizing multi-factor authentication every 6 months. Increase implementation of more systems that are two-factor(multi factor), with a goal to make 95% of systems multifactor in 3 years.
3. Employees will learn the importance of not reusing passwords for multiple accounts.
    a. Individual Metric: The employee will be able to answer CBT training quiz questions on password management.
    b. Organizational metric: External pentest will be conducted every 6 months, and will attempt to password crack a sample of employee credentials. Pentester will attempt to crack additional employee accounts with the same passwords.

Learning Objective - Cloud

Target Audience: IT(all)

Background: Oftentimes members of our IT staff use cloud services to share and collaborate on projects. Many instances in the company's past, vulnerability testing has discovered unauthorized applications have been installed on company resources that were cloud services.

Goal: The goal of this module is to educate users on what the cloud is, and how users can reduce company risk by only using authorized cloud services.

Learning Objectives

1. Employees will be able to explain and define what the cloud is.
    a. Individual Metric: The employee will be able to answer CBT training quiz questions on what makes the cloud.
    b. Organizational metric: % of employees who answered quiz questions correctly.
2. Employees will be able to explain why there is risk with using cloud providers, specifically unauthorized ones.
    a. Individual Metric: The employee will be able to answer CBT training quiz questions on cloud usage risk.
    b. Organizational metric: % of employees who answered quiz questions correctly.
3. Employees will learn about company authorized cloud services, and how to get to them.
    a. Individual Metric: The employee will be able to answer CBT training quiz questions on company approved cloud providers.
    b. Organizational metric: % of employees who answered quiz questions correctly. % of users that use the company cloud service provider.

How: Program Communication

Why Does Cyber Security Matter?

To an organization such as WestWorld who has created some of the world’s most innovative technology in Artificial Intelligence. All employees must work together to help protect all data the organization maintains. The data must be protected to help prevent the technology from getting into the possession of anyone who would want to use it for harm. This includes but is not limited to intellectual property and PII data for both employees, and park guests.

Culture Analysis and Localization Requirements

Despite the family fun nature the park has for park guests. The corporate culture is much more conservative because of the type of data and intellectual property the organization maintains. All employment is contingent upon prospective employees successfully completing a rigorous background check similar to government level clearance checks.. Following the background check, all employees must complete a 3-week long orientation at Headquarters.

All team members speak the English language, therefore all training will be delivered in English.

Branding

The following images will be used for branding purposes for the new security awareness campaign. The will be used on the LMS, brochures, clothing, and all other security awareness marketing materials.

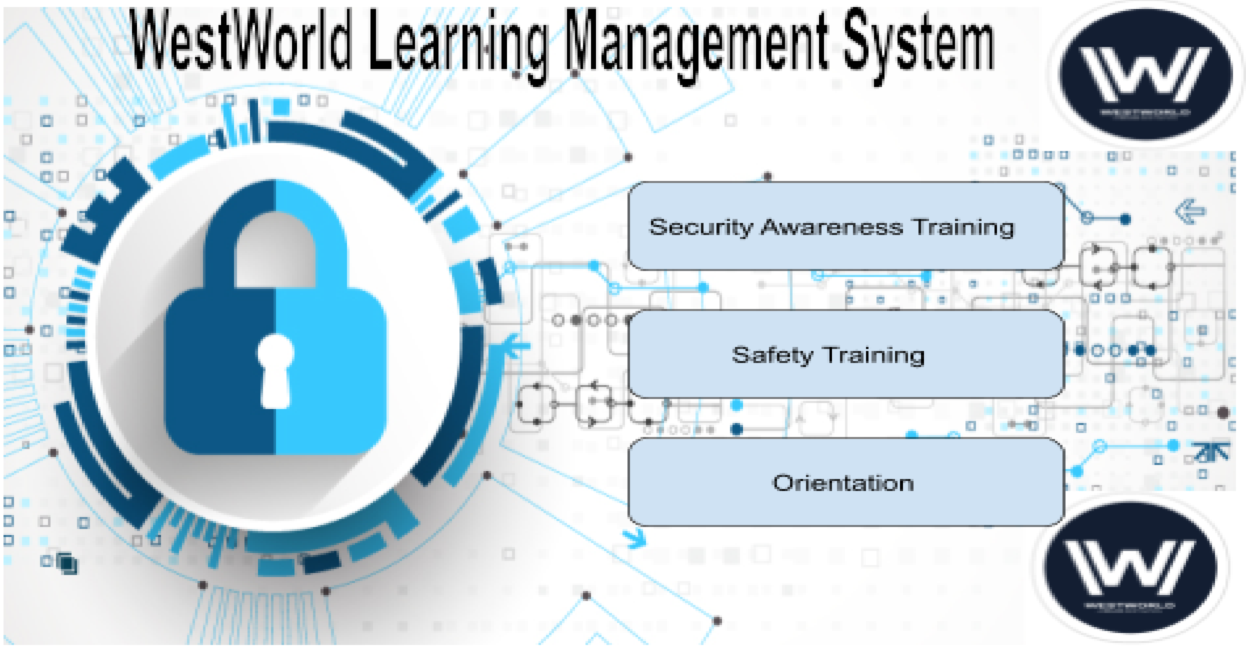
WESTWORLD
A DELOS DESTINATION

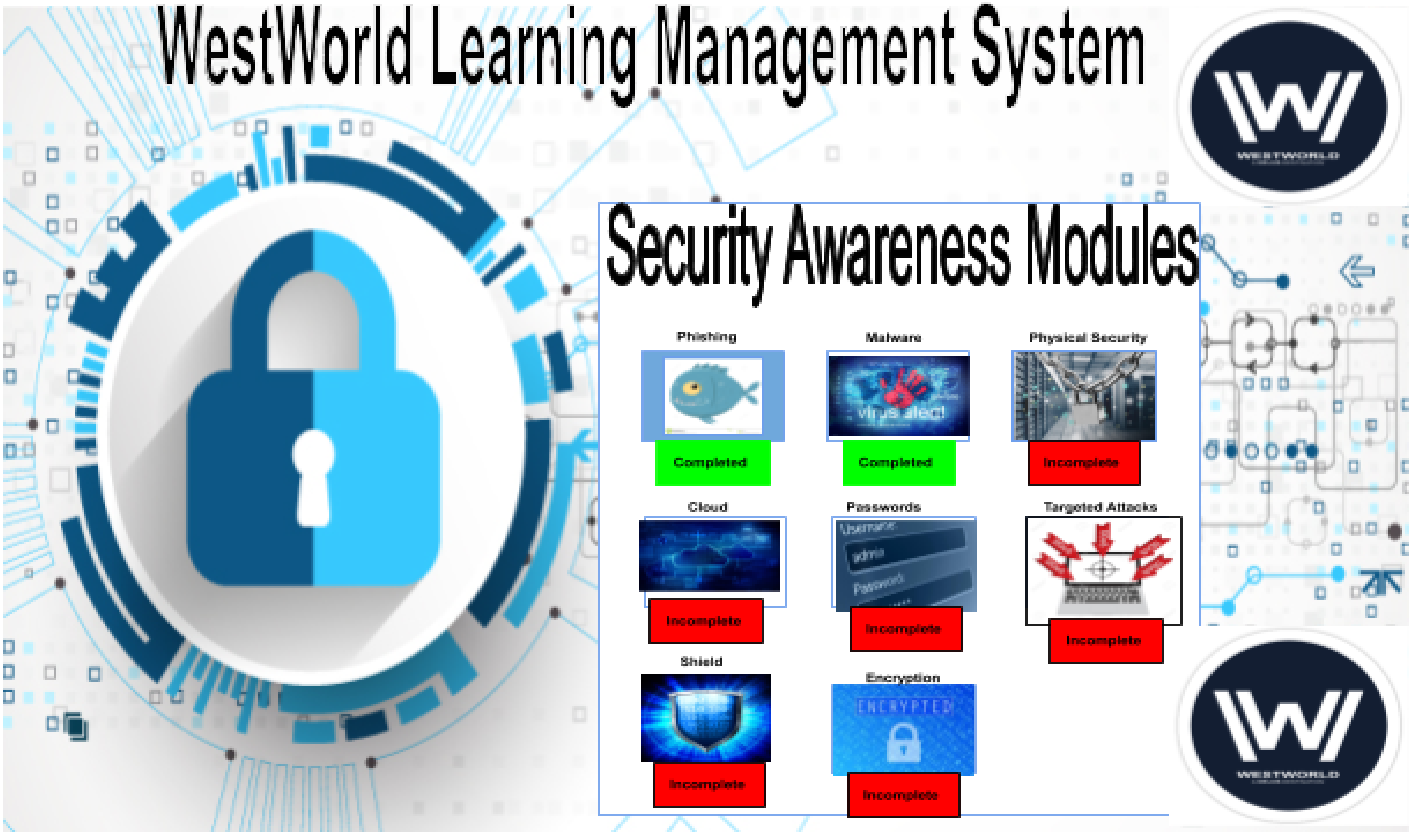
Confidential Data
[Identify Person]
Personal Data
Name
Home Address
Business Address
Identity Card No
Passport No
Driving License
Income Tax No
Car Registration
Other

CBT - WestWorld LMS Communication

The first image is the main screen of WestWorld's LMS system, in which an employee will have to select Security Awareness Training to get to new security awareness modules.

The second image shows the security awareness training screen and all modules available.


WestWorld Learning Management System
Security Awareness Training
Safety Training
Orientation



Initial Program Communication

Below outlines an initial communication plan of the new program for both new and current employees.

Employee Type	LMS- Security Awareness Module	Lunch and Learn/ Instructor based training Opportunities.	Simulated Phishing	Reinforcement Training.

New Employees	During orientation, all new employees will be given a demo and an information packet on how to use the WestWorld Learning Management System (LMS) for Training. The demo will unveil the new modules added for security awareness.	- Orientation -onboarding plan. -Calendar of upcoming company events.	- Orientation -onboarding plan. -Calendar of upcoming company events.	- Orientation -onboarding plan. -Calendar of upcoming company events.
Current Employees	All current employees will be made aware of the new security awareness module in the company's LMS by their manager. Since current employees already have knowledge of how to use the LMS, they will be sent the information packet on the specific security awareness training via email.	- Calendar of upcoming company events. - Management reminder. -Intranet page announcements.	- Calendar of upcoming company events. - Management reminder. -Intranet page announcements.	- Calendar of upcoming company events. - Management reminder. -Intranet page announcements.

Primary Training

Below outlines the primary training, a description, and company policy regarding training completion.

Event/Item	Description	Requirement type from policy

CBT - WestWorld LMS	This computer based training will have modules on the company’s highest cyber security risk. It will exist in the company’s current LMS system, and will be maintained and refreshed by the company’s IT,IT Security, and Communications team. The training will be refreshed yearly by representatives of each of those teams mentioned above. Duration: Each module will take 20 min or less. Survey: Quiz following each module	Must be completed annually by all employees within 3 weeks of email notification. Modules to be completed will depend on employee role/department. ● Incomplete 1 week following due date - Warning and notification to manager ● Incomplete within 2 weeks - required meeting with manager. ● Incomplete within 3 week - Employee will meet with manager and HR and face possible write up. Will be required to complete and sign up for additional training opportunities. **Four total write ups mandate automatic termination from the company.**
Lunch and Learn/ Instructor based training Opportunities.	Several times a quarter the organization will offer several training sessions to discuss topics on cyber security or company security during lunch. The training will be given by Instructors or IT employees. Duration: 30 min -45 min Survey: As each employee enters the area of the talk, they will be given a survey to fill out and hand in at each talk/session conclusion.	All employees that are not executives will be required to attend at least one session a quarter. ● Missed quarterly requirement - Warning sent, and required to attend an additional session the following quarter. ● Failure to make up missed quarter lunch and learn session - notification sent to manager, manager meeting, and required to attend two additional sessions the following quarter. ● Failure to make up multiple quarter sessions - Employee will meet with manager and HR and face possible write up. **Four total write ups mandate automatic termination from the company.**
PhishMe - Simulated Phishing campaigns	Quarterly members of the IT team will conduct simulated phishing campaigns for all employees. If the user does interact with the campaign. They will be sent to a	● If user clicks on phishing two quarters in a row - Warning sent to both user and manager. Employees are required to attend an additional Lunch and Learn/ ILT session in the current quarter.

	security awareness splash page on how to detect phishing in the future. Duration: Ongoing, once a quarter. Survey: Phishing system will provide metrics of users that were susceptible to phishing.	● If a user clicks on phishing three quarters in a row - notification sent to manager, and manager meeting is required. An additional Lunch and Learn/ ILT session must be completed in the current quarter. And a user must complete the phising module in the company's LMS system again. ● If a user clicks on phishing four quarters in a row - employee will meet with HR and manager and face possible write-up.
Monthly Executive Security briefings.	Once a month executives will have a similar session to the lunch and learn/ ILT. Their sessions will discuss current threat landscape and current security metrics for the organization. Hosted by the CEO and other members of the c-suite. Duration: 30 min < Survey: n/a	n/a

Reinforcement Communication

Event/Item	Description	Requirement type
Monthly newsletter	Every month the organization will send out a newsletter on tips and ways to help protect the employee and the company. The newsletter will also talk about all company statistics regarding security and upcoming events .	n/a

Cyber Security awareness month	Cybersecurity awareness month is every October. During the month of October the company will host guest speakers and have various talks and events promoting security and security awareness.	n/a

Long-Term Sustainment

	Description
Employee Feedback	Once a year employees are given a survey regarding views on several topics within the company. 3-4 questions will be added to that survey regarding the employees views on security training, security awareness, and the organization's overall security stance. Promotion will begin in October for cyber security awareness month. Announcements/reminders will be made in the newsletters. **When:** Yearly - November every year. **Requirement:** 2 weeks to complete, team manager enforcement completion. **Goal:** 75% completion of all employees in year 1.
Advisory board Meetings	The advisory board will hold monthly or bi-weekly meetings to discuss current metrics and training improvements for the following year.
Executive Level Meetings	Executives host monthly briefings in which they discuss security. They will also host a yearly security summit in which they review employee feedback, and metrics for current year and how to improve the following year.

Security Awareness Metrics

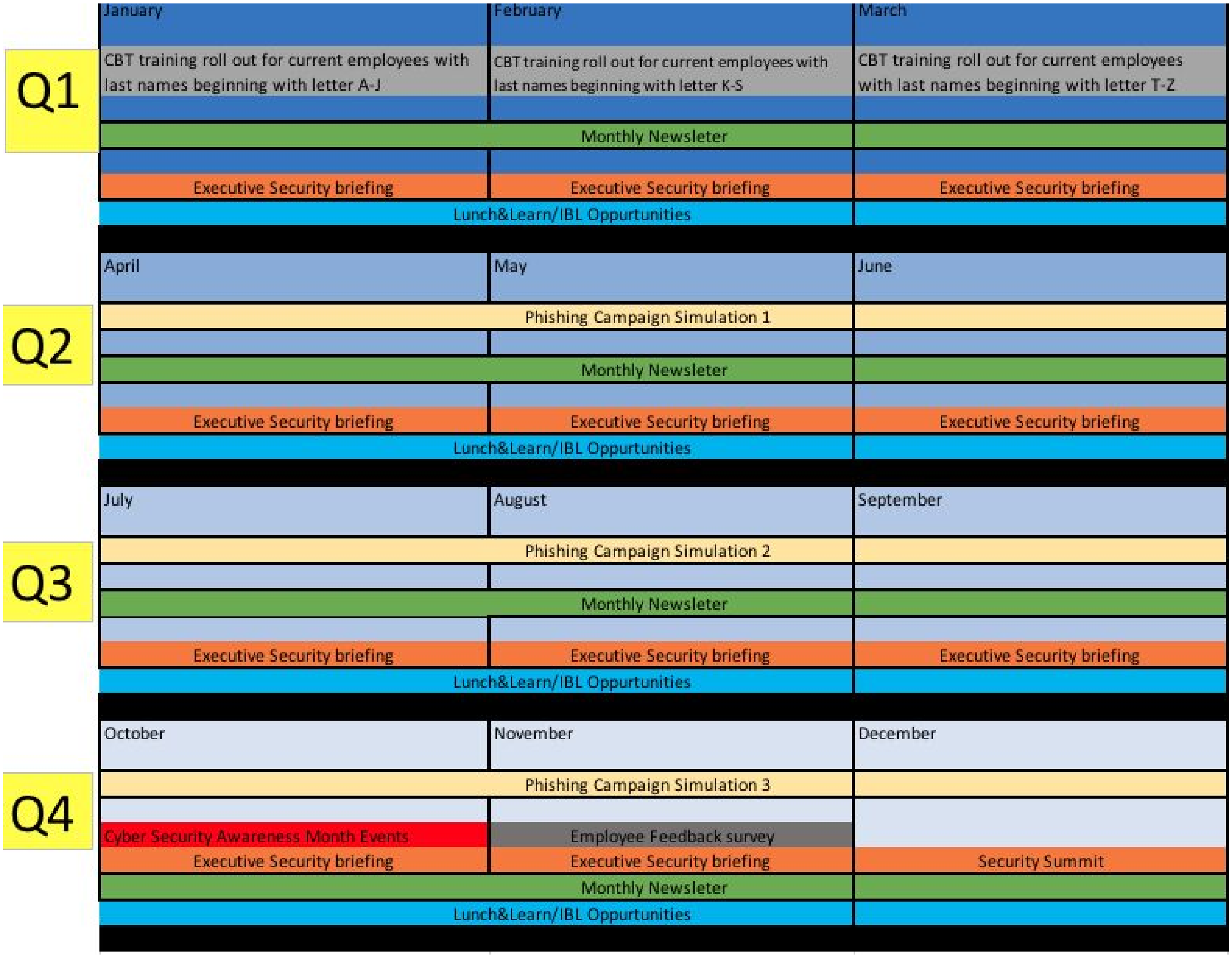
Below is an outline of metrics that will be gathered for the security awareness program.
*Type - Compliance (c) ; Impact (I)

Metric	What is Measured?	How is it Measur	When is it Measured?	Who Measures?	Details	Type

		ed?				
LMS-Security Awareness Module training completion	Average quiz scores for modules Amount of Users that have completed the training Amount of users that have not completed the training.	LMS system statistics.	Annually	LMS management team reports metrics to security awareness program owners.	This is a part of our primary training that will be completed once a year by all employees. Modules are assigned by the employee department.	C/I
Phishing	Amount of users that were susceptible to the simulated phishing.	PhishMe Reporter	Quarterly	Security Awareness team member responsible for Phishing.	This is a part of our primary training that will be completed once a quarter led by the security team for all employees.	I
Passwords	Internal/external pentest results for password audit.	External /Internal Pentest.	Every 4 months / Every 6 months.	External/Internal pentest teams.	This is a part of our primary training that will be completed once a quarter led by the security team for all employees.	I
Lunch & Learn/ IBT	Amount of users attending sessions Amount of users completing end of session surveys. Session survey % of favorable reviews vs not favorable reviews.	Session surveys data.	Quarterly	Session moderator/ Volunteer.	This is a part of our reinforcement training opportunities that all employees must participate in throughout the year according to company policy.	I
Monthly Newsletter	% of times a monthly newsletter is downloaded. % of times monthly newsletter is viewed by employees.	Files server statistics.	Monthly	IT Operations report metrics to security awareness program owners.	This is a part of our reinforcement training given to all employees monthly on different cyber security topics.	I

Security Awareness Plan Timeline

Below is a timeline of the security awareness project and highlighted events.



Q1	January	February	March
	CBT training roll out for current employees with last names beginning with letter A-J	CBT training roll out for current employees with last names beginning with letter K-S	CBT training roll out for current employees with last names beginning with letter T-Z
	Monthly Newsleter		
	Executive Security briefing	Executive Security briefing	Executive Security briefing
	Lunch&Learn/IBL Oppurtunities		
Q2	April	May	June
	Phishing Campaign Simulation 1		
	Monthly Newsleter		
	Executive Security briefing	Executive Security briefing	Executive Security briefing
	Lunch&Learn/IBL Oppurtunities		
Q3	July	August	September
	Phishing Campaign Simulation 2		
	Monthly Newsleter		
	Executive Security briefing	Executive Security briefing	Executive Security briefing
	Lunch&Learn/IBL Oppurtunities		
Q4	October	November	December
	Phishing Campaign Simulation 3		
	Cyber Security Awareness Month Events	Employee Feedback survey	
	Executive Security briefing	Executive Security briefing	Security Summit
	Monthly Newsleter		
	Lunch&Learn/IBL Oppurtunities		