State of Oregon Information Security Awareness & Training

2021 PROGRAM PLAN

Table of Contents

1. Executive Summary

The Enterprise Information Services (EIS) Cyber Security Services (CSS) shall develop, maintain, and implement the enterprise Information Security Awareness and Training Program. The State of Oregon Information Security Awareness and Training Program (hereinafter referred to as awareness program) shall include the following:

Annual Information Security Training

Scheduled and unscheduled awareness assessments and activities (for example, phishing exercises)

Additional training related to protecting state information assets and systems

The awareness program is a continuous effort to educate and empower the state’s workforce to adopt good security habits at work, at home and while mobile with awareness and targeted training to address specific roles and risks. The industry has increasingly come to an understanding that people are at least as important as technology and probably more important when it comes to protecting information assets. The goal of the awareness program is to reduce human vulnerabilities that could result in a breach of confidentiality, integrity, and availability of state information assets, thereby increasing the overall security posture of the state.

The awareness program applies to all Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 276A.300 and OAR 125-800 and as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

The state’s policy is that all state employees, contractors, and third party personnel accessing state information assets must receive cybersecurity and information security awareness training as a condition of access to state information assets.

The overall strategy of the awareness program is one of positive engagement, providing training that people want to take to help them not only at work, but in their personal lives. The awareness program is led by our Information Security Awareness and Training Program Coordinator and guided by a dedicated advisory board with the support and backing of the EIS Governance, Risk and Compliance Director.

2. Guidance

An effective awareness program requires input and support from more than just the security organization. The Information Security Awareness and Training Advisory Board (hereinafter referred to as the advisory board) was formed to guide the execution of the awareness program, through shaping the guiding principles, generating support throughout the enterprise, and being ambassadors for the cultural change this program is designed to achieve.

The advisory board is a cross-agency, cross-functional team, with key members representing a variety of our key business, roles and operational streams. The group meets as needed to discuss cyber security events, challenges, improvement opportunities, and metrics.

3. Who

The first step in building a mature security awareness program is to identify whose behaviors we want to change. Different groups have different risks, roles, and data that they handle. As such, the type, frequency, and modality of each group’s training should differ to ensure we have maximum impact for each group.

The current target audience for the awareness program is divided into two groups: enterprise workforce (all staff, contractors, board/commission members, and volunteers) and role based users (are included in the workforce but have additional access to sensitive information). Both groups will receive baseline security training and reinforcement material throughout the year that will cover a number of security topics that every staff member should understand.

The first group to be targeted in our program is the enterprise workforce. This group is required to complete the DAS-EIS Information Security Training on an annual basis. They will also receive monthly reinforcement materials, disseminated through their leadership, and participate in the EIS/CSS Phishing Awareness program.

We will continue to evaluate progress and when training for this group has been firmly established, we will then consider next steps for targeting role based users.

3.1. Target Group 1: Workforce

Target Group 1: All Staff / Contractors / Vendors / Board/Commission Members / Volunteers	
Description	Anyone in the enterprise that has access to state information assets or acts on behalf of a state agency.
Why:	Security awareness is a foundation to reducing risk. Therefore, all workforce members are required to complete annual training, will receive additional reinforcement training and will participate in various security awareness programs throughout the year as directed by the OSCIO.
Location	On-line and in-person.
Unique Requirements	None.
When	Continuously.

3.2. Target Group 2: Role Based Users

Target Group 2: Information Technology / Executives / HR / Budget / Contractors etc.	
Description	Any individual who has been granted additional access to systems and have elevated authority compared to the average user
Why	Role based users add an additional layer of risk due to their elevated authority and access to systems. They require additional, more specific training based on the technologies and sensitive information that they work with. Agencies are responsible for assigning role based training for the appropriate users.
Location	On-line.
Unique Requirements	This staff has elevated access to systems and data.
When	Additional training will be conducted periodically.

4. What

4.1. Methodology

Our goal is to focus on the smallest number of topics (human risks) possible that represent the greatest risk to the enterprise. The fewer human risks we focus on the more likely we will effectively change the required behaviors and manage human risk to our organization. In addition to managing human risk, several topics are also required for compliance or legal reasons.

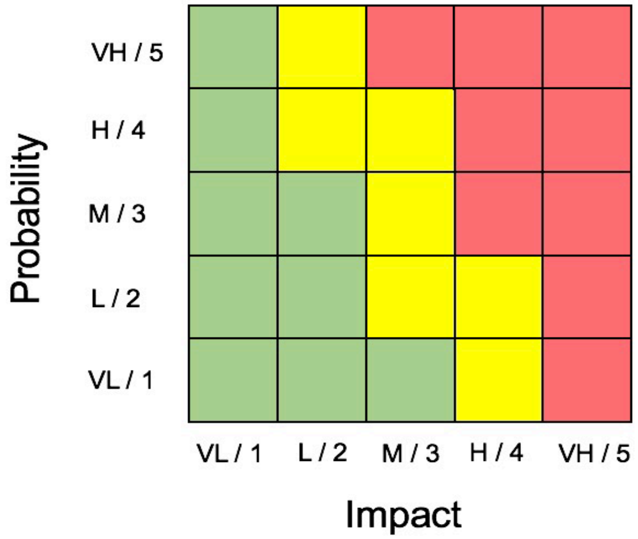
The awareness program utilizes multiple sources when identifying topics and creating awareness and training content. Training will be focused on reducing human vulnerabilities by helping employees learn how to mitigate risky behavior. Sources include, but are not limited to:

1. Results of security assessments and penetration tests.
2. Number and types of security incidents.
3. Advisory Board guidance.
4. Regulation, laws and compliance requirements.
5. Security breaches experienced by other organizations and industries.
6. Responses to surveys.

4.2. Risk Prioritization Process

To identify and prioritize the top human risks to our organization, we use a qualitative review process. While a qualitative assessment is not as precise or accurate as a quantitative approach, it is good enough in that we only need to identify our highest risks so we know what to prioritize and focus on. These are residual risk ratings; by residual we mean we take into account all existing technical controls and other security-related controls and training programs. Risk is defined as the probability of the event times the impact of the event. Below is an example of the qualitative heat map we use for prioritization.

Human Risks / Topics	Probability	Impact	Risk Score
Example Risk	Very High	Medium	High
Example Risk	5	3	15



Probability	VL / 1	L / 2	M / 3	H / 4	VH / 5
VH / 5	🟩	🟨	🟥	🟥	🟥
H / 4	🟩	🟨	🟨	🟥	🟥
M / 3	🟩	🟩	🟨	🟥	🟥
L / 2	🟩	🟩	🟨	🟨	🟥
VL / 1	🟩	🟩	🟩	🟨	🟥

Impact

5. How

5.1. Why Security Matters

To be successful, we must first engage the people. The first step is to ensure people believe in the value of security, why it matters to them, and what our ultimate goal is. We will communicate this on two levels:

- **Organizational:** As employees of the State of Oregon we are tasked with protecting the data in our care. The security and integrity of our organization is of the utmost importance. We will ensure that people understand that cyber is now the greatest risk to our organization and their behaviors can impact the lives of residents across the state.

- **Individual:** Our training will emphasize that what people learn not only protects them at work, but also protects them at home and in their personal lives. Our intent is to not only engage people at a personal level, but also change how they act by exhibiting the same secure behaviors at home. Ultimately, security becomes part of people’s culture.

5.2. Awareness & Training Content

A. Annual Training

Per the Department of Administrative Services (DAS) Statewide Employee Training policy 10.040.01, all users who have access to State information assets are required to complete annual computer-based training through the state’s Learning Management System (LMS).

The goal of the annual training is to provide foundational information security training for the state’s workforce and to ensure compliance. The due date of the annual training is December 31, 2021.

Managers are responsible for ensuring their employees have completed the training by the required due date.

Agencies whose workforce are unable to complete the annual training using the Oregon state government LMS of record should follow the *Information Security Annual Training – Alternative Request Information* instructions located at: https://www.oregon.gov/das/OSCIO/Pages/Securityresources-ag.aspx

B. Reinforcement Training

We understand and recognize that training people annually is not enough to change human behavior and reduce organizational risk. As a result, the awareness program will continuously reinforce key behaviors by utilizing various methods throughout the year. The reinforcement training consists of the following:

1. Monthly videos: Dissemination of awareness videos to the state workforce at least monthly. The videos will be distributed by email to agency leadership and made available to all employees.
2. Digital Signage: Create and distribute monthly security awareness posters. The posters will be distributed by email with instructions to print in multiple sizes to agency leadership and made available to all employees. We encourage organizations to print hard copies and hang in conspicuous areas.

C. Phishing Awareness Program (see EIS Phishing Awareness Program Expectations)

What is phishing?

"Phishing" is a social engineering attack using email or a messaging service to send messages intended to trick individuals into taking an action, such as clicking on a link, opening an attachment, or providing information. Phishing remains the number one attack vector for cybercriminals because it often leads to success. Oregon state government employees are a target because they have access to sensitive and confidential information and access to information systems.

What is a phishing awareness program?

A phishing awareness program, also known as a phishing simulation program, phishing assessment program or self-phishing, is a customizable training and awareness program used by security awareness professionals in various industries. This program allows organizations to simulate phishing emails that can be sent to their end users. Conducting these types of social engineering attack simulations helps identify which end users or programs are responsive and provides the opportunity for more focused training opportunities to help reduce organizational risk.

Strategy and Concept

All employees will receive phishing simulation emails that resemble real phishing attacks. They will be delivered monthly at various intervals.

Employees will continue to follow their organizations process if they believe they've received a real or simulated phishing email.

5.3. New Hires

DAS Statewide Employee Training policy 10.040.01 also requires all new employees to complete the computer-based training within 30 days of receiving access to the LMS. New employees will not need to complete the annual training if they completed the new employee training within the same calendar year.

6. Long-Term Sustainment

The awareness program will continuously be updated to stay current with evolving threats and to ensure behavioral change over time.

The awareness program will be updated yearly using the following data sources:

1. Emergent security incidents or unusual events observed during the previous year.
2. Security incidents experienced by the public and specific risks that have been identified.
3. Result of feedback surveys and assessments.

7. Metrics

It is important to test and measure if we are effectively educating users and changing their behaviors. The awareness program will focus on the following two metric categories for measuring the effectiveness and impact of the security awareness program. Results will be communicated to the advisory board, Information Security Council (ISC) and EIS leadership in an annual report.

7.1. Compliance Metrics

We track the following activities to ensure we meet compliance standards. These metrics track and measure what we are doing, not the impact.

Metric Name	What is Measured?	How?	Who?	Frequency
Annual Training Completion %	% of staff that have completed the required annual training	Completion reports from LMS	Security Awareness Program	Quarterly
Annual Training Completion #	# of staff that have completed the required annual training out of the total number of staff	Completion reports from LMS	Security Awareness Program	Annually

7.2. Impact Metrics

The goal of impact metrics is to measure the impact we are having. By impact, we mean either the behaviors of our workforces or their attitudes and beliefs toward security. These metrics were selected as they measure the greatest risk to our organization.

Metric Name	What is Measured?	How?	Who?	Frequency
Phishing - phish prone percentage	% of people that clicked on phishing simulations	Report from phishing tool	Security Awareness Program	Quarterly
Phishing – Reporting	% of people who detect and report phishing simulation (real and simulation)	Agency IT help desk metrics and/or Report from Phish Alert button	Security Awareness Program	Quarterly
Phishing – Repeat Responders	% of workforce that repeatedly fall victim to phishing simulations. These individuals are not changing behavior and represent a high risk.	Report from phishing tool	Security Awareness Program	Quarterly
Reinforcement Engagement	Number of monthly awareness video views	Report from LMS & YouTube	Security Awareness Program	Quarterly
Security Culture - Workforce attitudes towards security	Does the workforce understand the need for security, the important role they play, and support the behaviors needed?	Will collect results from cultural survey	Security Awareness Program	Annually

8. Key Dates and Milestones

The following is the general outline of key dates and milestones. See individual project plans for specific project dates.

1. January 1 – Post annual monthly reinforcement topics timeline on external website
2. January 1 – Annual training live on LMS
3. June (coincides with WDL date) – Annual training assigned to all staff not including agencies with an alternate delivery date (coordinated with the iLearn helpdesk) or prior 2021 completions.
4. December 31 – completion deadline for annual training not including agencies with an alternate delivery date (coordinated with the iLearn helpdesk)
5. Continuous / monthly – Phishing simulation sent to all staff participating in the EIS Phishing Awareness Program
6. Quarterly – Phishing data sent to CSS leadership and agency directors and CIO's of agencies participating in the EIS Phishing Awareness Program
7. Quarterly – Reinforcement Training materials sent to all agency Directors, CIOC and ISC for dissemination to agency staff.

Appendix 1

9. InfoTech Security Awareness and Training Program Maturity Assessment - State of Oregon Department of Administrative Services – Enterprise Information Services

The awareness program went through a very thorough InfoTech maturity assessment in 2020 that is used as a guide for program improvement.

The resources used are designed to help our organization build, maintain, and measure a high-impact information security awareness program that reduces risk by changing employee behavior while meeting legal, compliance, and audit requirements.

The InfoTech Security Awareness and Training Program Maturity Assessment criteria is as follows:

Training Quality	Considers how the organization delivers training to employees, and the type of content used in training.
Phishing Simulation Quality	Considers how the organization leverages phishing simulation tests to improve organizational security.
Program Governance	Considers how the organization manages the security awareness and training program.

10. SANS Security Awareness Roadmap

The awareness program also uses SANS Security Awareness Roadmap to help identify the program's maturity level.

The Security Awareness Roadmap has five stages of program maturity levels.

1. **No Awareness Program**

   Program does not exist. Employees have no idea that they are a target, do not know or understand organizational information security and privacy policies, and easily fall victim to attacks or their own mistakes.

2. **Compliance Focused**

Program designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad-hoc basis. Employees are unsure of organizational policies, their role in protecting the organization's information assets, and how to prevent, identify, or report a privacy or security incident.

3. **Promoting Awareness & Behavior Change**

   Program identifies the training topics that have the greatest impact in supporting the organization’s mission and focuses on those key topics. Program goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work, home, and while traveling. As a result, employees, contractors, and staff understand and follow organizational policies and actively recognize, prevent, and report incidents.

4. **Long-Term Sustainment**

   Program has processes and resources in place for a long-term life cycle, including (at a minimum) an annual review and update of both training content and communication methods. As a result, the program goes beyond just changing behaviors and begins to change the culture of the organization.

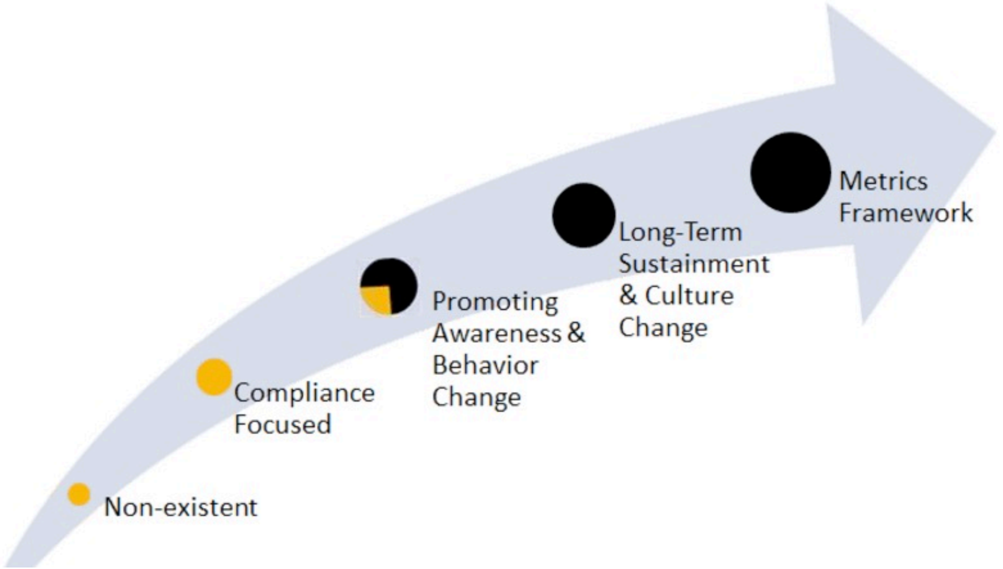
5. **Metrics Framework**

   Program has a robust metrics framework to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment.

Program Maturity

Based on the SANS Awareness Roadmap, the awareness program is in the third stage and is currently promoting awareness and behavior change and is actively working towards long-term sustainment.

Security Awareness Maturity Model


Non-existent
Compliance Focused
Promoting Awareness & Behavior Change
Long-Term Sustainment & Culture Change
Metrics Framework