IMMERSIVELABS

Immersive Labs - Workforce Experience Scenario Catalog

05-02-2024

Introduction

The Workforce Exercising scenarios offer a diverse range of interactive exercises and content designed to enhance workforce awareness, preparedness, and skills in cybersecurity and privacy matters. These scenarios cover various topics such as workforce exercising, data subject rights requests, smishing threats, and more, providing a comprehensive learning experience for users to strengthen their cybersecurity knowledge and practices.

Standard Scenarios (25)

These scenarios cover multiple risk areas. Written with a rich, realistic narrative, the participant makes decisions based on an evolving storyline.

Title	Risk Areas	Description
PayDay Blues	Social engineering Security reporting and responsiveness Digital footprint	You work in the head office at Freshter Ltd as a lead analyst and have built a positive reputation as the 'go-to' person whenever anyone needs assistance or advice. In this scenario, the topics of phishing, social media privacy settings, and reporting of security incidents are covered.
Safe Travels	Browsing securely Physical security Device security	You work as a solutions consultant in the financial services sector. On Monday you'll be flying out to meet with customers in Poland. In this scenario, the topics of security on the go, remote working, and VPNs are covered.

Title	Risk Areas	Description
A King's Ransom	Security reporting and responsiveness Browsing securely	You work for Freshter Ltd, an international just-in-time produce distribution company. You work from home, so frequently communicate with your colleagues via video calls, emails, and the company's messaging app. In this scenario, the topics of ransomware and insecure web browsing are covered.
Working Practices	Data handling Security reporting and responsiveness	You're an account manager for InsiteDataCorp and regularly handle customer data. You work solely in the office and rarely take work home. In the scenario, the topics of reporting incidents, phishing, and remote working are covered.
We Are The Champions	Data handling	You work for PunterPlay, an online gambling company. As a fast-growing company in a very competitive market, PunterPlay relies on close integration with third-party organizations to provide extra services in areas such as marketing and sales promotions. In this scenario, the topics of security champions, secure data handling, and security policies are covered.
First Day On The Job	Digital footprint Authentication Device security Security reporting and responsiveness Social engineering	You are about to start your new job at DicedPineapples, a small media startup. Your goals for the first day are to meet everyone in the company and set up your workspace. In this scenario, the topics of physical security, passwords, and social media privacy are covered.

Title	Risk Areas	Description
A Tough Call	Security reporting and responsiveness Authentication	You work as a customer service advisor at Katara10, a domestic energy supplier. Your colleague Amari is excited to tell you the news about his promotion, which includes receiving a work mobile phone. In this scenario, the topics of passwords, stolen devices, and security on the go are covered.
Pick Up and Play	Device security Security reporting and responsiveness	You're an account manager for Credita. As part of your role, you're in daily contact with data managers at multiple banks, sharing important credit check information with them. In this scenario, the topics of rogue USB devices and reporting security incidents are covered.
A Big Deal	Digital footprint Security reporting and responsiveness	You work at MilkshakeSocials as the executive assistant to its high-profile CEO. There's an important meeting today with a client and you're on hand to make sure everything runs smoothly. In this scenario, the topics of identity theft and privacy of information are covered.
Digging Deeper	Social engineering Security reporting and responsiveness	You're the finance manager at a startup company called Ouvi Automotive Insurance. You've got a busy day ahead that involves approving purchases, checking emails, and attending meetings. In this scenario, the topics of passwords, phishing, and verifying callers and contact requests are covered.
An Expensive Call	Physical security Security reporting and responsiveness	It's the beginning of a new week in your role at Cardamom, a startup software company. You've been booked to go on a last-minute work trip to meet clients across the country.

Title	Risk Areas	Description
		In this scenario, the topics of remote working and reporting incidents are covered.
Text Thread	Social engineering Digital footprint Security reporting and responsiveness	You've had a long and busy day at work and it's time for you to finally head home. You're just about to close down your computer when you receive a message from an unknown number. In this scenario, the topics of social engineering and identity verification are covered.
Business As Usual	Social engineering Digital footprint Security reporting and responsiveness	You've just started working at GreenBottle Inc, a software company that provides collaborative ways of data sharing with useful dashboards. As part of your role, you'll need to be active on social media to find new prospects for GreenBottle Inc. In this scenario, the topics of phishing, reporting incidents, and digital footprints are covered.
A Great Solution	Physical security Device security Data handling	Friday is finally here. You've spent the week working on a media project for a client, a short film, and the deadline is fast approaching. You're hoping to finally get it finished today so that you can enjoy the weekend. In this scenario, the topic of physical device storage versus cloud storage is covered.
Secret Santa	Social engineering Security reporting and responsiveness	You're an executive assistant for the CEO of Connectalize Communications. One of your seasonal duties is arranging end-of-year rewards from the CEO to the rest of the employees. Are you ready to be the office's Secret Santa? In this scenario, the topics of phishing, risk reduction, and incident reporting are covered.

Title	Risk Areas	Description
Strange Activity	Security reporting and responsiveness Data handling	You work as a customer service advisor for IM-Universe, an online gaming service that has recently made several staff redundant. You're just starting your day when you notice several reports from customers detailing strange activity on their accounts. In this scenario, the topics of security reporting and responsiveness, and data handling are covered.
Working from Home	Device security Physical security	You have started a new role as a Financial Manager in the financial services sector. It's an exciting opportunity enabling you to work from home. In this scenario, the topics of device security, and physical security are covered.
A Helping Hand	Security reporting and responsiveness	In this scenario, you work for a SaaS scale-up and have the potential to use AI to help you in your work. This scenario focuses on things to consider when using emerging technology in the workplace.
Visiting Hours	Physical security	You work for MoolAI, a FinTech company based at a coworking space in London. Several other businesses operate out of the same coworking space. You must escort a visitor safely through your workspace.
Footprints in the Sand	Digital footprints	In this scenario, you will have to decide on using social media appropriately, identifying OSINT risks, and deciding how and when to securely share information.
Password Problems	Authentication	You work in the finance department of a marketing agency, Bernard and Kate. It's a busy time of year, with lots of your big clients spending leftover budget with you. Your IT team is rolling out system upgrades. You must set new secure passwords, and keep your account safe.

Title	Risk Areas	Description
Browsing Around	Browsing securely	In this scenario, you work as a Product Designer. Part of your role is to conduct lots of research. You must effectively and securely browse the internet while setting up your browser software to mitigate security threats.
Public Demonstration	Security reporting and responsiveness	In this scenario, you work for a large energy company. You must respond to unusual activities of colleagues, suspicious behavior relating to your office premises, and security incidents.
Data Decisions	Data handling	In this scenario, you work in a data analytics company and are faced with several decisions related to the appropriate handling and management of data within your role.
New Job, New Hardware	Device security	In this scenario, you work for a technology start-up and have recently been promoted. This brings with it a technology upgrade! You'll need to consider various aspects of keeping your new device secure.

Multi-role scenarios (2)

The participant makes decisions across multiple job roles, as the storyline evolves. These scenarios can cover multiple risk areas.

Title	Risk Areas	Description
Internal Affairs	Security reporting and responsiveness Physical security	Dynamik Manufacturing is a robotics and manufacturing company. It produces and operates control systems and production line machines for multiple international companies. Some products and services are used to manufacture motor vehicles, aviation, train, and military equipment. In this scenario, you'll play multiple roles within the company as the situation unfolds, each with different responsibilities. In this scenario, the topics of security reporting and responsiveness, and physical security are covered.
Strange Activity Multi-Role	Security reporting and responsiveness	This scenario accompanies the 'Strange Activity' scenario and enables you to explore an unfolding incident from the perspective of several different job roles within the organization.

Baselining scenario (1)

An assessment-focused scenario. We recommend assigning this scenario at the beginning of your exercising journey to provide baseline data, identify priority areas for interventions, and monitor your human cyber risk profile over time.

Title	Risk Areas	Description
Security Hygiene Compass	Authentication Device security Physical security Security reporting and responsiveness Data handling Digital footprint Social engineering Browsing securely	This scenario is a series of 16 'mini-scenarios' that cover all topic areas. It has been designed to focus on data quality and enable you to understand your current human cyber risk profile in a single exercise. We recommend that this scenario is used at the beginning of your Immersive Labs journey to provide baseline data, identify priority areas for interventions, and monitor your human cyber risk profile over time.

Template scenario (1)

A standard scenario that follows a narrative storyline but requires customization. Replace the business names, logos, documents, and more, to personalize the scenario to your organization.

Title	Risk Areas	Description
A Successful Event Template	Data handling Security reporting and responsiveness	You've recently been joined in your team by a new colleague who's just coming to the end of their first week and have been busy helping them understand your organization's systems and processes. This is a template scenario focused on data privacy and data handling. It has been designed to enable you to easily customize the content and is accompanied by a user guide and editable rich media.

Policy & Regulation scenarios (2)

Simple scenarios to deliver a new or updated policy/regulation to your workforce and collect acknowledgement and agreement.

Title	Risk Areas	Description
ISO27001 and You	Data handling Device security Security reporting and responsiveness	You are the human resources coordinator at Connectalize Communications Ltd. Currently based in the US, the company is planning to expand into a new global market and is setting up a satellite office overseas to support this. In this scenario, you'll navigate a number of situations where you need to demonstrate ISO 27001 compliance in the setup of these new offices and staff recruitment.
Digital Operational Resiliency in The Workforce	Security Reporting & Responsiveness	You work for Deutsch UferImersiv. The bank's headquarters are in Germany, but it also has subsidiaries across Europe, the United States, and the Asia Pacific region. You're working from the bank's headquarters as a junior data analyst. This scenario is designed to educate your workforce on elements of security reporting that may be relevant to the Digital Operational Resilience Act (DORA). It's a standalone scenario or can be used in combination with its partner scenario in the crisis sim catalogue, using a linked narrative to target multiple groups.

Phishing Assessment scenarios (4)

Participants face multiple decisions around phishing, smishing, vishing, etc.

Title	Risk Areas	Description
Gone Phishing 1	Phishing Social Engineering	This is the first in a series of scenarios focused entirely on identifying phishing and social engineering. The scenario includes phishing emails, smshing, and vishing.
Gone Phishing 2	Social engineering	This is the second in a series of scenarios focused entirely on identifying phishing and social engineering. The scenario includes targeted phishing emails (spear phishing).
Gone Phishing 3	Social engineering	This is the third in a series of scenarios focused entirely on identifying phishing and social engineering. The scenario includes whaling and CEO impersonation.
Gone Phishing 4	Social engineering	This is the fourth in a series of scenarios focused entirely on identifying phishing and social engineering. The scenario includes targeted and generic phishing following a national holiday.

Spotcheck scenarios (2)

These micro-scenarios provide targeted and responsive content to enhance workforce awareness and preparedness in cybersecurity and privacy matters.

Title	Risk Areas	Description
Security Spotcheck Template	Social engineering	This micro-scenario allows you to create short, targeted content that is responsive to current threats to your workforce. This example focuses on smishing.
Privacy Spotcheck: Data Subject Rights Requests Template	Data handling	This micro-scenario allows you to create short content that is responsive to current threats to your workforce. This example focuses on data subject rights requests.

Enablement scenarios (2)

These scenarios use an exercise format to guide managers and learners through the benefits and importance of workforce exercising, as well as how to effectively utilize the content to achieve desired outcomes. These scenarios aim to enhance understanding and engagement with workforce exercising practices for both managers and learners within the organization.

Title	Risk Areas	Description
Managers: Using Workforce Exercising	NA	This scenario uses an exercise format to take managers through the benefits of workforce exercising, how it works, and how to use the content to achieve the outcomes that they want.
Learners: Using Workforce Exercising	NA	This scenario uses an exercise format to take learners through what workforce exercising is, why it's important, and what they can expect to see when using workforce content.