

SECURITY AWARENESS PROGRAM AUDIT

A Hands-On Exercise for HR and People Leaders

Based on principles from *The People Solution*
Dr. Jerrod Pickering | jerrodpickering.com

About This Exercise

This workbook guides HR and People leaders through a structured audit of their organization's security awareness program. You will evaluate a fictional organization, identify gaps, and develop a remediation plan — building the same critical thinking skills you need when assessing your own programs.

Learning Objectives

By the end of this exercise, you will be able to:

- Evaluate a security awareness program against a human-centered framework
- Identify the difference between compliance-driven and behavior-driven training
- Diagnose common gaps in HR-led security programs
- Develop a phased remediation plan with measurable outcomes

The Scenario: Meridian Health Services

Background

Meridian Health Services is a regional healthcare organization with 1,200 employees across three sites. The HR department owns the security awareness program, which consists of an annual online compliance module and a quarterly email newsletter. The CISO has raised concerns that employee behavior has not improved despite 94% completion rates.

DETAIL	INFORMATION
Organization	Meridian Health Services
Industry	Healthcare
Employees	1,200 across 3 sites
Current Training	Annual LMS module + quarterly newsletter

Completion Rate	94% annually
Recent Incident	3 phishing clicks in 90 days post-training

Exercise 1 — Diagnosing the Program

Part A: Identify the Training Model

Review the program description above. Answer the following questions based on what you know about effective security awareness design.

Key Concept
Compliance-driven training measures completion. Behavior-driven training measures change. A program can achieve 100% completion and still fail if it does not change what employees actually do.

1. How would you classify Meridian’s current training model?

Your answer:

2. The CISO reports three phishing clicks within 90 days of training completion. What does this tell you about the program’s effectiveness?

Your answer:

Part B: Gap Analysis

Using the five dimensions below, rate Meridian’s program on a scale of 1–5 and provide brief evidence for your rating.

Dimension	Score (1-5)	Evidence / Notes
Frequency & Reinforcement		
Behavioral Focus		
Role-Specific Relevance		
Manager Involvement		
Measurement & Feedback		

Exercise 2 — Building the Remediation Plan

Part A: Design Recommendations

Design Principle

Effective security awareness programs treat employees as people, not compliance checkboxes. They use spaced repetition, role-based scenarios, and real-world context to move knowledge into behavior.

For each gap you identified in Exercise 1, propose a specific intervention. Be concrete — ‘more training’ is not an acceptable answer.

Gap Identified	Proposed Intervention	How You Would Measure Success

Part B: 90-Day Implementation Roadmap

Sequence your top three interventions into a realistic 90-day plan. Consider organizational readiness, resource constraints, and quick wins.

Phase	Action Items	Success Indicators
Days 1–30 (Quick Wins)		
Days 31–60 (Foundation)		
Days 61–90 (Reinforcement)		

Exercise 3 — Stakeholder Alignment

One of the most common barriers to security awareness improvement is competing priorities between HR, IT, and the CISO. This exercise builds your skills for navigating that alignment challenge.

Scenario Update

New Information

The CISO wants to implement mandatory monthly phishing simulations. The Chief People Officer is concerned this will damage employee trust and create a culture of fear. The legal team wants everything documented for compliance purposes. You are the HR leader in the room.

1. What is each stakeholder’s underlying concern, beneath their stated position?

STAKEHOLDER	UNDERLYING CONCERN
CISO	
Chief People Officer	
Legal Team	
Employees	

2. Draft a brief statement (3–5 sentences) you would make to open the alignment meeting that acknowledges all three perspectives.

Your statement:

Reflection Questions

Use these questions to deepen your learning and connect the exercise to your own organization.

Individual Reflection

1. What does your organization’s current security awareness program have in common with Meridian’s?
2. Which of the five gap dimensions from Exercise 1 is your organization strongest in? Which needs the most work?
3. What would you need to bring to your CISO or CPO to make the case for a behavior-focused program redesign?

Group Discussion

- How does your HR team currently measure the effectiveness of security awareness training beyond completion rates?
- What is one quick win you could implement in the next 30 days without a budget increase?
- How do you balance psychological safety with accountability in security training?

Facilitator Note

Allow 10-15 minutes for individual reflection before opening group discussion. The most productive conversations tend to emerge from Question 3 — the business case framing — as it moves participants from theory to action.

THE MERIDIAN BREACH

A Security Awareness Case Study for HR Leaders

With Facilitation Guide
Dr. Jerrod Pickering | jerrodpickering.com

DOCUMENT	INFORMATION
Audience	HR Leaders, People Operations, Security Awareness Managers
Format	Case Study + Facilitation Guide
Delivery	Instructor-led, 90 minutes recommended
Materials	This document; whiteboard or shared digital workspace

PART I: THE CASE STUDY

Read the following scenario individually before the group discussion begins.

Background

Meridian Health Services is a regional healthcare organization with 1,200 employees across three campuses in the southeastern United States. The HR department has owned the security awareness program for five years, a decision made when the previous CISO argued that “security culture is a people problem.”

The program consists of three components: an annual HIPAA compliance module completed via the LMS, a quarterly email newsletter with security tips produced by HR Communications, and a mandatory password reset every 90 days. Completion rates have been consistently above 92% for three years.

In March, a billing coordinator at the Eastside campus received an email that appeared to be from the Director of Finance requesting urgent wire transfer approval. The coordinator forwarded the request to their manager, who approved it without verifying the sender's identity. Within 48 hours, \$127,000 had been transferred to a fraudulent account.

The Aftermath

Following the incident, the CISO commissioned a third-party assessment of the security awareness program. The assessment findings were shared with HR leadership, the CPO, and the Board’s Risk Committee.

Assessment Findings (Summary)
1. Training content was current and accurate, but organized around regulatory requirements rather than employee behavior. 2. The annual module format did not provide sufficient repetition for knowledge retention. 3. No role-specific content existed for finance or operations staff, who face the highest social engineering risk. 4. The program had no mechanism for employees to report suspicious communications without fear of discipline. 5. Completion rates measured whether employees clicked “Finish,” not whether they could recognize or respond to threats.

The Conversation

The following exchange took place during the post-incident review meeting:

CISO (Marcus)	<i>"We have 94% completion. What more do you want? The training was done. This is a human error problem."</i>
HR Director (Sandra)	<i>"With respect, Marcus, if 94% of our people completed the training and this still happened, maybe the training is the problem."</i>
CPO (Diana)	<i>"I agree with Sandra. Our people aren't failing us. Our program is failing them. We trained them to check a box, not to recognize a threat."</i>
CFO (Robert)	<i>"I don't care who owns the blame. I care about what changes on Monday."</i>
Legal (Kim)	<i>"We need to document whatever we decide today. The board will want to see a remediation plan within 30 days."</i>

Discussion Questions

Use these questions to guide your group analysis of the Meridian case.

Section A: Diagnosis

1. What specific design flaws in Meridian’s program contributed to this incident? Be specific — cite evidence from the case.
2. Marcus argues this is a “human error problem.” Sandra disagrees. Who do you think is right, and why? Is this a false dichotomy?
3. The billing coordinator actually did the right thing — they forwarded the request to a manager. Yet the incident still occurred. What does this tell us about where the program’s gaps actually are?

Section B: Design

4. If you were redesigning Meridian's program from scratch, what would you keep, what would you discard, and what would you add? Walk through your reasoning.
5. How would you design role-specific content for a billing coordinator vs. an HR generalist vs. a physician? What would be different and why?
6. The assessment found that employees had no safe mechanism to report suspicious communications. Why does this matter, and how would you build one?

Section C: Stakeholder Management

7. Sandra and Diana are aligned. Marcus is defensive. Robert wants action. Kim wants documentation. How do you move this group from conflict to a shared plan?
8. The CFO says "what changes on Monday?" What would you actually recommend for an immediate, low-cost intervention that could begin this week?

PART II: FACILITATION GUIDE

For Facilitators Only

This section is intended for the facilitator and should not be distributed to participants in advance. It contains discussion anchors, teaching points, and debrief guidance.

Session Overview

ELEMENT	DETAILS
Total Time	90 minutes (flexible to 60 min with reduced discussion)
Ideal Group Size	6–18 participants
Room Setup	Rounds or U-shape; avoid classroom rows
Materials Needed	Printed or digital case study; whiteboard or shared doc
Facilitator Experience	Intermediate; comfort with ambiguity and conflict helpful

Timing Guide

TIME	ACTIVITY
0:00–0:10	Welcome, framing, and individual reading time
0:10–0:25	Section A discussion (Diagnosis)
0:25–0:45	Section B discussion (Design)

0:45–1:05	Section C discussion (Stakeholder Management)
1:05–1:20	Full-group synthesis and key takeaways
1:20–1:30	Individual commitment — “One thing I’ll change”

Facilitation Notes by Section

Section A: Diagnosis (15 min)

The goal here is to move participants away from blame and toward systems thinking. Most groups will want to blame Marcus (the CISO) or the coordinator. Gently redirect.

Key Teaching Point

The coordinator did not fail — they escalated. The manager who approved without verification is a gap in the process, not a gap in the person. The program never trained managers on their specific role in verifying high-risk requests.

Watch for:

- Groups that quickly agree training was bad and move on — push them to be specific. “Which design flaw mattered most? Why?”
- Participants who defend completion rates — this is a productive tension; let it breathe before redirecting.
- The insight that the billing coordinator did the right thing — this is the most important diagnostic point in the case.

Section B: Design (20 min)

This is where HR leaders often feel most out of their depth. The facilitation goal is to build confidence that good instructional design principles are not complicated.

Key Teaching Point

Role-specific training doesn’t mean building 12 separate courses. It means using role-based scenarios within a shared framework. A billing coordinator and a physician face the same phishing threat — the difference is the context of the email they’d receive.

Watch for:

- Groups that jump to “more training” without questioning format — probe: “If annual training didn’t work, why would more annual training?”
- Strong ideas about psychological safety — validate and connect to reporting culture.
- Participants with L&D backgrounds who may dominate — invite quieter voices.

Section C: Stakeholder Management (20 min)

This section often generates the most energy because it mirrors real experiences. The goal is to practice reframing competing interests as shared interests.

Key Teaching Point

Marcus, Sandra, Diana, Robert, and Kim all want the same thing — they want this not to happen again. They disagree on the cause and the fix. The HR leader's job is to find the shared goal underneath the competing positions.

Discussion anchor for the CFO question:

Immediate low-cost interventions might include: a targeted email to finance staff from HR leadership (not IT) acknowledging the incident and offering a specific behavior to practice; a 10-minute team huddle script for managers to facilitate with their teams this week; or a clear, judgment-free reporting channel announced company-wide. The point is that behavior change doesn't require a new LMS module.

Synthesis Questions (Full Group)

Use these to close the discussion and drive commitment:

- What's the one insight from this case that most surprised you?
- What's one thing your organization's security awareness program has in common with Meridian's?
- If you had 30 days and a limited budget, what would you change first?

Closing Activity: Individual Commitment

Instructions

Ask each participant to write one specific, actionable commitment they will make in the next two weeks based on what they learned today. Invite 3-4 volunteers to share. This closes the session with accountability, not just insight.

Facilitator Preparation Checklist

- Read the case study twice before the session
- Identify 2-3 participants in advance who may have relevant experience to draw on
- Prepare the room to minimize hierarchical dynamics (avoid staging facilitator above group)
- Have whiteboard or shared document ready for capturing key ideas in Section B
- Practice the CFO question — it often catches facilitators off guard

eLEARNING STORYBOARD

When Training Isn't Enough: Security Awareness for HR Leaders

Dr. Jerrod Pickering | jerrodpickering.com

ELEMENT	DETAILS
Module Title	When Training Isn't Enough: Security Awareness for HR Leaders
Target Audience	HR Directors, People Operations Managers, Security Awareness Owners
Estimated Duration	15–20 minutes
Development Tool	Articulate 360 (Storyline)
Number of Slides	5 core slides + branching paths
Learning Objective	Learner will identify at least two design flaws in a compliance-driven security awareness program and propose one behavior-focused alternative.

Storyboard

Each slide entry includes: visual description, narration script, on-screen text, interaction design, and facilitator/developer notes.

Slide 1	When Training Isn't Enough	Title / Hook
VISUAL	Split screen: Left side shows a completion certificate with 94% next to a progress bar labeled 'Training Complete.' Right side shows a breaking news banner: 'COMPANY LOSES \$127K IN WIRE FRAUD.' Subtle red tint on right side.	
NARRATION	Your team completed the training. Every checkbox was checked. Every module was finished. So why is your company in the news today? In this course, we'll explore why completion rates and safety are not the same thing — and what HR leaders can do about it.	
ON-SCREEN TEXT	WHEN TRAINING ISN'T ENOUGH What completion rates can't tell you — and what actually keeps your people safe.	
INTERACTION	Click to continue. No branching on this slide.	

DEV NOTES	Objective: Create cognitive dissonance immediately. The learner should feel the gap between what they measure and what matters. Tone: calm, not alarmist.
------------------	---

Slide 2	Meet the Team at Meridian	Scenario Introduction
----------------	----------------------------------	-----------------------

VISUAL	Four illustrated character avatars in a 2x2 grid. Each has a name, title, and role badge. Characters: Sandra (HR Director), Marcus (CISO), Priya (Billing Coordinator), and David (Finance Manager). Clean, professional illustration style. Subtle Meridian Health Services logo in corner.
---------------	--

NARRATION	Meet the team at Meridian Health Services. Sandra owns the security awareness program. Marcus leads IT Security. Priya handles billing on the Eastside campus. And David is Priya's manager. Their stories will unfold throughout this course.
------------------	--

ON-SCREEN TEXT	Meridian Health Services character introductions with name cards beneath each avatar.
-----------------------	---

INTERACTION	Hover interaction: Clicking each character reveals a one-sentence bio and their role in security awareness. All four must be clicked before 'Continue' button activates.
--------------------	--

DEV NOTES	Design note: Characters should be diverse and professionally illustrated. Avoid stereotyping. The hover interaction ensures learners engage with all four before moving forward. This also models the kind of interaction design you would bring to an Articulate 360 build.
------------------	--

Slide 3	The Email Priya Received	Scenario / Decision Point
----------------	---------------------------------	---------------------------

VISUAL	Realistic email mockup centered on screen. From: d.chen@meridian-finance.net. Subject: URGENT – Wire Transfer Approval Needed. Body: Short, pressured language requesting \$127K transfer by end of day. Three red flag indicators are hidden in the email, revealed on interaction.
---------------	--

NARRATION	On a Tuesday afternoon, Priya received this email. It looked legitimate. The sender name matched her Director of Finance. The request was urgent. She had 20 minutes before end of day. What would you do?
------------------	--

ON-SCREEN TEXT	Email displayed prominently. Below it: "Before Priya responds, look carefully at this email. Click on anything that seems unusual."
-----------------------	---

INTERACTION	Clickable hotspot interaction. Three hidden red flags: (1) misspelled domain 'meridian-finance.net' vs. official 'meridianhealth.org'; (2) no standard email signature block; (3) 'reply-to' address is different from 'from' address. Learner must
--------------------	---

	find all three. Counter shows 'X of 3 found.'
DEV NOTES	This is the highest-interactivity slide in the module. The hotspot interaction builds the skill of careful observation, not just recall of policy. If the learner misses flags, provide gentle feedback: 'Look more carefully at the sender domain.' Do not penalize — this is discovery learning.

Slide 4	What Happened Next	Branching Scenario
VISUAL	Two-path branching visual. Left path labeled 'Priya escalated.' Right path labeled 'David approved.' Each path has a character avatar and outcome indicator (green/red). Timeline shows where the breakdown occurred.	
NARRATION	Priya did exactly what she was supposed to do. She forwarded the request to her manager for approval. She recognized she didn't have authority to approve this alone. The problem was what happened next.	
ON-SCREEN TEXT	Branching diagram. Learner clicks on David's decision point to explore what happened and what should have happened instead.	
INTERACTION	Click David's decision node to expand two sub-paths: (A) David verifies by calling Finance directly — fraud prevented. (B) David approves without verification — \$127K lost. Learner explores both. Question follows: "What specific knowledge or habit would David need to take path A?" Three multiple-choice options. Correct answer: a practiced verification habit, not just policy knowledge.	
DEV NOTES	Key insight this slide must land: The program failed David, not the other way around. He likely knew the policy but had never practiced the behavior. This distinction — knowledge vs. habit — is central to The People Solution framework. Reinforce it explicitly in feedback text.	

Slide 5	What You Can Change	Synthesis / Call to Action
VISUAL	Three-column layout with icons. Column 1: Frequency icon (calendar with multiple checkmarks). Column 2: Relevance icon (person with role-specific target). Column 3: Practice icon (rehearsal arrows). Clean, minimal design. Each column has a headline and two-line description.	
NARRATION	You can't control whether someone clicks a malicious link. But you can design a program that builds the habits, not just the knowledge, to reduce that likelihood. Three things you can do starting this week: increase touchpoint frequency, make content role-relevant, and build in practice, not just instruction.	
ON-SCREEN	Three-column synthesis with icon, headline, and 2-line description for each	

TEXT	principle. Below: “Download your Program Audit Checklist” button.
INTERACTION	PDF download button for a one-page Program Audit Checklist (job aid). Final reflective prompt before module closes: “Which of these three principles is your program weakest in? Type your answer below.” Free-text response recorded in LMS. No right or wrong answer — metacognitive prompt only.
DEV NOTES	Closing the module with a free-text reflection rather than a scored quiz sends an intentional message: this is about growth, not compliance. The job aid download ensures the learner leaves with something tangible. This is the ‘performance support’ layer of the design.

Appendix: Design Rationale

This storyboard reflects several intentional instructional design decisions drawn from adult learning theory and behavior science.

DESIGN DECISION	RATIONALE
Hook with cognitive dissonance (Slide 1)	Adult learners engage when their existing mental model is disrupted. The completion rate vs. breach outcome gap creates immediate relevance.
Character-based scenario vs. abstract content	Narrative increases retention. Learners remember stories; they forget bullet points. The Meridian characters anchor all content in a relatable context.
Discovery learning on Slide 3 (hotspots)	Finding red flags independently builds a transferable skill. Being told what to look for does not.
Branching on Slide 4 — both paths must be explored	Exploring the ‘what went wrong’ path is as instructionally valuable as the ‘correct’ path. Failure states teach more than success states.
Free-text reflection vs. scored final quiz	A compliance module ends with a quiz. A behavior-change module ends with a commitment. This design choice is intentional and should be discussed with stakeholders before development.
Job aid download on Slide 5	Performance support extends learning beyond the course. The checklist gives learners a tool they can use next week — not just knowledge they will forget.