



Training & Awareness

90 DAY HRM PLAYBOOK

Table of Contents

Executive Summary 3

Training & Awareness..... 5

 Play - Transform Awareness
 into Risk Reduction 9

Executive Summary

Human Risk Management (HRM) has evolved from a box-checking task to a critical business strategy. Today's cyber threats exploit human behavior, making it essential for organizations to move beyond generic, one-size-fits-all training. The path forward is clear: engage employees directly, use data to understand behavior, and act with precision.

According to [Cyentia's analysis of 100+ global organizations using HRM](#), just **10% of employees typically account for 73% of total human risk**.

The key to reducing risk isn't more training — it's targeting the right people, with the right interventions, at the right time.

This playbook is your guide to doing exactly that: implementing HRM with purpose, achieving measurable results, and building a security culture that works.

Designed around a Crawl, Walk, Run concept, the playbook provides modular "plays" — each a self-contained, outcome-oriented plan that addresses a key aspect of HRM. Whether your organization is just beginning to baseline human risk or is ready to automate risk-based interventions, these plays help operationalize your HRM strategy.

Each play includes:

- Clear business purpose
- Stakeholder alignment
- Step-by-step execution guidance
- Metrics for success

The goal of this playbook is to enable cross-functional teams — Security, HR, Compliance, and IT — to move from reactive programs to proactive, measurable risk reduction. Traditional compliance often causes employees to disengage, thinking "it's not me, I'm not the problem." HRM changes that by personalizing risk, showing individuals how their behaviors contribute to risk or vigilance. When paired with peer comparisons and clear business context, people take ownership, adapt their actions, and actively work toward vigilance.

By aligning real behavior data and stakeholder ownership, these plays turn security from an abstract concept into an integrated part of how your organization works and grows.

Use this playbook as a living toolkit. Select plays based on your current HRM maturity, or build a sequence tailored to your goals. Wherever you start, every play brings you closer to a culture of security ownership, accountability, and resilience.

Your Next Step:

Pick a Starting Point That Drives Outcomes

This playbook is a living toolkit. You can:

- 1** Select plays based on your current HRM maturity
- 2** Build a sequence tailored to your organizational goals
- 3** Progress step by step toward a culture of security ownership, accountability, and resilience

Where to begin: Identify your top priority — Security Culture, Training and Awareness, or Risk Measurement. From there, we'll guide you from goal to play to outcome with focused one-page resources.

Training & Awareness

Turning Awareness Into Risk Reduction

The **90-Day Human Risk Playbook** helps organizations elevate awareness from a compliance task to a measurable driver of behavior change. Within that framework, the **Training & Awareness Plays** focus on using targeted, data-driven interventions to transform awareness programs into engines of risk reduction and employee engagement.

These plays show how to connect awareness initiatives to real risk indicators, prioritize interventions for high-risk cohorts, and measure impact in terms executives care about — fewer incidents, stronger vigilance, and demonstrable ROI.

Expected Outcomes of Training & Awareness Plays

A strong security culture isn't just about awareness—it's about **measurable outcomes** that prove employees are engaged, accountable, and actively reducing risk. By focusing on recognition, personalization, and organizational visibility, the following plays drive tangible improvements in how people think, act, and own security every day.

Expected Outcomes of Training & Awareness Plays

A mature Human Risk program isn't about more alerts or generic compliance training — it's about showing measurable progress in reducing exposure. When executed together, these plays deliver:

Visibility into human risk

surface the riskiest 10% of employees and enroll them into tailored learning journeys

Prioritization of interventions

reduce phishing click rates among privileged access employees by 10%

Reduced incident exposure

cut repeat clickers by 40% quarter over quarter and lift Behavior Scores by 12+ points across employees flagged with multiple risky actions

Improved detection and reporting

Increase phishing report rates by 15% in heavily targeted employee cohorts

Executive and board alignment

deliver metrics that tie behavior change directly to enterprise risk frameworks like MITRE, NIST, and ISO

Together, these initiatives transform Training & Awareness from a compliance exercise into a proactive, data-driven discipline — reducing the probability of breaches and building executive confidence that human risk is being managed at scale.

Why Modern Security Awareness & Training (SA&T) Teams Drive ROI

Security Awareness & Training is often viewed as a **compliance checkbox**—mandated training, annual refreshers, phishing simulations—but that’s a narrow, outdated view. When done right, SA&T is a **behavioral engine** that reduces risk, improves resilience, and aligns people with business strategy.

To shift from cost center to value driver - Awareness teams must prove how training and engagement:

- Positively change behavior
- Strategically reduce actual risk - quantifiable
- Effectively influence measurable security outcomes

And it all starts with moving **beyond compliance**—and toward **data-driven, risk-focused programs**.

1. Human Risk Is the Dominant Threat Vector

Today, 82–90% of cyber incidents are tied to human behavior—phishing clicks, credential reuse, poor data handling, misconfigured systems.

The attack surface isn’t just digital. It’s behavioral. Awareness and training programs that focus on **measuring human risk indicators**, not just training completion, become **direct contributors to breach prevention**.

ROI is no longer about “who took training,” but “**what behaviors changed and reduced exposure.**”

2. Compliance Isn’t the Goal—Culture and Vigilance Are

Traditional SA&T metrics (e.g., completion rates, phishing click rate, and survey feedback) **don’t reflect true organizational security posture**.

Forward-looking teams measure:

- Engagement over time (click-to-complete, nudge response rate)
- Risk by cohort (e.g., elevated access + phishing failure + no MFA)
- Behavior change across high-risk groups (e.g., reporting increase after campaign)

These metrics speak the language of risk and vigilance—not just compliance. That’s what gets executive buy-in, budget, and influence.

- HR support for lifecycle-specific risks (onboarding/offboarding)

That’s a multiplier effect—**awareness influencing prevention, not just education.**

3. Awareness Teams Shape Security Culture from the Middle

SA&T is one of the few security functions that directly interfaces with **every employee**. That reach, when used strategically, can create:

- Trust
- Habit formation
- Psychological ownership
- Recognition loops (positive reinforcement after secure actions)

When awareness is **continuous, contextual, and targeted**, it creates the conditions for cultural transformation.

Behavior change **doesn't scale through policy—it scales through repetition, context, and feedback**.

4. Awareness-Led Programs Amplify Cross-Team Collaboration

SA&T teams are uniquely positioned to **bridge silos** between security, HR, IT, and business units.

When training aligns to real risk (e.g., phishing behaviors mapped against real threat actor behavior), you enable:

- Better reporting and detection from frontline employees
- Earlier intervention from IT or IAM based on observed behavior

5. Executive Support Starts with Better Metrics

Security leaders and boards don't want to see click rates—they want to see:

- Which **behaviors** have changed and **why**?
- Which employee cohorts are **improving or regressing**?
- Which teams/groups/regions are **vigilant** and which groups are **risky**?
- How are we reducing actual exposure in our **riskiest roles**?

When SA&T reports are built on behavioral risk metrics, they align to enterprise risk reports, not just LMS platforms.

The SA&T function becomes a **data-backed enabler of risk reduction**—not just a training vendor.

Bottom Line for Enterprise Security

Awareness and training programs that:

- Focus on **risk-aligned cohorts**
- Prioritize **engagement and reinforcement**
- Measure and report on **behavioral outcomes**
- Move the needle on real-world threats and **drive measurable ROI**
- Measure and report on **behavioral outcomes**
- Move the needle on real-world threats and **drive measurable ROI**

Without this approach, organizations face:

- Employees trained but still behaving insecurely (usually in the name of efficiency)
- Awareness programs dismissed as checkbox requirements, cost center
- Lack of visibility into who's truly at risk

With this approach, they gain:

- A security-aware workforce that understands context and consequences
- Reduced frequency and impact of human error
- Culture change that starts with metrics, not slogans

Play - Transform Awareness into Risk Reduction

Goal:

Adopt a Human Risk Management (HRM) approach within your Training & Awareness (T&A) program to shift from compliance-based education to risk-aligned behavior change. This play is designed for mature programs operating in the “Walk phase” of HRM.

We need to move beyond training completions and phishing simulations as standalone metrics. Instead, we must align awareness efforts to actual behavioral risk, by integrating security education with user behavior data, threat exposure, and access context.

Ultimately, the goal is to reduce human-enabled incidents—like phishing clicks, mishandled data, or risky downloads—by continuously identifying at-risk cohorts and delivering relevant, timely, and targeted interventions.

Step by Step:

Modernize how your program defines success—focus on the people who need support, not just completion stats. The Cyentia Report shows that 10% of employees create 73% of the risk - if we were to just focus on the risk by leveraging data - imagine the work we could all do to improve behavior with that level of focus!

A high-impact T&A program recognizes that not all employees pose the same level of risk, and not all risky behaviors require the same response. By personalizing risk insights, employees see exactly how their actions affect the organization — which motivates them to change. This context-driven approach allows security teams, even with limited bandwidth and large populations, to focus interventions where they will create the greatest behavior shift and lasting impact.

Step ① : Set Clear Goals

What KPIs do we want to report to reflect **training value and behavior change**, not just task completion?

Set Clear Goals

- Reduce the number of repeat phishing clickers
- Improve secure behavior scores within high-risk cohorts
- Achieve strong completion rates for targeted learning paths
- Increase voluntary engagement with microlearning and training activities
- Raise phishing report rates in heavily targeted groups

Define Success Metrics (KPIs)

Here are examples of what leading T&A programs report:

- % of employees in high-risk cohorts (e.g., clickers + no MFA + elevated access) who completed tailored learning paths
- Change in secure behavior score by cohort (before/after training + nudges)
- % of targeted employees who moved from “risky” (e.g., clicked or ignored training) to “vigilant” (e.g., reported phish)
- Drop in repeat clickers or DLP violations post-targeted training
- Increase in training engagement (voluntary completions, microlearning opt-ins)

Align on Risk Cohorts:

Choose to prioritize segments like:

- “Heavily targeted employees” who have poor phishing resilience
- “Privileged access” employees who are clicking
- New hires in high-risk business units
- Repeat offenders with multiple behavioral flags

Step 2: Dependencies

To evolve from awareness campaigns to **measurable behavior change**, you’ll need:

- **Identity and Access Data** (to align employees to risk-relevant roles)
- **Simulation + Behavior Data** (phishing clicks, reporting trends, training completion)
- **Threat Intel or Email Gateway Logs** (to show targeting patterns)
- **Learning Management System (LMS)** data (completion, quiz outcomes, recertifications)
- **Security Behavior Scores** - way to measure change over time to automate what is working and scrap programs that are not shifting behavior towards vigilance



Supported by:

- » Learning & Development (L&D) or People Team
- » Security Operations (for simulation data and behavior signals)
- » HR Business Partners
- » Executive Sponsor (e.g., CISO, CHRO, VP of Risk)

Step ③: Prerequisites / Setup

- Integrate 2–3 core data sources (e.g., LMS, phishing tool, IAM platform)
- Create user segments that combine **behavioral and access context** that are agreed upon risk pockets
 - » Examples:
 - Heavily targeted employees, who have recently clicked, and have elevated access
 - Clickers without MFA
 - employees targeted 5+ times/month to align to phishing sim program
 - » Communicate to leadership that future reporting will highlight **training impact on risk**, not just compliance
 - » Gain stakeholder buy-in for behavioral nudges and recognition triggers (e.g., “You reported a phish this week—nice work!”)

Step ④: Create Execution Plan

Step 1: Identify High-Risk User Segments (Week 1)

- » Pull 90-days of data to set a baseline
- » Cross-reference with employees targeted by phishing or flagged by threat intel
- » Prioritize elevated access roles or employees with repeat behavior issues

Step 2: Analyze Learning Gaps and Threat Patterns

- » Identify where secure behavior is breaking down (e.g., ignoring file warnings, poor phishing detection)
- » Map attack types (e.g., credential phishing, invoice fraud) to learning content gaps

Step 3: Build Targeted Learning Path

- » Assign short, contextual microlearning (3–5 minutes) based on:
 - Simulated Phishing - monthly - to employees who are targeted consistently to measure click vs targets
 - Real Risk roles - let the data tell you which groups are risky vs. gut feel (finance, executive assistants, IT admins)
 - Additional Learning pathways solely for the risky 10% of the org- allow everyone else to focus on their jobs
 - Everyone needs baseline compliance training, but only the riskiest employees need extra. So why train everyone the same when just 10% truly need targeted intervention?
- » Efficiency back to the business - give time back to those who do not require the training interventions

Step 4: Launch Campaign with Context

- » Send personal messages to impacted employees:
 "We have noticed your inbox is under threat this quarter - stay vigilant out there."
- » Provide optional manager resources to reinforce

Step 5: Reinforce with Nudges & Behavior Tracking

- » Deliver real-time nudges tied to behavior (e.g., "You clicked a link that could've been malware. Here's what to look for next time.")
- » Run a follow-up simulation or DLP test to measure change
- » Track and report shifts in user behavior (e.g., phishing report rate, reduced repeat clickers)

Step 5: Avoid Pitfalls (Lessons Learned)

- Don't run the same training for everyone—**focus on behavior + context**
- Don't rely solely on LMS completion—**measure outcomes, not outputs**
- Avoid generic phishing modules—**tie simulations to real attack methods**
- Don't skip recognition—**positive reinforcement drives stronger retention**
- Don't work in a silo—partner with **SOC, IAM, and HR** to align visibility and intervention

Step 6: Make This Real—Report the Wins

Example OKRs or Goals:

- Identify and enroll top 10% of behaviorally at-risk employees into tailored learning journeys
- Increase reporting rate by 15% in the "heavily targeted" cohort
- Decrease phishing click rate by 10% in the "privileged access" cohort
- Improve Behavior Score by 12+ points across all employees flagged with 2+ risky actions
- Reduce repeat clickers by 40% quarter over quarter

Ready to Put the 90-Day Human Risk Playbook Into Action?

1

Share this playbook with your peers in Security, HR, Compliance, and IT to start the conversation about Human Risk Management.

2

Choose your starting point — Training & Awareness, Security Culture, or Risk — and select the plays that align to your most urgent priorities.

3

Request a personalized demo of Living Security's Unify platform to see how real-time data can bring these plays to life and make progress visible across your organization.

[Schedule a Demo](#)

About Living Security

Living Security's mission is to reduce human risk by transforming security awareness into measurable business outcomes. With Unify, our Human Risk Management platform, we enable organizations to:

- Gain visibility into high-risk behaviors and cohorts
- Prioritize interventions where they will have the most impact
- Prove ROI through measurable risk reduction and cultural resilience

Our solutions combine behavioral data, targeted interventions, and executive-ready reporting to turn human risk from a blind spot into a business advantage.

Living Security has been recognized by industry analysts and leading enterprises as a pioneer in Human Risk Management, delivering measurable results for global organizations.

