



90 DAY HRM PLAYBOOK

Table of Contents

Executive Summary	3
Security Culture	5
Play - Nudges	8
Play - Scorecards	11
Play - Cultural Dashboards	14
Training & Awareness.....	18
Play - Transform Awareness into Risk Reduction.....	22
Risk Plays.....	26
Social Engineering Risk Cohort	29
Play - Decrease Exposure to Social Engineering	31
Insider Threat Risk Cohort.....	34
Play - Decrease Exposure to Insider Threat	37
Account Compromise Risk Cohort	40
Play - Decrease Exposure to Account Compromise.....	43
Data Leakage Risk Cohort	47
Play - Decrease Exposure to Data Leakage	51
Malware Exposure Risk Cohort.....	55
Play - Decrease Exposure to Malware	59

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.

Security Culture

Operationalizing Security Culture

The **90-Day Human Risk Playbook** is built to help organizations move from awareness to measurable behavior change. Within that framework, the **Security Culture Plays** focus on embedding secure practices into everyday routines — turning culture into a driver of resilience rather than a byproduct of compliance.

These plays — Nudges, Scorecards, and Culture Dashboards — are designed to move security beyond campaigns and annual events. By reinforcing behaviors in the moment, providing personalized feedback, and making progress visible, they create a culture where employees feel accountable, engaged, and recognized for contributing to security.

Expected Outcomes of Security Culture 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.

When executed together, these plays deliver:

Higher vigilance at scale

10% more phishing reports across the business and a 5% increase among executives.

Improved behavior scores

5-point lifts across the organization through scorecards and up to 10-point improvements driven by culture dashboards.

Stronger employee engagement

300+ positive recognition interactions per quarter, higher training participation, and survey feedback reflecting greater trust and buy-in.

Manager-enabled coaching

consistent, data-driven security conversations supported by personalized scorecards.

Executive and board-level visibility

dashboards actively referenced in leadership meetings and board reports, driving alignment and accountability across business units.

These outcomes are powered by three complementary plays:



Nudges

reinforcing positive behaviors in the moment to build engagement and trust.



Scorecards

giving employees and managers clear visibility into behaviors, progress, and opportunities for improvement.



Culture Dashboards

elevating cultural maturity to a measurable business asset that leaders can act on.

Together, these initiatives transform security from a compliance requirement into a **culture of ownership, accountability, and resilience**—embedding secure behavior into daily routines and scaling human risk reduction across the organization.

Why Positive Cyber Culture Is Crucial

A strong culture—whether in business or personal life—shapes how people think, act, and interact when no one is watching. It creates shared values, trust, and accountability, which lead to better decisions, stronger relationships, and consistent behavior over time. In any setting, culture determines whether people feel empowered to take ownership, speak up, and support each other. Ultimately, it's the invisible force that turns strategy into action and good intentions into real outcomes.

1. Scale Magnifies Risk, but a Single Weak Link Can Trigger a Breach

- Larger organizations have more endpoints, systems, third parties—and *people*.
- A single compromised account or unreported incident can cascade into a major breach.
- Without a strong culture, you're reliant on inconsistent behaviors across departments and geographies.

According to the [*State of Human Risk Management report*](#), organizations with **10,000+ employees** experience the **highest concentration of human risk indicators**, especially in **privileged employees and siloed teams**.

2. Decentralization Creates Gaps

- Large orgs often operate in silos: security, HR, IT, and business units each have their own processes and tools.
- A positive culture aligns these groups under a shared responsibility for security.
- It builds **cross-functional accountability**, not just top-down mandates.

3. Behavior Change Doesn't Scale Without Culture

- Awareness programs don't move the needle at scale unless they're *supported by a culture* of trust, feedback, and reinforcement.
- Culture ensures consistency across regions, roles, and seniority levels.
- Large organizations must go beyond training to build **habits and norms**—especially in high-risk cohorts.
- To build culture, everyone must be engaged and feel a sense of ownership.

4. Leadership Influence Has Broader Reach

- In large enterprises, **executive sponsorship and visible modeling of secure behavior** set the tone.
- A strong culture encourages managers to support security programs—not treat them as distractions.
- It helps security teams influence from the middle, not just push from the top.

Bottom Line for Enterprises

Cyber risk at scale is human risk at scale.

Without a positive culture, large organizations face:

- Inconsistent reporting
- Delayed response to threats
- Employees demonstrate slow adoption of security tools
- Higher risk from trusted insiders

With a strong culture, they gain:

- Proactive detection of emerging threats
- Empowered employees who act as sensors
- Alignment across business units
- Resilience that scales

A study by *Yale University* found that **positive reinforcement increases long-term memory retention by 70%**, especially when applied shortly after the learning occurs. This is because positive feedback enhances dopamine release, which plays a key role in memory encoding.



Play - Nudges

Goal:

This play tackles the lack of recognition for positive security behaviors, which often leaves employees disengaged and viewing security as purely punitive. Too often, programs only reach out when something has gone wrong — and that needs to change. Constant negativity trains employees to tune out, blending security messages into the white noise of alerts from other tools. Instead, catch them doing good. Recognize and reward positive actions, and you'll foster engagement, build trust, and drive a security-first culture.

Strategically, it reinforces a **proactive and empowering security culture**, where employees feel they are active contributors to organizational security, not just "the weakest link".

It supports organizations in the **Crawl transition** of Human Risk Management (HRM) maturity by evolving from reactive metrics to behavior celebration and reinforcement.

Step by Step:

Celebrate Secure Wins with Positive Reinforcement Nudges

Encourage and reinforce secure behaviors by recognizing employees who report phish, avoid risky clicks, complete security training, effectively utilize MFA or a password manager - turning everyday actions into culture-building moments.

Step 1: Set Clear Goals

- **Increase reporting** of real phishing emails across the organization
- **Improve simulated phishing report rates** among targeted employee groups
- **Reduce risky password reset incidents** through proactive coaching
- **Achieve high training completion rates** within required timeframes
- **Establish a culture of recognition** by consistently celebrating both habitual and occasional secure behaviors
 - » For habitual activities, recognize consistent behavior, not just a single incident. "Thank you for utilizing MFA successfully for the entire month. You are part of the Human Firewall keeping our company safe from hackers. We couldn't do it without you"
 - » For occasional activities, celebrate the good in the moment. "Thank you, your proactive reporting of a Phish will help keep our company safe from hackers. Stay vigilant"



Step ②: Dependencies

This is a team game, our customers typically need to work with other key stakeholders to get this play stood up. Here is who our customers typically work with to get this play approved and rolled out to the employees:



Led by: Security Awareness Program Manager

Supported by:

- » Communications team (for tone and branding)
- » IT/Engineering (for automation and segmentation setup)
- » HR or People Ops (for cross-org visibility)
- » Executive Sponsor (e.g. CISO, VP of HR)

Step ③: Prerequisites / Setup

- Nudge delivery platform enabled (Microsoft Teams, Slack, or email platform)
- Filters or segments created (e.g. employees who reported a phish, completed training, etc)
- Communication templates reviewed and approved
- Stakeholder sign-off on tone and frequency of recognition nudges
- Data integrations functioning to power the “nudge”

Step ④: Create Execution Plan

Step 1: Identify Recognition Events

- » Pull behavior data to celebrate in real time (e.g. phish reported, password reset, training completed)
- » Qualifying employees will be queued up to receive acknowledgement of positive activities
- » Test nudge outreach with your teams first - then go wide

Step 2: Build Recognition Messaging

- » Draft friendly, motivating nudge templates (“Thanks for reporting that phish, you helped keep our company safe!”)



- » Creative Examples:
 - 15 second video from CEO/CISO/VP thanking the employee and why it was important
 - For every positive action (reporting a phish) - let them know they are entered to win a prize at the end of the month / quarter
 - Fun GIF letting them know you appreciate them for what they are doing

Step 3: Automate or Manually Send Nudges

- » Launch campaign via MS Teams, Slack, or email
- » Ensure cadence is sustainable (weekly or monthly)

Step 4: Monitor and Optimize (Sprint 3 – Owner: CSM)

- » Track opens, responses, reporting volume changes
- » Survey recipients on how it felt to be recognized
- » Use dashboard in Unify to measure impact of positive reinforcement - are reports going up across the org due to this play

Step 5: Avoid Pitfalls (Lessons Learned)

- » **Don't nudge on negative behaviors** – massive focus area when speaking with HR and Comms. Be clear this tool will be used for positive feedback and not be used in a punitive way! We are building a positive, engaged, vigilant security culture.
- » **Avoid generic messages** – personalization boosts impact!
- » **Don't over-nudge** – recognition should feel meaningful, not spammy

Step 6: Make this real, report the wins

Example OKR's or Goals:

- » 300+ positive interactions this quarter with our employees
- » Baseline - how many reported phish did you have last quarter and use that to baseline your interactions
- » 10% increase of reported phish this quarter
- » 5% increase of report phish by executives this quarter
- » 10 point increase in Behavior Scores



Play - Scorecards

Goal:

Employee scorecards personalize risk, making it clear how an individual's actions impact the organization's security — for better or worse. By showing exactly what they're doing well, where they can improve, and how they compare to peers, scorecards turn "it's not me" into "I can make a difference." This clarity builds ownership, reinforces positive habits, and drives a culture of vigilance where every employee plays an active role in reducing risk.

Step by Step:

Step 1: Set Clear Goals

When used right, scorecards become **mirrors, not microscopes**—helping employees grow rather than policing them. Bring the employees into the conversation so they have a better grasp of what is important and how they can make an impact!

- **Promote Self-Awareness** by using scorecards to surface behaviors and metrics tied to both success and risk, helping employees see how their actions impact broader goals (e.g., security, productivity, customer experience).
- **Foster healthy competition** by benchmarking employees and teams against peers when scorecards are shared, encouraging continuous improvement through transparent comparisons.
- **Guide targeted improvement** by providing clear, personalized data that highlights where adjustments are needed, enabling employees to focus on actionable areas such as phishing click rates, secure file sharing, or training engagement.
- **Enable manager-led coaching** by equipping managers with visibility into their team's vigilance and risk posture, and giving them concrete insights for meaningful 1:1 discussions that are evidence-based rather than subjective.



Step ②: Dependencies

Partnering with HR is essential when using scorecards because HR ensures that feedback is aligned with company values, performance frameworks, and employee development goals. They play a critical role in shaping the culture, ensuring scorecards not only measure security behaviors but also reinforce the kind of workplace the organization wants to build. HR helps design scorecards that are fair, consistent, and legally sound, reducing the risk of bias or misuse. They can also integrate scorecard insights into broader talent initiatives like coaching, recognition, or improvement plans. Ultimately, their involvement turns scorecards into a strategic tool for both security and workforce growth.



Led by: Security Awareness Program Manager

Supported by: Communications / HR (employee messaging strategy)

Step ③: Prerequisites / Setup

- Identify which behaviors you want to be communicating back to the employees
 - » Examples:
 - Real phish reported or clicked
 - Simulated phish reported or clicked
 - Data moved successfully
 - Training taken or overdue
- Scorecard template reviewed, approved, and tested
- Communications prepared to announce the scorecard roll outs

Step ④: Create Execution Plan

Step 1: Finalize Configuration & Data Mapping

- » Confirm integration with phish, training, MFA, and endpoint sources
- » Validate that user identity mapping is complete for scorecard delivery

Step 2: Internal Testing & QA

- » Deliver sample scorecards to internal testers (Security team, HR)
- » Verify scoring logic, delivery timing, formatting, and behavior trends



Step 3: Prepare Launch Communications

- » Draft messaging explaining what the scorecards are and why they matter
- » Include: sample screenshot, interpretation guide, and resource links

Step 4: Full Employee Rollout

- » Enable regular (weekly, monthly or quarterly) email scorecard delivery to all employees
- » Monitor delivery and open rates

Step 5: Reinforce with Managers

- » Send talking points to line managers to encourage usage
- » Optional: Office hours or AMA sessions for questions

Step 6: Monitor Behavior Change Over Time (Ongoing)

- » Track improvements in phish reporting, training completion, and MFA adherence
- » Surface "Scorecard Success Stories" for future comms or executive reports

Step 5: Avoid Pitfalls (Lessons Learned)

- **Don't skip Quality Assurance** – Misaligned scores or formatting can cause distrust
- **Avoid vague messaging** – Explain what employees *should* do with their score
- **Don't overpromise on changes** – Set expectations that score trends take time to improve
- **Communications** – Let employees know what the scorecards are (education) and what they are not (punitive)

Step 6: Make this real, report the wins

Example OKR's or Goals:

- 100% of employees receive a scorecard per month/quarter
- Company behavior score improves 5 point over next quarter



Play - Cultural Dashboards

Goal:

Goal: Culture is the **invisible engine** behind performance, risk reduction, and employee satisfaction. What's valued gets acted on—and what's measured gets managed. Without measurement:

- Culture remains abstract, subjective, or reactive.
- You can't identify gaps between stated values and lived behaviors.
- It's difficult to drive intentional improvement or gain leadership buy-in.

Measuring culture turns it from a "soft" concept into a **strategic asset**—shaping how people think, behave, and protect the organization every day.

Step by Step:

Quantify your culture!

Measuring culture—especially in cybersecurity or organizational performance—means translating values and behaviors into observable, trackable indicators. Here's how:

Step 1: Set Clear Goals

A **culture dashboard** is a strategic tool that turns intangible values into measurable results. Its goals span executive visibility, board alignment, supporting technology spend vs. risk, and organizational momentum. Here's how it delivers value at each level:

- **Secure executive buy-in** by demonstrating how culture directly impacts business outcomes such as risk reduction, productivity, and employee engagement, and by equipping leaders with clear metrics (e.g., phishing report rates, human risk scores, training engagement) that justify investment and support cross-functional initiatives.
- **Elevate board reporting** by providing credible, digestible data that links people-driven behaviors to enterprise risk posture, and by showing progress over time through trendlines, benchmarks, and risk movement across the organization, departments, or regions.
- **Celebrate company-wide wins** by sharing improvements in cultural maturity—such as increased secure behaviors or cross-team alignment—in a transparent way that motivates teams, reinforces positive behaviors, and builds ownership through stories and metrics that connect employee actions to real-world outcomes.



Ultimately, a culture dashboard is more than a reporting tool—it's a **storytelling engine** that drives strategic decisions, builds momentum, and turns human behavior into measurable business value.

Step 2: Dependencies

- **Behavioral Data Infrastructure**
 - » **Inputs:** Data from tools like phishing simulations, training platforms, HRIS, DLP, collaboration tools, and incident reports. Start with a minimally viable data set and then layer on after proven success.
 - » Must capture *actual behaviors* (e.g., reporting suspicious emails, secure data movement, and training completions) rather than just passive metrics (e.g., login counts).
 - » Requires integration pipelines and normalization logic to make diverse data sources usable.
- **Defined Cultural Indicators**
 - » Clear agreement on what “culture” means in your org (e.g., trust, accountability, security ownership).
 - » Translate values into **measurable signals**: reporting rates, manager engagement, escalation actions, sentiment trends, etc.
 - » Set baselines and thresholds for what “good, better, best” looks like.
- **Cross-Functional Alignment**
 - » Security, HR, IT, and Compliance must align on:
 - What’s being measured and why?
 - How will it be used (coaching vs. compliance)?
 - Who owns which components?
 - » Collaboration ensures the dashboard reflects reality, not just isolated metrics.



- **Executive Sponsorship**

- » A champion at the leadership level who ensures:
 - The dashboard aligns with strategic goals
 - Results are reviewed and acted upon
 - It doesn't become "just another report" but drives change

- **Communication & Enablement Layer**

- » Context and narratives behind the numbers (e.g., "Why did phishing reporting spike?").
- » Training for managers or culture champions on how to use the insights for coaching and recognition.

Step ③: Prerequisites / Setup

- Unify Dashboards module enabled
- Key integrations feeding data into Unify (e.g., phishing, MFA, endpoint, training)
- Roles and access permissions configured by audience (exec, manager, analyst)
- Data validation and scorecard alignment complete
- Optional: Custom views created by department or role

Step ④: Create Execution Plan

Step 1: Confirm Dashboard Configuration

- » Validate all required data sources are feeding into Unify
- » Confirm behavior scores, HRI scores, and categories display accurately

Step 2: Develop Role-Based Views

- » Create executive view (org-wide risk trends, top departments)
- » Create department/manager views if needed
- » Add filters: HRI scores, phish click rates, training completion, etc.

Step 3: Pilot with Internal Champions

- » Share dashboards with 2–3 executives or directors for feedback
- » Incorporate any usability or interpretation suggestions



Step 4: Launch Executive Visibility

- » Introduce dashboards in monthly security, audit, or ops review
- » Provide slide snapshots or portal walkthroughs for reference

Step 5: Rollout to Additional Stakeholders

- » Extend access to business unit leaders and risk owners
- » Use office hours or async guides to support adoption

Step 6: Measure Usage & Drive Action

- » Track access frequency, behavior shifts, and feedback loops
- » Identify top risks, assign microlearning or nudges from insights
- » As more training and phishing becomes automated, measuring usage and effectiveness will become more necessary and strategic to tune the automation.

Step ⑤: Avoid Pitfalls (Lessons Learned)

- **Avoid sharing dashboards without guidance** – Stakeholders may misinterpret data without context
- **Align on look and feel** – are these in the right formats that leadership likes to see updates?
- **Be cautious with raw comparisons** – Normalize by department size or exposure
- **Avoid data blind spots** – Missing data sources can skew insights and reduce trust
- **Create a takeaway** – “Based on what we are seeing, we are planning to do X to focus on this cohort of risk that is still present”.

Step ⑥: Make this real, report the wins

Example OKR's or Goals:

- CISO and leadership use dashboards for decision making
- Increase behavior scores by 10 points via actions (like controls or training) that were deployed against known risk areas
- 3+ departments are using dashboard to share with their teams
- Dashboard is referenced in quarterly board meetings or audits

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

Risk Plays

Making Human Risk Visible and Actionable

The **90-Day Human Risk Playbook** is designed to help organizations move from reactive to proactive risk management. Within that framework, the **Risk Plays** provide a focused path to identify high-risk cohorts, reduce exposure, and show measurable progress in just 90 days.

These plays address the behaviors most often exploited by attackers — Social Engineering, Insider Threat, Account Compromise, Data Leakage, and Malware Exposure. By applying Human Risk Management principles, each play shifts the approach from broad, generic policies to targeted interventions that reduce the probability of incidents and prove ROI.

Expected Outcomes of Risk 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.

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 across multiple attack vectors (e.g., insider threat

indicators, account compromise configurations, or repeated malware triggers) and enroll them in tailored interventions.

Prioritization of interventions

focus resources where behavior, access, and exposure converge, such as reducing phishing click rates by 8% in heavily targeted cohorts and cutting anomalous file transfers in critical insider threat roles by 15%.

Reduced incident exposure

drive measurable decreases in compromise risks, including a 20% reduction in shadow IT usage, 30% fewer executable file downloads from unverified sources, and a 50% reduction in repeat malware-triggering employees within 90 days.

Improved detection and reporting

increase phishing and malware reporting rates by 10–20% across high-risk cohorts, decrease time-to-remediate account misuse from 10 days to under 48 hours, and raise policy adherence training completion in insider-risk populations by 20%.

Executive and board alignment

deliver metrics that prove progress, such as increasing MFA coverage in privileged users from 85% to 98% and improving behavior scores by 10–15 points across social engineering, account compromise, and data-handling cohorts.

Together, these initiatives transform risk management from a reactive, incident-driven function into a proactive, data-driven discipline — reducing the probability of breaches and building executive confidence that human risk is being managed at scale.

Why Human Risk Management (HRM) Is Critical to Reducing Risk Exposure

Cyber risk is no longer just a technical challenge—it's a **human behavior challenge**. HRM gives organizations the tools to identify, understand, and influence the human side of security before it becomes an incident. Rather than reacting to incidents, HRM enables a **proactive strategy** that surfaces patterns of risky behavior and intervenes before harm occurs.

Reactive vs. Proactive: The Shift That HRM Enables

Traditional (Reactive) Approach:

- **Incident occurs**, then investigate and discipline.
- Often lacks context on *why* the behavior occurred.
- Employee is NOT part of the process - they are the subject only
- Compliance training treats all employees the same, regardless of behavioral risk
- Fails to show long-term behavior change.

According to “Risky Business” report, 74% of organizations focus on reactive policies like security training after violations—yet they lack insight into pre-incident behavior patterns.

HRM-Driven (Proactive) Approach:

- **Surfaces early indicators** like failure to report phishing simulations or unsafe file sharing.
- Leverages data from multiple tools to build a **risk-informed user profile**.
- Targets high-risk individuals with **just-in-time interventions**, not blanket policies.
- Contextualizes users with the greatest exposure — factoring in not only their behaviors, but also how targeted they are and the level of access or impact they have on the business.
- Tracks improvement over time to show ROI.
- Celebrates the wins to avoid “us vs. them” culture

The report shows that 10% of employees account for 73% of all risky behavior within their organizations while 78% of employees actually help to reduce exposure more than they add to it.

The Role of HRM in Cultural and Operational Maturity

HRM helps security teams move from compliance checklists to **continuous behavior improvement**. It enables:

- Risk reduction at the individual and group level
- Better prioritization for security teams
- A measurable way to communicate improvement to executives and boards

As the report notes, mature HRM programs not only reduce risk—they “make human risk visible, quantifiable, and actionable,” which builds executive trust and cultural momentum.

Final Takeaway

Reactive security reacts to today's threat. HRM prevents tomorrow's.

It shifts organizations from responding to problems toward *reducing the probability that they'll happen at all*. Backed by real-world data, HRM empowers security teams to act on risk, not just policy—and that's how you protect the business at scale.

Social Engineering Risk Cohort

Making Human Risk Visible and Actionable

Social Engineering Exploits People, Not Just Technology. Unlike traditional cyberattacks that target systems, social engineering manipulates human psychology. Attackers exploit trust, urgency, curiosity, fear, and even helpfulness to trick people into revealing sensitive information or taking harmful actions — like clicking malicious links or transferring funds.

For too long, programs have been putting phishing simulation click rates in front of boards — and that is not the risk metric the business should be focused on. Click rate alone ignores critical factors that define real risk, such as: Who is targeted most? Who has access to the “crown jewels”? Who is protected with measures like MFA? All of these influence risk, yet leadership is often shown a single vanity metric instead.

An effective HRM strategy reframes the conversation, prompting better questions and metrics that leadership can act on — so we focus on reducing true risk, not just reporting on it:

- What is my click rate within my “heavily targeted employees” cohort? This is where behavior meets external threats (real risk).
- What is my click rate within my privileged access user cohort?
- What is my click rate within my privileged access cohort who also are targeted 5+

times per month by malicious emails?
(larger risk, increase blast radius)

- What % of my clickers have MFA in place to protect them?

Once we have a granular view of risk, we can design programs and policies that actually make a difference — instead of targeting large groups based on a single metric. For years, programs have treated all “clickers” the same, and it’s not working. It’s time to stop the blanket approach and focus on targeted interventions that truly move the needle.

Framework Alignment Cheat Sheet

Framework	Relevant Areas	How It Relates to Social Engineering
MITRE ATT&CK	- T1566: Phishing- T1204: User Execution - T1199: Trusted Relationship	Social engineering appears in the Initial Access and Execution phases. It maps to phishing, user interaction with malicious content, and abuse of trusted relationships.
NIST CSF	- PR.AT: Awareness Training - PR.AC: Access Control - DE.CM: Monitoring- RS.RP: Response Planning	NIST emphasizes training, access restrictions, and incident planning to detect and respond to human-driven threats like phishing and impersonation.
ISO/IEC 27001	- A.7.2.2: Security Awareness - A.9: Access Control - A.16: Incident Management	ISO integrates social engineering risk into governance, requiring formal training, access policies, and structured responses to manipulation-based attacks.

Examples of Data needed to power this cohort:

- **Events** - Observable user actions that indicate susceptibility or strength against social engineering tactics.
 - » Clicked on Real Phish
 - » Clicked on Simulated Phish
 - » Reported a Real Phish
 - » Reported a Simulated Phish
 - » MFA or No MFA
- **Threats**: Signals of real-world adversarial activity targeting the employee.
- Employee targeted with malicious email (data from Email Gateway)
- **Impact Modifiers**: Factors that amplify the potential damage if a social engineering attack succeeds.
 - » Employee has Elevated Access
 - » Executive or High-Trust Role
 - » Employee is on Leaver Status

No matter how strong your firewalls, encryption, or endpoint security are, a single human mistake can bypass them all. Social engineering is often the doorway to larger attacks like ransomware, data breaches, or supply chain compromises.

And attackers are getting smarter. With AI-generated phishing emails, deepfakes, and highly targeted spear-phishing campaigns such as Business Email Compromise, they can convincingly impersonate executives or vendors — making their requests nearly indistinguishable from the real thing.

Impact to Organizations

- Data breaches and regulatory violations (e.g., GDPR, HIPAA)
- Financial fraud or loss (e.g., wire transfer scams)
- Ransomware or malware infections
- Loss of reputation and customer trust

Play - Decrease Exposure to Social Engineering

Goal:

Implement a Human Risk Management (HRM) program to combat social engineering by pinpointing and influencing the behaviors that leave employees vulnerable to phishing, pretexting, baiting, and other human-targeted attacks. For organizations in the “walk” or “run” phase of HRM, this means moving beyond annual training and reactive incident reviews to proactively measure and reduce behavioral risk using simulation results, reporting cadence, and real-world near-misses.

The ultimate objective is to lower both the likelihood and impact of social engineering attacks by continuously identifying, tracking, and shaping human behavior to align with secure practices.

Step by Step:

Mature the way we detect and communicate social engineering—and focus on the employees who matter most!

An effective HRM program for social engineering acknowledges that **not all behaviors are equal**, and **not all employees pose the same level of risk**. You need data and context to act.

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

- Reduce phishing click rates among heavily targeted employees
- Increase phishing report rates in privileged access cohorts
- Achieve complete MFA coverage for employees identified as repeat clickers
- Improve behavior scores within social engineering risk cohorts

What KPIs do we want to report on to reflect true social engineering exposure?

Here are examples of what modern HRM programs report:

- % of clickers who are targeted with malicious emails
- % of employees with elevated permissions
- % of employees with **clicks + elevated access + external threats**
- % of clickers with no **MFA detected**

Align on the risk cohort focus:

Once you narrow in (e.g., “privileged access employees with repeat clicks”), you can drive targeted engagement **instead of treating every user action the same.**

Step ②: Dependencies

To shift from generic phishing exercises to risk-focused HRM, you’ll need a few data sources:

- **Phishing Simulation Platform: Simulation clicks and reports**
- **Secure Email Gateway** (malicious email targets, real phish clicked/reported)
- **Security Awareness LMS** (training completion, quiz scores)
- **IAM Data** (to segment by access levels, department, and tenure)



Supported by:

- » Identity and Access Management (IAM) Team
- » Security Operations
- » HR or Compliance
- » Executive Sponsor (e.g., CISO, VP of People, GC)

Step ③: Prerequisites / Setup

- Set up API connections to the data sources to power your more focused risk reporting (typically 1-3 integrations)
- Filters for segments created for fast reporting in the areas that you are focused on (e.g. employees who clicked, heavily targeted, w/ no MFA)
- Communication to leadership they will be seeing new metrics in future reports
- Stakeholder sign-off on tone and frequency of recognition “nudges” when an employee moves from risky (click) to vigilant (report)

Step ④: Create Execution Plan

Step 1: Identify High-Risk User Segments

- » Pull 90-day behavior and threat trends from Unify (phish clickers, heavily targeted)
- » Cross-reference with high-value roles (Elevated Access)
- » Benchmark segments who have different risk profiles specific to this risk area

Step 2: Analyze Threat Patterns

- » Review recent phishing and vishing (if applicable) campaign data
- » Flag impersonation trends (CEO fraud, invoice scams, etc.)

Step 3: Build Targeted Learning Path

- » Send custom “thank you nudge” for all reporters
- » Assign 3–5 minute scenario-based modules focused on real tactics to employees under threat
- » Include pretexting, suspicious sender cues, and reporting protocol

Step 4: Launch Campaign with Context

- » Message impacted employees with clear framing: “You’re in a high-risk role—here’s how to stay secure.”
- » Optional: Include manager overview to support coaching

Step 5: Reinforce with Nudges & Retest

- » Deliver in-the-moment nudges (e.g. after real phish attempts)
- » Schedule a follow-up phishing simulation to measure behavior change (ROI)
- » Report on behavior changes found post intervention

Step 5: Avoid Pitfalls (Lessons Learned)

- Don’t treat all employees equally—this is a **risk-based**, not compliance-based play
- Avoid generic training—scenario-based modules have stronger retention
- Don’t skip manager briefing (manager score cards)—support from direct leadership drives participation
- Measure more than clicks—include multiple metrics for increased context for better decision making
- Don’t just assign training without sharing the exhibited risk to the employee. The more they understand, the more they will buy in and own the risk

Step 6: Make this real, report the wins

Example OKR’s or Goals:

- Increase Report Rate by 10% in the “Elevated Access” cohort
- Decrease click rate by 8% in “heavily targeted employee” cohort
- Increase Behavior Score by 10 points in “social engineering risk” cohort

Insider Threat Risk Cohort

Insider threats stem from individuals within the organization—employees, contractors, or third-party partners—who either **maliciously** or **accidentally** compromise data, systems, or security processes. These threats are particularly dangerous because insiders already have a degree of **trusted access** and may bypass many traditional perimeter defenses. This play is for our customers who are in the “**run**” phase of their program.

Insider incidents aren't always about malice. More often, they involve **negligence**, **poor security hygiene**, or **unintentional actions** that lead to exposure or compromise—think uploading sensitive data to personal drives, misconfiguring permissions, or falling for targeted social engineering.

And like social engineering, insider threats:

- Exploit human behavior and organizational blind spots
- Bypass firewalls and endpoint defenses
- Create high-impact, low-visibility risk vectors

Why Traditional Approaches Fall Short

Many organizations still approach insider threat with:

- After-the-fact investigations
- Generic data loss prevention (DLP) policies
- **Heavy surveillance tactics** that can harm trust

But they fail to ask:

“Who has access to sensitive assets, and what behaviors indicate *elevated risk*?”

And instead of proactive detection and support, organizations often treat every insider incident as a policy failure—when in reality, it's often a **cultural**, **visibility**, or **training issue**.

Framework Alignment Cheat Sheet

Framework	Relevant Areas	How It Relates to Insider Threat
MITRE ATT&CK	- T1078: Valid Accounts - T1081: Credentials from Password Stores - T1056: Input Capture	Captures both misuse of legitimate access and techniques used by insiders or external actors with internal credentials.
NIST CSF	- ID.AM: Asset Management - PR.AC: Access Control - DE.CM: Anomalous Behavior Detection - RS.RP: Response Planning	Emphasizes visibility into access, behavioral monitoring, and structured response to insider events.
ISO/IEC 27001	- A.9: Access Control - A.10: Cryptography - A.12: Operations Security - A.16: Incident Management	Requires policy and process controls around identity, access, and secure data handling—key to insider threat governance.

Metrics That Actually Measure Insider Risk

Boards and security leaders need to move beyond static reports (e.g., policy violations, access logs) and instead focus on **behavioral and contextual metrics** that surface **who is most likely to become an insider threat**—whether intentional or not.

Here are key risk-aligned questions your HRM strategy should drive:

- **Who has privileged or “crown jewel” access, and how is it being used?**
 - Not all privileged employees are equal—track who accesses sensitive data frequently, moves large amounts, or breaks patterns.
- **Which employees show risk-indicating behaviors?**
 - Examples include downloading large files off-hours, accessing systems outside their job role, or bypassing MFA.
- **Are employees combining high access, behavioral anomalies, and poor security posture?**
 - This intersection highlights the *true insider threat cohort*.

Examples of Data Needed to Power this Cohort:

- **Events** - Observable user actions that indicate susceptibility or strength against Insider Threat
 - » Download data in bulk
 - » Moved data externally
 - » Accessed sensitive systems or data outside business hours
 - » DLP policy violations
- **Threats**: Signals of real-world adversarial activity targeting the employee.
 - » Targeted with malicious emails
 - » Targeted with malicious emails + malware detections
- **Impact Modifiers**: Factors that amplify the potential damage if a social engineering attack succeeds.
 - » "Leaver Status" - employee is leaving the business (HR signal)
 - » Employee is part of business reorganization
 - » "New Hire" - in first 6 months of employment
 - » Employee has Elevated Access
 - » Provisioning rights

Maturing the Strategy

To address insider threat meaningfully, organizations must:

- Build **behavioral baselines** using usage patterns and anomalies.
- Segment employees by **access level**, **role criticality**, and **risk behavior**.
- Flag and engage employees early—before mistakes become incidents—through tooling, positive just-in-time guidance (training)
- Replace blanket surveillance with **trust-building and targeted intervention** strategies.

Most importantly, **stop treating insider threats as purely a compliance issue**. It's a **human risk** issue.

Play – Decrease Exposure to Insider Threat

Goal:

Adopt a **Human Risk Management (HRM)** program to address **Insider Threat** by identifying and influencing behaviors that could lead to unintentional or malicious internal compromise. This is for mature programs, typically in the **“run phase”** of HRM.

We need to move beyond static access logs or reactive incident reviews and start **proactively measuring and reducing behavioral risk** based on access, anomalies, and usage patterns.

Ultimately, the goal is to **reduce the likelihood and impact of insider threats** by continuously identifying high-risk roles and behaviors and engaging the right employees with the right intervention—**before** an incident occurs.

Step by Step:

Mature the way we detect and communicate insider risk—and focus on the employees who matter most!

An effective HRM program for insider threat acknowledges that **not all access is equal**, and **not all employees pose the same level of risk**. You need data and context to act.

Step ❶: Set Clear Goals

- Identify and engage employees with elevated insider threat risks
- Reduce anomalous data movement outside approved systems
- Improve training and policy adherence in high-risk cohorts
- Decrease insider access misuse alerts in critical roles

What KPIs do we want to report on to reflect true insider threat exposure?

Here are examples of what modern HRM programs report:

- % of employees with elevated access + behavioral risks
- # of employees showing data movement outside expected systems or hours
- % of privileged employees lacking MFA or training completions
- Incidents of policy violations by role (e.g. unapproved data uploads/downloads)

Align on the risk cohort focus:

Once you narrow in (e.g., “privileged access employees with risky data movement”), you can drive targeted engagement **instead of treating every user action the same**.

Step 2: Dependencies

To shift from generic insider threat monitoring to **risk-focused HRM**, you'll need a few data sources:

- **Identity and Access Data** (IAM tool for access levels and department roles)
- **UEBA/Behavior Monitoring** (e.g., file movement, odd hours, policy violations)
- **Security Training & Policy Records** (LMS or HR system)
- **Data Movement Logs or DLP Tools**



Supported by:

- » Identity and Access Management (IAM) Team
- » Security Operations / Insider Threat Analysts
- » HR or Compliance
- » Executive Sponsor (e.g., CISO, VP of People, GC)

Step 3: Prerequisites / Setup

- Set up API or data connections to integrate identity, behavior, and policy systems
- Create filters/segments for:
 - » Employees with elevated access
 - » Employees with repeated anomalies (file movement, shadow IT, privilege misuse)
 - » Employees lacking training or MFA
 - » New Hires, typically a higher risk for Insider Threat
 - » Employees leaving the business + DLP violations
- Communicate to leadership that insider threat metrics will be **contextual, risk-based** and **actionable**, not purely access or compliance logs
- Get stakeholder sign-off on tone and cadence of interventions (e.g., nudges, manager coaching)

Step 4: Create Execution Plan

Step 1: Identify High-Risk User Segments

- » Pull 90-day behavior trends (e.g., off-hours access, downloads, DLP violations)
- » Cross-reference with privileged roles or sensitive system access

Step 2: Analyze Behavior and Exposure Patterns

- » Review risk cohort
- » Define "owner of risk profile" and plan to mitigate these risks

Step 3: Build Program Response to risk profile

Example:

- » NIST SP 800-53 Recommendations
 - **PS-4 Personnel Termination & PS-5 Personnel Transfer:** Revoke privileges immediately upon role change or departure.
- » ISO/IEC 27001 (Annex A) Recommendations; People- Focused Controls
 - **Awareness, Education & Training (A 6.3):** Mandate and track completion of insider-risk and social-engineering training.
- » MITRE Insider Threat Guidance
 - **Adopt a Multi-Sensor, Multi-Perspective Approach:** Insider risk is a human challenge—combine behavioral, organizational, cyber, and physical indicators rather than relying solely on log data

Step 4: Reinforce and Reassess (Week 4–5 – Security Ops)

- » Use behavioral nudges after risky events (e.g., uploading unapproved docs)
- » Conduct access reviews or simulated insider risk exercises
- » Track behavior change over time (e.g., fewer incidents, better tool usage)

Step 5: Avoid Pitfalls (Lessons Learned)

- Don't treat every elevated access user the same—**context matters**
- Avoid relying solely on DLP alerts—**behavioral risk is more than policy violations**
- Don't skip manager coaching—they are key to reinforcing secure practices
- Measure **behavioral improvement**, not just compliance task completion
- Reactive measures are usually too late, flag risk early and work with the Insider Threat / Investigations teams along with the Training / Awareness team.

Step 6: Make this real, report the wins

Example OKR's or Goals:

- Identify top 10% of employees with **elevated insider threat risk indicators** and create tailored engagement
- Decrease **anomalous file transfers** in critical roles by 15%
- Increase policy adherence training completion rate in high-risk cohort by 20%
- Reduce number of **access misuse alerts** within key departments by 25%

Account Compromise Risk Cohort

Account compromise is one of the most dangerous and underreported forms of cyber risk. It occurs when a threat actor gains unauthorized access to a legitimate user account—often via credential theft, phishing, session hijacking, or brute-force attacks. Once inside, they operate as a trusted user, enabling lateral movement, privilege escalation, data theft, and fraud—all while avoiding detection.

Account compromise is not just a technical failure; it's a human-layer security challenge. Whether due to password reuse, weak credentials, phishing, or poor MFA hygiene, human behavior plays a central role in account takeover events.

We're Focusing on the Wrong Metrics

Security programs have long emphasized password resets or authentication compliance metrics, but **those don't reflect true compromise risk**. What's missing is context:

- Who has elevated access?
- Who has poor MFA posture?
- Who is being actively targeted?
- Who reuses passwords or ignores identity alerts?

We can't reduce compromise risk if we're only measuring login events and training completion. We need to measure **who is most exposed, who is most valuable, and who is most vulnerable**.

Framework Alignment Cheat Sheet

Framework	Relevant Areas	How It Relates to Account Compromise
MITRE ATT&CK	- T1078: Valid Accounts - T1556: Modify Authentication Process - T1550: Use Alternate Authentication Material	Covers credential theft, token abuse, session hijacking, and misuse of valid accounts—core techniques in compromise events.
NIST CSF	- PR.AC: Access Control - PR.IP: Identity Protection - DE.CM: Anomalous Behavior Detection - RS.AN: Incident Analysis	Focuses on controlling identity, enforcing MFA, detecting anomalies, and responding quickly to access misuse.
ISO/IEC 27001	- A.9: Access Control - A.10: Cryptography - A.12.4: Logging and Monitoring - A.16: Incident Management	Emphasizes strong identity controls, session monitoring, credential protection, and response planning.

HRM-Driven Metrics that Actually Reflect Risk

Here are the types of questions your HRM strategy should drive—ones that help you surface and mitigate real account compromise risk:

- **Who are my employees with elevated access AND no MFA?**
 - These are high-value accounts without a security barrier.
- **Who logs in from multiple geographic locations or unknown devices within short timeframes?**
 - Signs of possible credential sharing or token hijacking.
- **Which employees have re-used breached credentials (per threat intelligence) but haven't updated them?**
 - Known vulnerable employees.
- **What is my compromise rate among "privileged + targeted" cohorts?**
 - This reveals risk convergence—value + exposure.

Examples of Data needed to power this cohort:

- **Events:** Observable user actions that indicate susceptibility or strength against social engineering tactics.
 - » Clicked on a real credential phish
 - » Clicked on a simulated credential phish
 - » Disabled or bypassed MFA
 - » Reused Password
 - Or breached password on dark web

- **Threats:** Signals of real-world adversarial activity targeting the employee.
 - » User Targeted with real credential phish
 - » Device Login multiple geographies
- **Impact Modifier:** Factors that amplify the potential damage if a social engineering attack succeeds
 - » Employee has Elevated Access

Common Attack Techniques Include:

- Credential Phishing: Capturing usernames and passwords via fake login pages
- Password Spraying & Brute Force: Automated login attempts using common passwords
- Token Hijacking: Capturing session tokens to impersonate employees
- OAuth Abuse: Malicious app permissions granting long-term access
- MFA Fatigue: Flooding employees with MFA prompts to gain approval

It's a Silent Breach Vector

Account compromise often **bypasses traditional detection methods**, since the attacker is using valid credentials. By the time it's caught, damage has already occurred—access granted, data exfiltrated, and trust eroded. Worse, compromised accounts are often **used as launchpads for further internal attacks**, including phishing, fraud, and privilege escalation.

Impact to Organizations

- **Data Breaches:** Compromised accounts often enable access to cloud storage, messaging systems, or internal apps
- **Financial Fraud:** Wire transfers, fraudulent vendor payments, and BEC scams
- **Reputation Damage:** Trust lost with partners and clients due to email abuse or impersonation
- **Compliance Violations:** Unauthorized access to regulated data (e.g., GDPR, HIPAA, SOX)
- **Lateral Movement & Ransomware:** Used to establish persistence and escalate access

Play – Decrease Exposure to Account Compromise

Goal:

Adopt a **Human Risk Management (HRM)** program to reduce the likelihood and impact of **account compromise** by addressing the behaviors, configurations, and vulnerabilities that enable unauthorized access to employee accounts.

We need to move beyond authentication compliance checks and after-the-fact incident response. Instead, we must leverage behavioral, access, and control data to measure *who is most vulnerable*, *who is most valuable*, and *who is most exposed*.

Ultimately, the goal is to surface account compromise risk **before** an attacker does—through visibility, segmentation, and human-centric mitigation.

Step by Step:

Modernize how we detect and communicate account compromise risk—and focus on the employees who matter most.

An HRM-aligned approach to account compromise understands that **not all employees and accounts are created equal**, and security posture isn't just about MFA checkboxes—it's about behavior, access, and threat targeting

Step ①: Set Clear Goals

- Achieve full MFA coverage for employees with privileged access
- Reduce login anomalies across geographic and device patterns
- Shorten remediation time for account misuse incidents
- Improve authentication hygiene and behavior scores

What KPIs do we want to report on to reflect true account compromise exposure?

Examples of modern HRM account compromise metrics:

- % of employees with **elevated access + no MFA**
- % of employees with **reused or breached credentials**
- % of logins from **anomalous geo/IP/device patterns**
- Number of employees with **token-based sessions** exceeding standard duration
- Volume of **privileged employees** flagged for high-risk authentication events

Align on the risk cohort focus: Focus on where value, vulnerability, and threat exposure intersect. For example:

- Privileged access employees with no MFA
- Employees targeted by phishing AND who use weak or breached passwords
- Employees logging in from multiple IPs and locations with high access levels

Step ②: Dependencies

To evolve your account compromise detection and mitigation strategy, you'll need access to:

- **Identity and Access Data** (IAM/SSO platform: Okta, Azure AD, etc.)
- **Authentication Logs & Geo-IP Patterns** (via SIEM or Identity Provider)
- **Credential Exposure Data** (via dark web monitoring or threat intel feed)
- **MFA Enrollment & Enforcement Status**
- **Phishing & Real Attack Targeting Data** (from email security or XDR)



Supported by:

- » IAM Team
- » Security Operations / Identity Engineering
- » Threat Intelligence Team
- » Executive Sponsor (e.g., CISO, CIO, VP of Security)

Step ③: Prerequisites / Setup

- Establish API or direct integrations with IAM, secure email gateway, and SIEM/XDR
- Create filters or cohorts for:
 - » Employees with high access + no MFA
 - » Employees with anomalous login activity (geo/IP/device patterns)
 - » Employees with weak or reused credentials
 - » Employees frequently targeted by phishing and spoofing
- Communicate to leadership that **account compromise metrics will reflect real exposure**, not just policy compliance
- Align with stakeholders on response flows, training cadence, and messaging tone (nudges, coaching, enforcement)

Step 4: Create Execution Plan

Step 1: Identify High-Risk User Segments

- » Pull 90-day authentication logs and flag:
 - Privileged access with weak auth controls
 - Repeated MFA push attempts (MFA fatigue)
 - Multiple IP logins within short timeframes

Step 2: Analyze Threat and Exposure Patterns

- » Correlate with email threat data (phishing volume, spoofing attempts)
- » Match compromised credential reports against user population
- » Identify reuse of breached passwords (via threat intel or external feeds)

Step 3: Build Targeted Plan to drive down risk

Examples:

- » **NIST (SP 800-63B & SP 800-53)**
Compromised Credential Screening & Revocation: Check all new and changed passwords against breach corpora and promptly suspend or revoke any authenticator proven to be compromised.
 - Account Lockout & Throttling (AC-7): Lock or delay accounts after a small number of failed logins to thwart brute-force and credential-stuffing attacks.
- » **ISO/IEC 27001 & 27002**
 - Mandate MFA (e.g., hardware tokens, biometrics) for all high-risk accounts.
- » **MITRE ATT&CK® Mitigations**
 - M1018 – User Account Management: Enforce end-to-end lifecycle controls (creation, modification, deactivation) and least-privilege for every account.
 - M1036 – Account Use Policies: Configure lockouts, inactivity timeouts, login-time restrictions, and session-timeout policies to limit credential abuse windows.
 - M1015 – Active Directory Configuration: Use group policies to enforce strong password rules, MFA enforcement, and account siloing for high-value roles.

Step 4: Launch Targeted Campaign

- » Notify affected employees: "Your role or access level makes your account a high-value target. Here's how to protect it."
- » Optionally, include manager briefings and coaching materials to reinforce

Step 5: Reinforce and Reassess

- » Re-assess login patterns post-intervention
- » Conduct controlled phishing + credential harvesting simulations to track impact
- » Partner with other stakeholders to create plans to target this risk cohort.

Step 5: Avoid Pitfalls (Lessons Learned)

- Don't rely solely on MFA enforcement—it must be **measured by implementation AND behavior**
- Don't assume you have 100% MFA compliance, use the data
- Avoid one-size-fits-all enforcement—**contextual risk** matters (e.g., traveling execs vs. desk-bound employees)
- Don't ignore credential hygiene—**password reuse + phishing** is a leading cause of compromise
- Don't skip the dark web exposure checks—your employees may already be exposed
- Ensure close coordination between **IAM, Awareness, and Incident Response** teams

Step 6: Make this real, report the wins

Example OKR's or Goals:

- Identify and secure top 10% of accounts with **compromise-prone configurations** (e.g., no MFA, reused credentials, high-value access)
- Reduce login anomalies by 20%
- Decrease time-to-remediate account misuse indicators from 10 days to <48 hours
- Increase MFA coverage in privileged user population from 85% to 98%
- Improve behavior score (e.g., risk-aware authentications, password hygiene) by 15 points in targeted cohorts

Data Leakage Risk Cohort

Data leakage is a critical and growing security risk—where sensitive or regulated data is exposed, mishandled, or exfiltrated, either accidentally or intentionally. It occurs when employees move, share, or store data outside of approved systems or controls, such as downloading files to personal devices, emailing documents externally, uploading to unsanctioned apps (shadow IT), or misconfiguring access permissions.

While it's often treated as a technical or compliance failure, **data leakage is fundamentally a human-layer risk**—driven by poor habits, productivity shortcuts, lack of awareness, or even malicious intent.

We're Focusing on the Wrong Metrics

Traditional DLP (Data Loss Prevention) programs focus on event logs or blocked actions, but these **don't reflect actual risk posture**. They often overlook:

- Who consistently interacts with sensitive data?
- Who uses unapproved tools?
- Who bypasses controls or ignores policy nudges?
- Who has a pattern of risky file behavior?

You can't reduce data leakage if you're only tracking what gets blocked. You need visibility into **behavior, intent, and context**—who poses the most risk, and why?

Framework Alignment Cheat Sheet

Framework	Relevant Areas	How It Relates to Data Leakage
MITRE ATT&CK	- T1048: Exfiltration Over Alternative Protocol - T1020: Automated Exfiltration - T1537: Transfer Data to Cloud Account	Maps to techniques used to move sensitive data off-network or to unsanctioned platforms.
NIST CSF	- PR.DS: Data Security - PR.IP: Protection Processes and Procedures - DE.CM: Monitoring - RS.AN: Analysis	Addresses detection, protection, and response tied to data handling and exfiltration behavior.
ISO/IEC 27001	- A.8: Asset Management - A.9: Access Control - A.13: Communications Security - A.16: Incident Management	Emphasizes classification, access rules, and monitoring of data movement to detect and prevent leaks.

HRM-Driven Metrics that Actually Reflect Data Leakage Risk

These are the kinds of questions your Human Risk Management strategy should help you answer:

- **Who frequently downloads or uploads sensitive data outside of normal business apps?**
→ This may indicate shadow IT usage or policy evasion.
- **Who shares files externally from cloud storage platforms?**
→ Track which employees are moving sensitive data into less-controlled environments.
- **Which employees have triggered multiple DLP alerts but haven't received targeted training?**
→ Missed opportunities for intervention.
- **What percentage of risky file transfers are coming from new hires or offboarding employees?**
→ Lifecycle transitions are high-risk moments for accidental or malicious leaks.
- **Which employees with elevated access have transferred files to personal or unknown domains?**
→ Behavior + access = high potential impact.

By identifying **risk cohorts**—employees with elevated access + frequent data interaction + poor tool hygiene—you can move from reactive to proactive protection.

Examples of common Events (behaviors), Threats, and Impact Modifiers needed to power this view of risk:

- **Events:** Observable user actions that indicate susceptibility or strength against social engineering tactics.
 - » Shared sensitive information externally
 - » Used unauthorized apps
 - » Copied internal content to personal cloud or device
 - » Ignored or skipped policy training
 - » DLP violations (multiple)
- **Threats:** Signals of real-world adversarial activity targeting the employee.
 - » Targeted with Malicious emails
 - » Data leaked on dark web
- **Impact Modifier:** Factors that amplify the potential damage if a social engineering attack succeeds
 - » Employee has Elevated Access
 - » Leaving the business
 - » Under performance review
 - » Remote workers

Common Data Leakage Vectors Include:

- **Email Misdelivery:** Sending sensitive attachments to the wrong external party
- **Shadow IT:** Uploading files to unauthorized apps like Dropbox, Box, or personal Gmail
- **USB or Removable Media:** Downloading confidential data to insecure devices
- **Improper Sharing Permissions:** "Anyone with the link" access on confidential documents
- **File Mislabeling:** Sensitive data treated as public or non-classified
- **Screenshots or Copy/Paste** into unapproved systems

It's a Hidden, Habit-Based Risk

Unlike malware or phishing, **data leakage often stems from well-intentioned but insecure behavior**—employees working faster, bypassing slow tools, or misunderstanding policies. That's why detection alone isn't enough.

The real risk lies in **repeat behaviors, high-value roles, and unguarded systems**. Without context, even sophisticated DLP systems miss the human story behind the leak.

Impact to Organizations

- **Data Breaches:** Leaks of customer data, IP, or regulated information
- **Compliance Failures:** Violations of GDPR, HIPAA, PCI-DSS, etc.
- **Loss of Competitive Advantage:** IP exfiltration or exposure
- **Brand and Trust Damage:** Loss of customer or partner confidence
- **Legal and Financial Penalties:** Due to mishandling or unauthorized disclosures

Play – Decrease Exposure to Data Leakage

Goal:

Adopt a **Human Risk Management (HRM)** program to address **data leakage risk** by identifying and influencing behaviors that lead to the mishandling or unintentional exposure of sensitive data. This play is best suited for mature HRM programs operating in the **“walk/run phase.”**

We need to move beyond DLP event logs and generic usage policies. Instead, we should proactively track behaviors, context, and access patterns that indicate true data exposure risk—and take targeted, human-focused action **before the leak occurs**.

Step by Step:

Mature the way you identify and communicate data leakage risk—and focus on the employees who matter most.

A modern HRM approach acknowledges that **data risk varies by role, behavior, and access**. Not every document move is a threat, but some user patterns should trigger concern and proactive engagement.

Step ①: Set Clear Goals

- Reduce external file sharing to unauthorized domains
- Decrease use of unsanctioned or shadow IT tools
- Achieve high acknowledgment rates for data handling policies
- Improve behavior scores among data-handling cohorts

What KPIs will help us reflect real human-driven data leakage exposure?

Here are examples of what modern HRM programs report:

- % of employees with frequent external file sharing from sanctioned apps
- % of employees downloading sensitive data to personal or unmanaged devices
- % of “offboarding” employees with recent DLP alerts

- % of privileged employees who move data between apps without approval (e.g., copy/paste from internal to external systems)
- % of data transfers to shadow IT or unauthorized domains
- % of repeat DLP alert generators who haven't completed data handling training

Align on the risk cohort focus: Once you focus on employees with **high access, frequent movement, or poor tool hygiene**, you can build **cohort-specific programs** instead of reacting to every alert the same way.

Step ②: Dependencies

To shift from general DLP reporting to **HRM-powered data risk reduction**, you'll need:

- **Identity and Access Data** (IAM system to know who has access to what)
- **DLP and Data Movement Logs** (e.g., CASB, Endpoint DLP, email/file sharing controls)
- **Shadow IT Monitoring** (visibility into unsanctioned app usage)
- **Security Training & Acknowledgments** (LMS, HR system for tracking user readiness)
- **Behavioral Analytics** (e.g., unusual transfer patterns, bulk downloads)



Supported by:

- » Identity and Access Management (IAM) Team
- » Security Operations / Data Protection Analysts
- » Compliance or Legal
- » Executive Sponsor (e.g., CISO, DPO, GC)

Step ③: Prerequisites / Setup

- Set up API/data connectors to unify data movement, access, and user behavior signals
- Create filters or segments for:
 - » employees who share externally
 - » employees downloading to USB or personal cloud
 - » Employees in transition (new hires, resignations)
 - » Privileged employees with data handling privileges
- Communicate to leadership that future reports will reflect **risk context**, not just blocked/allowed events
 - » Align stakeholders on tone, messaging, and coaching flows for intervention (nudges, learning, manager briefing)

Step 4: Create Execution Plan

Step 1: Identify High-Risk User Segments

- » Pull 90-day data movement logs
- » Flag employees who have:
 - Shared files externally
 - Moved large volumes of data
 - Used unsanctioned storage or collaboration tools
 - Cross-reference with role-based access and DLP events

Step 2: Analyze Patterns

- » Identify top data sources being leaked or mishandled
- » Highlight specific vectors (e.g., Box → Gmail, USB → PDF export)
- » Look for clusters: offboarding employees, new hires, contingent workers, or departments with repeat offenses

Step 3: Build Response plan against risk

Examples:

- » NIST: Employee Engagement:
 - **Policy Roll-out & Awareness (AT-2):**
 - Regular, role-based training on data-handling policies and hands-on DLP demos (“see how your own files are classified”) for employees who are showing risky behaviors.
 - Champions Program: “data-classification champions” program where volunteers from each team help train peers on labeling/safe-sharing.
 - **Just-In-Time Microlearning:**
 - Trigger short guidance modules (“why we block that export”) after a user hits a DLP block or exception
- » ISO/IEC 27001 & 27002 Recommendations

- **Data Classification & Handling Training (A.8.2):**
- Hands-on workshops where employees practice classifying real documents and see the DLP outcomes.
- Quarterly “data-tagging challenges” with gamified rewards to reinforce correct labeling.
- **Incident Reporting & Feedback Loops (A.6.8):**
- Simplify “report a false positive” or “request transfer exception” via one-click forms in your DLP alerts.
- Monthly “DLP digest” newsletters highlighting near-misses and lessons learned, with anonymized examples.

Step 4: Monitor Change

- » Use in-the-moment nudges (e.g., after external sharing or download)
- » Re-assess movement patterns to track impact
- » Optional: simulate “near miss” exercises with decoy data access attempts

Step 5: Avoid Pitfalls (Lessons Learned)

- Don’t treat all data movers as threats—**context matters**
- Avoid broad-brush DLP block policies that harm productivity—**target the patterns, not the people**
- Don’t skip manager briefings—they’re often best positioned to guide secure workflow changes that are specific to that group and how they work!
- Look beyond compliance alerts—you **need behavior, frequency, and intent to understand true risk**
- Assume employees *want* to do the right thing—support them with frictionless, clear guidance

Step 6: Make This Real—Report the Wins

Example OKRs or Goals:

- Reduce external file sharing to personal domains by 20%
- Increase data handling policy acknowledgment rate to 95% in “data-handling” roles
- Reduce shadow IT usage by 30%
 - » Improve behavior scores for “data-handling” cohorts by 15+ points over a 60-day period

Malware Exposure Risk Cohort

Malware is not just a technical threat—it's a **human risk vector**. Modern malware infections are typically enabled by human action: clicking a malicious link, opening a disguised attachment, disabling security controls, or plugging in an infected USB. Attackers exploit behavior just as much as code.

Malware comes in many forms—ransomware, trojans, keyloggers, backdoors—and often serves as a **launch point for broader attacks** like data exfiltration, credential theft, or infrastructure takedown.

We're Focusing on the Wrong Metrics

Too many programs still track malware risk using volume-based indicators—antivirus detections, system infections, endpoint alerts. But these **don't tell us who's most at risk or why**.

We need to stop measuring the **outcome** and start tracking the **exposure** that leads to malware incidents. That means asking:

- Who is engaging with known malicious content?
- Who is bypassing warnings and running unknown files?
- Who is disabling endpoint protections?

- Who is in a high-value role with broad access and a history of risky behavior?

We can't reduce malware risk by treating every user the same. We need to identify **who's exposed, who's vulnerable, and who can cause the most damage**.

Framework Alignment Cheat Sheet

Framework	Relevant Areas	How It Relates to Malware Risk
MITRE ATT&CK	- T1204: User Execution - T1059: Command and Scripting Interpreter - T1566: Phishing - T1027: Obfuscated Files	Describes how malware is delivered, executed, and hidden—often via user interaction or social engineering.
NIST CSF	- PR.DS: Data Security - PR.IP: Protection Processes - DE.CM: Monitoring - RS.MI: Mitigation	Guides prevention, detection, and mitigation of malware across people, process, and technology layers.
ISO/IEC 27001	- A.12.2: Protection from Malware - A.13.2: Information Transfer Policies - A.16: Incident Management	Requires malware protection, safe file handling policies, and incident response—linked to human activity.

HRM-Driven Metrics That Actually Reflect Malware Risk

These are the questions your HRM strategy should help answer—and communicate clearly to leadership:

- **What is the rate of malware events among employees who bypass browser or email warnings?**
→ Indicates a behavior risk, not just a technical gap.
- **What % of employees download and execute unverified files from the internet?**
→ Tracks high-risk behavior patterns over time.
- **Which employees have been involved in repeat malware infections within the past 12 months?**
→ Signals unaddressed behavioral vulnerabilities.
- **Which employees with elevated access have poor endpoint hygiene (e.g., outdated AV, missing patches)?**
→ High-value employees with weakened defenses.
- **Which employees clicked on malware-laced phishing links that bypassed initial filters?**
→ Behavior + targeting = actionable risk cohort.

When you combine technical alerts with behavioral telemetry, you stop tracking **what** malware was blocked and start measuring **who** is most likely to bring it in.

Examples of common Events (behaviors), Threats, and Impact Modifiers needed to power this view of risk:

- **Events:** Observable user actions that indicate susceptibility or strength against social engineering tactics.
 - » Clicked on a malicious link or file
 - » Bypassed browser or email security warnings
 - » Downloaded unverified executables
 - » Removable media
- **Threats:** Signals of real-world adversarial activity targeting the employee.
 - » User receives emails with malware payload
 - » Endpoint flagged suspicious behavior or malware attempt
- **Impact Modifier:** Factors that amplify the potential damage if a social engineering attack succeeds
 - » Employee has Elevated Access
 - » Lacks endpoint protection enforcement

Common Infection Techniques Include:

- **Malicious Email Attachments:** Executables disguised as documents (e.g., invoice.pdf.exe)
- **Drive-by Downloads:** Malware installs when visiting compromised or malicious websites
- **Malicious Macros:** Embedded in office files prompting employees to “enable content”
- **USB-Based Infection:** Physical devices dropped intentionally or inserted by internal employees
- **Executable Droppers:** Files that install malware payloads after tricking the user into interaction

It Only Takes One Click

Even with advanced threat detection, EDR, and sandboxing, malware often **succeeds through user behavior**. A single employee running an infected file or ignoring an OS warning can lead to:

- Ransomware outbreaks
- Credential theft via keyloggers
- Network-wide persistence through lateral movement
- Payloads that disable defenses before triggering
- Without behavioral insight, we don’t understand **why infections happen**—only that they did.

Impact to Organizations

- **Operational Disruption:** Ransomware or destructive malware can bring business to a halt
- **Financial Loss:** Downtime, recovery, legal fees, or ransom payments
- **Reputation Damage:** Public disclosure of security failures and potential data compromise
- **Data Exfiltration:** Sensitive internal data siphoned off via backdoors or spyware
- **Regulatory Consequences:** Breach of customer, financial, or healthcare data

Play – Decrease Exposure to Malware

Goal:

Adopt a Human Risk Management (HRM) program to address malware risk by identifying and influencing behaviors that lead to infections. This play is best suited for mature HRM programs operating in the “walk/run phase.”

We need to move beyond endpoint alerts and AV detections. Instead, we should proactively track the human behaviors that trigger malware — clicking malicious links, opening risky attachments, bypassing warnings, or running unverified files — and take targeted, human-focused action before infections spread.

Step by Step:

Mature the way we detect and communicate malware risk—and focus on the employees who matter most!

An effective HRM approach to malware risk recognizes that **technology catches what employees trigger**.

To reduce malware exposure, you must understand **why employees are triggering it in the first place**.

Step 1: Set Clear Goals

- Reduce downloads of unverified executables or unsafe files
- Cut down repeat malware-triggering behaviors
- Improve secure file handling practices across high-risk groups
- Increase malware reporting rates after simulations or nudges

What KPIs should we report on to reflect true malware exposure?

Here are examples of what modern HRM programs report:

- % of employees who run unverified executables from email or browser downloads
- % of repeat malware event employees (3+ incidents in 90 days)
- % of privileged employees with poor endpoint hygiene (e.g., no MFA, outdated systems)
- % of employees with both high click rates *and* high-risk device behavior
- % of employees interacting with malicious USBs or unauthorized apps

Align on the risk cohort focus:

For example, “employees with elevated access who frequently download or execute unknown files” are a more meaningful risk group than all “malware detection” employees.

Step ②: Dependencies

To transition from reactive malware alerts to **proactive malware risk management**, you'll need:

- **Identity and Access Data** (IAM tools to determine privilege levels)
- **EDR / AV Alert Logs** (e.g., malware detections, blocked executables)
- **Email & Web Filtering Tools** (employees bypassing or ignoring file warnings)
- **Device Configuration & Patch Management Data** (endpoints missing updates or AV)
- **Security Awareness Engagement Records** (training participation, simulations)



Supported by:

- » Endpoint & Identity Teams
- » SOC / Malware Triage Analysts
- » Awareness / L&D Teams
- » Executive Sponsor (e.g., CISO, VP of IT, VP of Security Ops)

Step ③: Prerequisites / Setup

- Establish API/data integrations for:
 - » Endpoint alerts
 - » User roles and access levels
 - » Device health status
 - » Training records and user history
- Create filters or segments for:
 - » Employees with 2+ malware-related detections in 90 days
 - » High-access employees who executed unknown files
 - » employees who bypassed security warnings
 - » Devices with unpatched OS or AV disabled
- Communicate to leadership: **new risk-centric malware metrics** are coming that combine user behavior, endpoint status, and threat exposure
- Get stakeholder buy-in for tone and cadence of feedback nudges (supportive, not punitive)

Step 4: Create Execution Plan

Step 1: Identify High-Risk User Segments

- » Pull 90-day malware alert and behavioral event logs
- » Segment employees who executed flagged files, bypassed warnings, or used unauthorized media
- » Cross-reference with roles (admin, finance, IT, etc.)

Step 2: Analyze Threat Patterns

- » Review malware campaign reports:
 - Recent dropper malware delivery methods
 - Fake invoice or resume campaigns
 - USB baiting events
- » Flag campaigns that overlap with high-risk cohort

Step 3: Build Targeted Plan

Examples:

- » NIST Recommendations:
 - Role-Based Malware Awareness (AT-2): Provide targeted, hands-on training for high-risk groups (e.g., finance, engineering) on recognizing malware delivery vectors—email attachments, USB drives, and drive-by downloads.
 - Just-In-Time Nudges: Trigger micro-learning (“Don’t run unknown .exe files”) when users attempt risky actions, such as opening attachments from new senders or plugging in removable media.
 - Rapid Reporting Workflows: Integrate a one-click “Report Suspicious File” button into email clients and desktops, ensuring that potential malware samples feed immediately into the SOC triage queue.
- » ISO/IEC 27001 & 27002 Recommendations
 - Malware Simulation Exercises: Periodically send harmless, instrumented “malware” samples via approved channels (e.g., simulated USB drops) to assess real-world responses and reinforce correct handling.
 - Data-Handling Workshops: Host quarterly sessions where employees practice identifying and quarantining malware, reviewing sandbox analysis results to understand attack mechanics.
 - Feedback & Recognition: Publish a monthly “cyber-hygiene leaderboard” celebrating teams with the fastest malware reporting times and lowest infection rates.

» MITRE ATT&CK Guidance

- Collaborative Threat Reviews: Involve end users in regular “Malware Roundtable” sessions where analysts share sanitized samples, dissect infection chains, and gather feedback on defensive workflows.
- Continuous Threat Spotlight: Send succinct weekly bulletins on emerging malware trends (e.g., new ransomware variants), paired with one-minute video tips on avoidance and remediation.

Step 5: Reinforce with Nudges & Simulations (Week 4–5 – Security Ops)

- Deliver real-time nudges after malware alert (e.g., “You downloaded a suspicious file—here’s what to do next time.”)
- Run targeted malware simulation tests (e.g., macro-infected doc or spoofed software link)
- Measure follow-up behaviors: blocked downloads, reported files, or successful detection and ensure that program is changing behaviors at the employee level.

Step 6: Avoid Pitfalls (Lessons Learned)

- Don’t treat all malware events as equal—**focus on user behavior + impact**
- Avoid broad campaigns—**tailor to high-exposure roles**
- Don’t skip role-specific education—executives and IT teams face different threats
- Don’t rely only on EDR logs—**merge behavior, awareness, and context**
- Don’t forget manager involvement—they **help normalize secure file behavior**

Step 7: Make This Real—Report the Wins

Example OKRs or Goals:

- Reduce executable file downloads from unknown sources by 30%
- Increase secure file handling behavior score by 15 points across high-risk user cohort
- Reduce repeat malware-triggering employees by 50% in 90 days
- Increase malware simulation report rate by 20%

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.

