



Security Culture

90 DAY HRM PLAYBOOK

Table of Contents

Executive Summary 3

Security Culture 5

 Play - Nudges 8

 Play - Scorecards 11

 Play - Cultural Dashboards 14

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

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.

