

Executive Business Case Pack

Financial Modeling, Governance Alignment,
and ROI Justification for AI-Native HRM



Living Security enables organizations to quantify and reduce human cyber risk using AI-native Human Risk Management (HRM). This executive guide is designed to help CISOs, CFOs, and board stakeholders align investment decisions with measurable risk reduction outcomes.

Executive Summary

Human-driven cyber incidents account for the majority of enterprise breaches — yet most organizations lack measurable visibility into workforce risk exposure.

This guide helps executive stakeholders:

- Quantify projected human-driven loss exposure
- Model potential risk reduction impact
- Align HRM investment with enterprise risk strategy
- Frame board-level governance reporting
- Secure cross-functional budget alignment

This document focuses on financial justification and executive alignment for HRM adoption.

Building the Internal Business Case for HRM

To adopt HRM successfully, you'll need more than technical readiness. You'll need internal alignment, financial justification, and an empowered champion.

Positioning the Budget

HRM investments can be aligned to multiple budget categories:

- Security transformation initiatives
- Risk management modernization
- Cyber resilience programs
- Evolution of existing SAT budgets
- Identity and access optimization
- AI governance initiatives

For organizations under long-term SAT contracts, HRM can operate in parallel, adding visibility, automation, and exposure reduction without requiring immediate vendor replacement.

This lowers political friction and accelerates approval.

Talking Points for the CFO:

Quantifying the Value

Finance leaders do not fund “improvements.”
They fund risk-adjusted return.

Anchor the discussion in three measurable areas:

1. Incident Loss Reduction

- Average cost of a data breach: ~\$4.8M
- ~74% of breaches involve a human element (Verizon DBIR)
- Human-risk concentration: ~10% of users drive most exposure

2. ROI Modeling Framework

Use this model to build your CFO-ready business case:

> Step 1: Estimate human-driven incident exposure

Annual incidents × average cost

Example: 10 human-driven incidents × \$4.8M = \$48M annual exposure

> Step 2: Apply conservative reduction range

Even a 20–40% reduction in human-driven incidents or impact meaningfully shifts risk.

If HRM reduces exposure by 30%: $\$48M \times 30\% = \$14.4M$ avoided impact

> Step 3: Add operational efficiency gains

Automation of:

- Risk scoring
- Targeted interventions
- Reporting workflows

Often reduces manual administrative effort by 30–50%, freeing SecOps and GRC resources for higher-value initiatives.

3. CFO Framing Statement

“If a \$X annual investment reduces projected human-driven loss exposure by even Y%, the avoided risk exceeds the platform cost within Z months.”

Keep assumptions conservative and let finance validate them.

Talking Points for the Board: From Activity to Risk Governance

Boards care about measurable exposure and governance posture.

HRM enables reporting on:

- Quantified human risk exposure across the enterprise
- Identification of highest-risk users and risk concentration trends
- Reduction in exposure duration (time spent in elevated risk states)
- Movement from compliance metrics to outcome-based risk indicators

This aligns human risk management with enterprise risk oversight and AI governance responsibilities.

It changes the board narrative from:

“Training completion rates”

to:

“Reduction in measurable workforce risk.”

Who Typically Owns the Initiative?

HRM initiatives are most often driven by:

- The CISO or Deputy CISO
- Security Awareness or Human Risk leaders
- GRC leadership
- Security Operations teams seeking behavioral telemetry integration

In more mature environments, HRM is positioned not as a training upgrade, but as an enterprise risk management capability aligned with identity governance, resilience strategy, and AI risk oversight.

The framing matters. Training budgets get scrutinized. Risk infrastructure gets funded.

Addressing Common Internal Objections: Stronger Responses

Objection: *"Our existing training is sufficient."*

Response:

"Can your current platform tell you, right now, which 50 users represent the greatest risk to the organization? And how long they've been in an elevated risk state?"

If it cannot, it is measuring activity — not risk.

HRM integrates and operationalizes training into a measurable governance framework.

Objection: *"HRM costs too much."*

Response:

"The cost of a single human-driven breach often exceeds the annual investment in HRM multiple times over. This is risk mitigation infrastructure — comparable to identity protection or endpoint detection — not discretionary training spend."

Reframe from expense to risk control.

Objection: *"We don't have bandwidth."*

Response:

"HRM reduces manual workload through automation — risk scoring, intervention workflows, and reporting. The goal is fewer spreadsheets, fewer ad hoc remediation campaigns, and fewer reactive incidents."

Position HRM as operational simplification.

Building a Cross-Functional Coalition

HRM initiatives are most successful when stakeholders from:

- Security
- IT
- HR
- Compliance
- Procurement
- Business Units

are engaged early. Position HRM as shared risk accountability, not a security-only program. When human and AI risk intersect culture, identity, and governance, the initiative must as well.

Champion Enablement Kit: Turning Strategy into Internal Momentum

The biggest bottleneck in enterprise adoption is not technical validation. It is internal persuasion.

Equip your internal champion with ready-to-use assets:

1. One-Page Executive Summary Template

Customizable brief including:

- Current maturity level
- Estimated financial exposure
- Projected reduction range
- Alignment with enterprise risk strategy

2. Three-Slide Internal Pitch Outline

> Slide 1: The Risk Gap

- % of breaches involving humans
- Visibility limitations of current approach

> Slide 2: The Architectural Shift

- SAT vs HRM vs AI-native HRM
- Exposure duration impact

> Slide 3: Business Case

- Modeled financial exposure
- Conservative reduction scenario
- Operational efficiency gains

3. Pre-Written Stakeholder Emails

- CFO: Financial impact and risk-adjusted return
- CIO: Integration architecture and telemetry alignment
- CHRO: Cultural alignment and behavioral reinforcement
- Board: Governance and exposure reduction

This transforms the toolkit from a static document into an internal mobilization package.

Quantify Your Risk & Action Plan

Leverage the Risk → Data → Actionable Intelligence playbook to:

- Connect risk signals to measurable outcomes
- Align exposure reduction with financial impact
- Build a CFO-ready narrative tied to business outcomes

View the Risk → Data → Actionable Intelligence Guide

Visit: <https://www.livingsecurity.com/risk-data-actionable-intelligence>

