livingsecurity

Human Risk Management
Trends Guide

Navigating Human Risk Management in the Age of AI and Behavioral Insights

2025

Introduction

68%
of breaches involved the human element [1]

In 2025, managing human security risks continues to be a top priority for organizations worldwide. As the digital landscape expands, so do the vulnerabilities tied to human behavior. According to Verizon's 2024 Data Breach Investigations Report, **68% of breaches involved the human element**, highlighting the critical need for Human Risk Management (HRM) to evolve beyond traditional security awareness training into a comprehensive strategy focused on behavior-driven insights and interventions.[1]

This year's Verizon DBIR analysis of 30,458 security incidents, of which 10,626 were confirmed data breaches spanning 94 countries, underscores the global scale and complexity of human-related security risks.[1] Modern HRM solutions, such as Living Security's Unify platform, offer the tools needed to deliver real-time visibility, data-driven insights, and actionable metrics that can transform human risk from a vague concept into a clearly defined business risk. The trends outlined in this guide will define HRM in 2025, empowering organizations to take a data-driven, proactive approach to managing and reporting human risk.

01 AI-POWERED BEHAVIOR INTELLIGENCE

AI has become a cornerstone in Human Risk Management solutions, offering capabilities that transform how organizations assess and mitigate human-centric risks. Living Security's HRM platform is increasingly utilizing AI to support automated responses and deliver behavior-driven insights, fundamentally reshaping the landscape of cybersecurity.

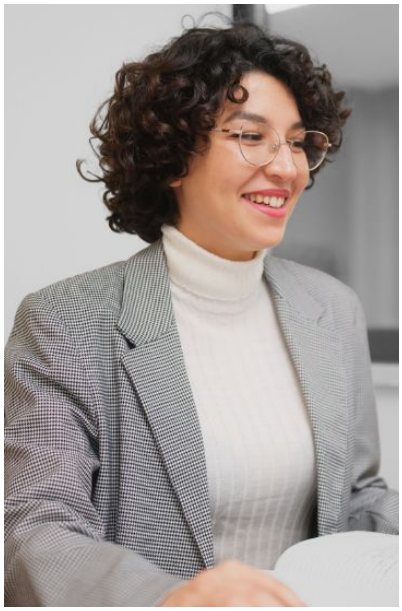
By processing vast amounts of behavioral, contextual, and technical data in real time, AI enables HRM solutions to detect subtle patterns and anomalies that might otherwise go unnoticed. This precision reduces false positives and ensures security teams focus on the most critical issues. AI-driven automation further streamlines workflows, instantly triggering appropriate interventions—such as assigning tailored training, sending targeted nudges, or implementing access controls—without manual oversight.

Moreover, AI enhances the scalability of HRM platforms, allowing organizations to effectively manage risk across a growing workforce and expanding attack surface. Its ability to continuously learn from historical data and adapt to new threats ensures that risk assessments remain accurate and actionable. By alleviating the operational burden on security teams and providing rapid, data-informed responses, AI not only improves the efficiency of HRM processes but also fortifies an organization's overall defense posture. This integration underscores why AI is no longer optional but essential for modern HRM solutions.

A few key components AI provides in Living Security's Unify Human Risk Management Platform include:

- **Behavioral Analytics** detect and analyze over 250 discrete user behaviors and events, identifying patterns that may indicate risky actions or deviations from baseline norms.
- **Real-Time Data Processing** of vast amounts of data to deliver instant insights, reducing response times and enhancing situational awareness.
- **Automated Workflows** such as assigning training, sending behavior-based nudges, and implementing policy changes to mitigate risks without manual intervention.
- **Proactive Risk Interventions** flag high-risk behavior coupled with events and triggers targeted actions, such as immediate training modules or restrictions on access, to prevent escalation.
- **Predictive Insights** anticipate future risk scenarios using historical data and behavioral trends, enabling proactive measures to address potential threats.

Together, these AI-driven capabilities empower Living Security's Unify Human Risk Management Platform to provide a comprehensive, adaptive approach to mitigating human risk, ensuring organizations stay one step ahead of evolving threats.



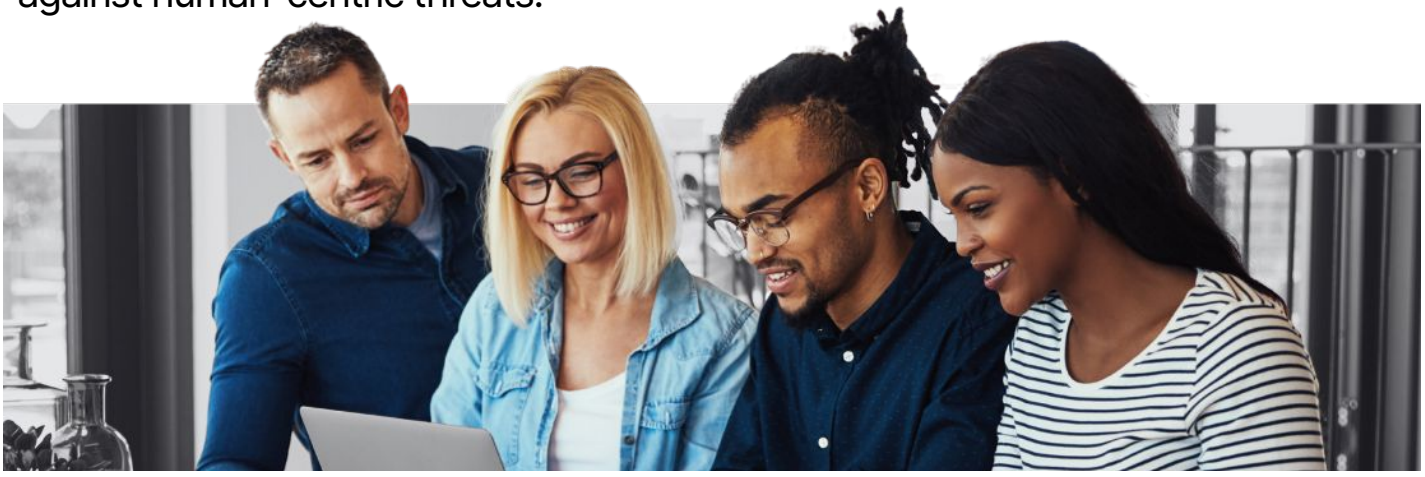
Key Takeaways:

- **Efficient AI-driven data processing at scale** help vast volumes of security incident data, enabling organizations to rapidly analyze and prioritize high number of incidents with precision and efficiency.
- **Actionable intelligence** is the result of automating the analysis of complex data sets, empowering organizations to implement timely targeted interventions and significantly reduce response times.

02 COMPREHENSIVE RISK SCORING

Traditional metrics like phishing click rates are no longer sufficient to measure the complexity of human risk in cybersecurity. As cyber threats evolve, so must the tools and approaches organizations use to identify and mitigate these risks. Modern Human Risk Management platforms now offer multi-dimensional risk scoring to deliver a more accurate and actionable view of individual risk. According to The Forrester Wave™: Human Risk Management Solutions Q3, 2024 report, Living Security's "Unify provides a comprehensive Human Risk Index that estimates the likelihood and impact of human behaviors on a firm's overall security posture and is based on behaviors, external threats, and user access."[2]

This advanced approach goes beyond static metrics by incorporating behavioral indicators, identity context, attack surface exposure, and knowledge assessments, empowering organizations to tailor interventions based on real-world data. For example, HRM platforms can flag high-risk behaviors across security tools, analyze exposure to targeted attacks, and correlate cultural sentiment with observed actions—ensuring a dynamic, personalized defense against human-centric threats.



Modern HRM platforms using multi-dimensional risk scoring, consider the following factors:

- **Behavioral Indicators** that monitor users' real actions, across various security tools, flagging high-risk behaviors that need intervention
- **Identity Context** assess a user's role, access levels, and history with security incidents to calculate risk
- **Attack Surface Exposure** assess individuals' exposure to attacks, including whether they are classified as "Very Attacked Persons" (VAP), ensuring tailored risk assessments
- **Knowledge and Culture Assessments** measure security awareness and cultural sentiment, correlating this data with actual behavior to refine risk assessments

This granular risk measurement enables organizations to apply personalized interventions that are specific to each user's behavior and access privileges.

Key Takeaways:

- **Granular human risk indicators** allow for more accurate risk management and tailored interventions
- **Risk-driven policies and workflows** can be activated based on real-time behaviors, identity risks, and external threat data

03 ENHANCED WORKFORCE ENGAGEMENT

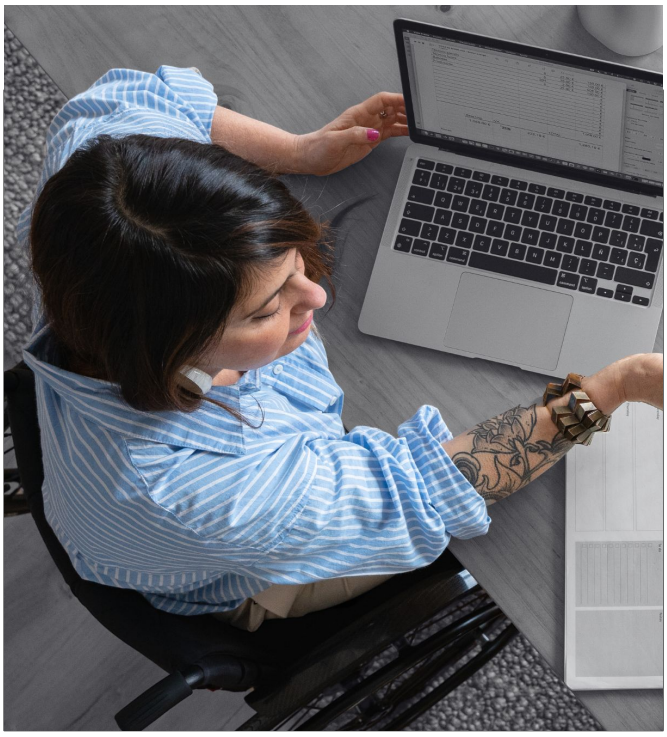
A key trend emerging in 2025 is the deeper integration of workforce engagement into HRM solutions, shifting the focus from passive to active participation. Traditional security training, often characterized by static, one-size-fits-all modules, is being replaced by dynamic, two-way communication models that place employees at the center of the risk management process.

This evolution recognizes that an engaged and informed workforce is not just a target for awareness campaigns but an active contributor to an organization's security posture. HRM platforms are now incorporating real-time feedback loops, personalized risk insights, and gamified elements to drive engagement, fostering a culture where employees take ownership of their role in cybersecurity.

Modern Engagement Strategies:

- **Interactive Communication** allows the workforce to ask questions, receive real-time feedback, and interact with personalized risk dashboards. This helps users take responsibility for their security behaviors.
- **Adaptive Learning** platforms adjust training content based on user behavior and risk, offering training tailored to the actions and risks specific to each user.
- **Cultural Measurement** is becoming increasingly important. By tracking how security sentiment influences behavior, organizations can foster long-term improvement in security culture.

Deepening end-user engagement is key to changing risky behaviors and fostering a proactive security culture within the organization. By delivering personalized training and interactive tools, HRM platforms create a more meaningful connection between users and their cybersecurity responsibilities.



Key Takeaways:

- **Interactive communication** and real-time feedback create more engaging and effective hyper-customized training and risk mitigation
- **AI-driven adaptive learning** ensures that users receive relevant, risk-specific content, reinforcing security behaviors

04 INCREASED VISIBILITY AND REPORTING FOR BUSINESS LEADERS

In a Harvard Business Review article, it indicates that 65% of organizations struggle to translate technical cybersecurity risks into business-relevant metrics for board members.[4] As cybersecurity continues to shift from a technical issue to a critical business risk, boards of directors and executive teams are demanding greater visibility into human risk. In 2025, this evolution has reached a pivotal moment: the ability to quantify and communicate human risks has become a cornerstone of effective cybersecurity strategies.

With nearly 70%of boards now ranking cybersecurity among their top concerns, traditional metrics such as click rates and training completion statistics are no longer sufficient.[5] Security leaders must leverage modern tools such as HRM platforms that provide customized risk dashboards that deliver granular visibility into the likelihood and impact of human risks while presenting actionable, business-relevant insights that drive decision-making at the highest levels.

This shift from reactive reporting to proactive risk management empowers boards and executives to make more informed decisions and allocate resources effectively.

- **Human Risk Dashboards** offer real-time assessments that correlate human behaviors with organizational risk, providing a clear, data-driven view of vulnerabilities. This visibility allows leadership to prioritize mitigation efforts that align with business objectives.
- **Business Relevant Reporting** presents risks in a format that connects directly to business outcomes, HRM platforms bridge the gap between technical data and executive priorities. The clarity not only improves communication but also enhances trust between security teams and leadership.
- **Enhanced Budget Justification** is supported by real-time visibility into security awareness, behavior and human risk impact. This enables security teams to demonstrate the effectiveness of existing strategies, making a compelling case for ongoing or increased investment in cybersecurity initiatives.

Key Takeaways:

- Detailed, business-friendly reporting allows for better communication of cybersecurity risks to the board, aligning security strategies with business outcomes
- **Granular visibility** into human risk strengthens an organization's security posture and builds trust between security teams and leadership

05 COLLABORATIVE SECURITY PLATFORMS

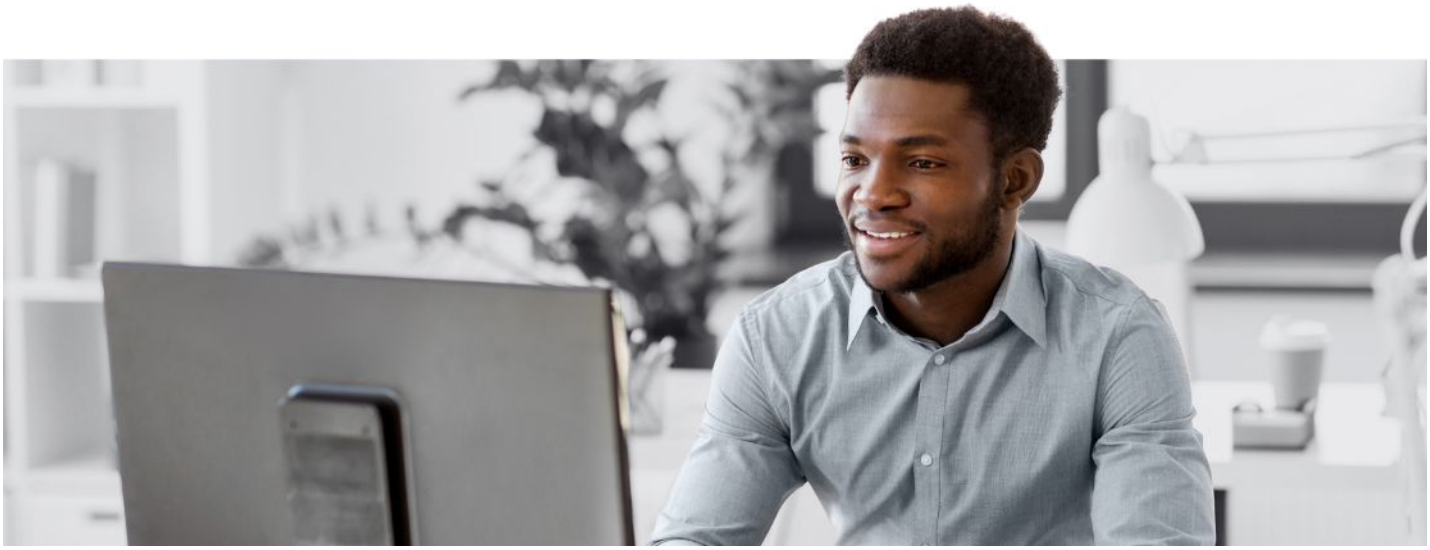
As cyber threats grow more sophisticated, the need for organizations to evolve their approach to security becomes even more critical. The future lies in collaborative security platforms—integrated systems that bring together people, processes, and technologies to create a unified defense. A key component of this transformation is HRM platforms, which prioritize the human element in cybersecurity.

Gartner predicts that by 2026, enterprises that combine generative AI (GenAI) with an integrated platform-based architecture in security behavior and culture programs (SBCP) will experience 40% fewer employee-driven security incidents.[6] This highlights a pivotal shift: empowering employees and teams to become active participants in securing their organization through shared insights, collaboration, and streamlined processes. Collaboration in security isn't just about technology; it's about connecting the dots between people and systems.

Leading HRM solutions are emerging as centralized hubs where:

- Teams share actionable insights
- Responses to security incidents are coordinated
- Security initiatives and outcomes are tracked and measured over time

By fostering a culture of shared responsibility, collaborative platforms enhance resilience and improve outcomes in the face of evolving threats.



Key Takeaways:

- **Centralized visibility** across security functions provides a holistic view of security operations, allowing teams to identify risks, monitor behavior, and detect vulnerabilities in real-time
- **Integrated response** capabilities enable seamless response actions across departments, ensuring that incidents are handled efficiently and effectively
- **Shared insights and metrics** fosters transparency and allows teams to benchmark performance, track progress, and identify areas for improvement
- **Coordinated incident response** streamlines communication during incidents, ensuring that all stakeholders are aligned and ready to act

Conclusion

As we move toward 2025, HRM solutions continue to evolve in response to the complex threat landscape. The data in this report clearly shows that human risk management must be comprehensive, adaptive, and data-driven.

By embracing these five trends, organizations can better mitigate human risks, foster a proactive security culture, and build long-term resilience in an increasingly complex cyber landscape.

REFERENCES:

[1] Verizon (2024), Data Breach Investigations Report

[2] Forrester (2024), The Forrester Wave™: Human Risk Management Solutions Q3, 2024

[3] Recorded Future (2024), 2024 State of Threat Intelligence

[4] Harvard Business Review (2023), Boards are Having the Wrong Conversations about Cybersecurity

[5] EY (2024), Americas board priorities 2024

[6] AI Wire (2024), Gartner Reveals Top Trends in GenAI Cybersecurity for 2024