

Human Risk Management

BUYER'S GUIDE

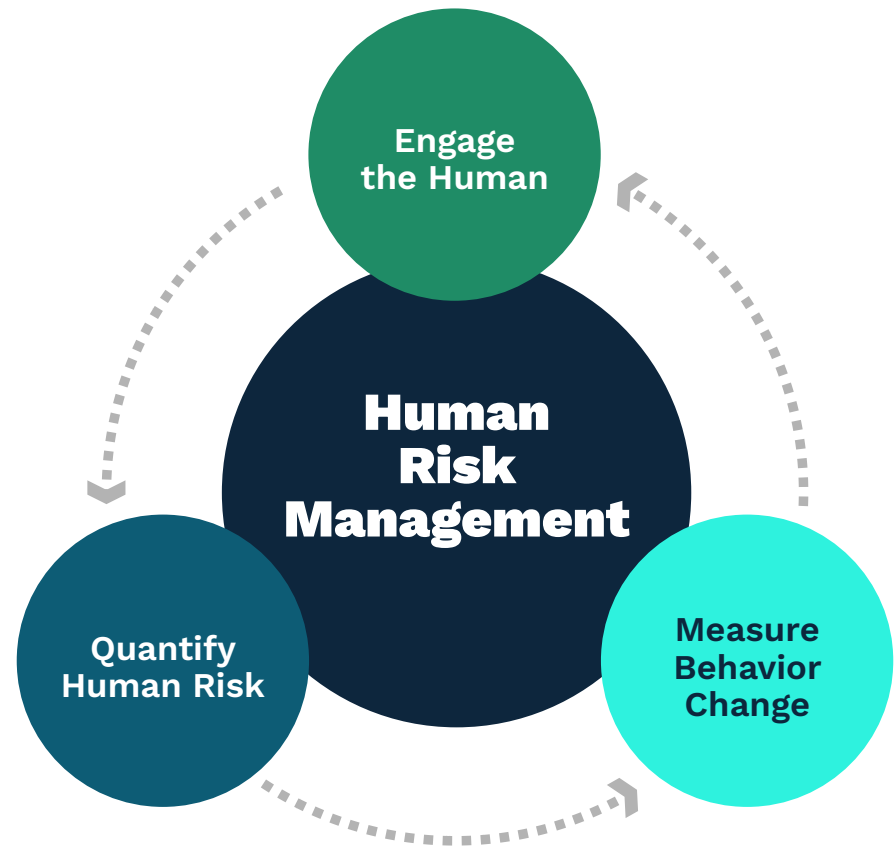
Selecting the Right Human Risk Management Platform

BUYER'S GUIDE

Selecting the Right Human Risk Management Platform

Compliance-focused Security Awareness & Training (SA&T) programs lack the ability to track the impact of behavioral change and organizational risk. Human Risk Management, however, focuses on the human side of risk, enabling enterprises to identify, respond to, and report on human-initiated risk within their organization. Moving to a Human Risk Management model and platform helps security leaders quantify risk with actionable insights, make more informed security decisions, and transform employees into a proactive line of defense.

After helping dozens of companies change their workforce behavior and build a vigilant security culture, Living Security has identified the most essential criteria to include when evaluating Human Risk Management platform options. This guide highlights three key areas and associated elements every robust Human Risk Management platform must have.



QUANTIFY HUMAN RISK

Quantifying human risk requires aggregating internal data across a wide range of existing siloed systems to provide an accurate assessment of human risk to the business. Having a 360-degree view into your workforce's use of security tools helps you identify and quantify areas of risk and vigilance. This data enables you to make quick, effective decision-making and intervention.



Data Visibility

It integrates with and pulls historical data from a wide variety of sources including web authorization and access, emails, devices, and other sources like DLP, Active Directory, and SaaS suites. Ideally the platform integrates with all your existing security technology.



Save hours of manual data collection and calculations of human risk behavior.



Automate Data Collection

The right platform should provide continuous tracking of security behaviors across the enterprise, so your organization can assess individuals, teams, and locations that need the most help.



Reduce the time spent manually uploading data from disparate technology sources.



Correlative Analysis

The ability to use AI-based algorithms to provide context of individual behaviors based on the individual's role and aligned to business needs to assess risk.



Take quick action by understanding which behaviors to accept and which to isolate to avoid unnecessary risk.



Risk Categorization

Enable administrators to compare risks by risk category, such as phishing email, web security, device security, authentication/access, activity, data security, and privacy, in addition to the more traditional approach of training and/or assessment completion.



Activate action plans to speed up remediation and change risky behaviors across your organization.



Actionable Dashboard

Compile a sortable view of human risk by roles, departments, and locations over time, comparing aggregate behavior, and providing insights into the most dangerous problems.



Make smarter and faster decisions by highlighting trends, anomalies, and clusters while boosting resilience.

ENGAGE THE HUMAN

High-quality, immersive training engages individuals and boosts their retention of key security concepts. Targeted training helps get the right intervention to the right people, at the right time, for the right risks.



Data Visibility

Detailed mitigation plans for the riskiest teams, locations, or individuals to address the most urgent threats, with out-of-the-box plans for common risks.



Improve outcomes and security posture without unnecessary business disruption, reduces hard and soft costs.



Scalability Across the Enterprise

Proven roll-out and deployment guidelines or playbooks to assure seamless enterprise-wide implementation.



Create a vigilant culture that turns every employee into a security asset.



Role-Based Courses

Training directly applicable to an employee's role, responsibilities, and the work they do, instead of a one-size-fits-all approach.



Increase employee engagement due to highly-relevant content, focused on changing risky behavior.



Risk-Based Courses

Training directly applicable to employees based on their riskiest behaviors, instead of broad-based training content.



Reduce risk faster by focusing on the riskiest employees without requiring more training for those that are not exhibiting risky behavior.



Gamified, Team-Based Training

Ability to train teams together—even virtually — to solve interactive cybersecurity puzzles.



Fun, immersive team-based experience increases retention and gives context to cybersecurity risks, leading to higher information retention. Training groups also reduce speed-to-learning for individuals.



MEASURE BEHAVIOR CHANGE

Access to data, metrics, and reporting enables you to track trends over time and correlate them to overall organizational risk and gauge the success of Human Risk Management initiatives.



User-level Reporting

Provide regular user-level report cards that track training completion, uncover hidden behavior vulnerabilities, and highlight vigilant behavior.



Drive behavioral change at the individual level so they can understand the impact of their actions in the moment.



Department-level Reporting

Provide robust department-level report cards across all security initiatives to give managers needed visibility into group strengths and weaknesses.



Improve departmental ownership over changing risk behavior with the ability for interventions, coaching, and guided action plans.



Leaderboards

Provide leaderboards to facilitate public recognition and incentive programs that motivate the workforce.



Reward employees for steps toward changing disruptive behavior that puts the business at risk.



ROI Analytics

ROI analysis tools that quantify risky behavior in terms that non-security leaders understand and appreciate.



Improve security leadership's ability to communicate human risk, show the value of Human Risk Management program, and gain executive-level buy-in.



Ready to Explore What an Human Risk Management Platform Can Do?

Request a demo of Living Security's Human Risk Management platform and learn how your workforce can become your strongest security asset.

See Human Risk Management in Action



livingsecurity

About Living Security

Living Security's mission is to transform human risk to drive dramatic improvement in human behaviors, organizational security culture, and infosec program effectiveness. With our Human Risk Management platform, Living Security engages each employee with innovative and relevant context and content, while simultaneously providing the ability for leadership to identify, report on and directly mitigate the risk brought on by human behavior. Living Security is trusted by security-minded organizations like MasterCard, Verizon, Biogen, AmerisourceBergen, Hewlett Packard, and Target. Learn more at www.livingsecurity.com.