KnowBe4

Critical Capabilities When Evaluating Human Risk Management Platforms

WWW.KNOWBE4.COM

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

Human Risk Management (HRM) is more than just the next step in security awareness training (SAT)—it's a fundamental shift in how organizations approach human security risks. Traditional SAT focuses on knowledge transfer, but HRM takes a data-driven, holistic approach to understanding, measuring and reducing risks tied to human behavior. Instead of simply making employees aware of threats, HRM actively works to change behaviors and improve decision-making.

Plenty of vendors claim to offer HRM or human-centric security products, but many are still rooted in purely technical approaches and only address a portion of the problem. True HRM needs to be more than a veneer of human centricity—it requires a platform built around human behavior that integrates elements like habits, awareness and decision-making.

Here are the key capabilities an HRM platform must deliver in order to identify, quantify and mitigate human risk:

Risk Identification and Assessment

A strong HRM platform starts with the ability to identify and assess human-related cyber risks. This goes beyond basic security awareness metrics—it's about gaining real insight into employee behaviors, vulnerabilities and the threats they encounter daily. To effectively pinpoint and measure human risk, an HRM platform must include these five capabilities:

AI-Driven Behavioral Analysis

Using advanced analytics to analyze user interactions across systems and platforms. This creates a true understanding of an employee's risk profile and learning needs. AI-driven behavioral analysis continuously monitors user actions, detecting deviations that may indicate risky behavior, such as repeated interactions with phishing attempts or unsafe downloads. This proactive approach both identifies at-risk employees and tailors security training to their specific vulnerabilities.

Adaptive Assessment

Conducting sophisticated social-engineering attack simulations and security assessments that adapt to each user's current level of knowledge and behavior patterns. These assessments should mirror real-world threats while providing valuable learning opportunities. By adjusting difficulty levels and attack vectors based on employee responses, adaptive assessments ensure that training remains relevant and challenging. Employees who consistently demonstrate strong security awareness receive different scenarios than those who struggle with basic concepts. This personalization fosters growth while preventing complacency.

Comprehensive Risk Monitoring

Implementing continuous monitoring across email, cloud applications, and other systems to identify potential risks before they lead to incidents. Effective risk monitoring goes beyond static reporting by actively analyzing communication patterns, access behaviors, and device usage to detect anomalies.

Security Posture Assessment

Regularly evaluating the overall security stance of the organization, including policy effectiveness, technology implementation, and cultural factors that influence human risk. This can even involve proactive scanning of web, deep web, and dark web forums and marketplaces for exposed credentials or sensitive information that could be used to target employees or the organization.

Integrated Threat Intelligence

Incorporating external threat intelligence and crowdsourced security data to understand evolving attack vectors and tactics that specifically target human vulnerabilities. Cybercriminals constantly adapt their techniques, making real-time intelligence essential for staying ahead of threats.
By analyzing data from global threat feeds, dark web activity, and industry-specific attack patterns, HRM platforms can provide organizations with early warnings of targeted phishing campaigns, credential-stuffing attempts, and social engineering schemes.

Personalized Education and Enablement

HRM goes beyond traditional SAT by delivering engaging, hyper-personalized, and continuous learning that aligns with how people actually learn and behave. Effective security education isn't one-size-fits-all—it must adapt to each employee's unique risk profile. That's why a strong HRM platform leverages AI to create dynamic training experiences that evolve based on individual needs and behaviors. Here are six key HRM capabilities that power personalized, adaptive learning for your employees:

AI-Driven Training Recommendations

AI is now crucial to automatically selecting and delivering the most relevant training content based on an individual's risk profile, role and learning history. This ensures training remains challenging yet achievable for each employee. By analyzing behavioral data and past interactions with security content, AI can fine-tune recommendations over time, prioritizing the most pressing risks. Personalized pathways keep employees engaged, ensuring they stay ahead of emerging threats. Additionally, AI-driven insights allow security teams to identify trends and adjust their awareness strategies proactively.

Real-Time Security Coaching

Providing just-in-time learning and immediate feedback and guidance when risky behaviors are detected by delivering contextual learning when it's most relevant and impactful. This proactive approach fosters continuous awareness and reinforces secure habits without disrupting productivity. Over time, employees develop a stronger security mindset, reducing the likelihood of mistakes that could lead to breaches.

Microlearning

Delivering bite-sized, focused training content that can be easily consumed and applied in real-world scenarios. This approach helps combat information overload and improves retention. By breaking complex topics into short, digestible lessons, employees can absorb critical security concepts without feeling overwhelmed. Microlearning modules can be seamlessly integrated into daily workflows, making security awareness an ongoing part of an employee's routine.

Continuous Reinforcement

Moving beyond one-time training sessions to create an ongoing process of learning and adaptation. This includes regular updates, refresher courses, and real-world scenario practice. Continuous reinforcement ensures employees don't forget critical lessons by incorporating quizzes, scenario-based exercises, and periodic reminders. Gamification elements such as leaderboards, rewards and interactive challenges further encourage participation.

Multi-Channel Communication

Using various communication channels (email, Teams, Slack, LMS, Google Chat) to deliver security tips and reinforce training concepts where employees are already working. This ensures security awareness is seamlessly woven into daily workflows rather than treated as a separate task. Short security reminders, quick quizzes, and interactive discussions help reinforce key lessons in a natural, engaging way. Additionally, personalized nudges based on individual risk behavior can be delivered through preferred channels, ensuring employees receive timely, relevant security guidance.

Simulated Attack Testing

Running sophisticated phishing and social engineering simulations that mirror current threats, thus providing safe learning environments for employees to practice their security skills. These realistic simulations expose employees to evolving social engineering techniques, helping them recognize and respond to malicious attempts with confidence.

Integration and Automation

A true HRM platform is more than just a collection of loosely connected tools—it's a fully integrated platform designed to manage human risk at scale. When evaluating HRM platforms, look for one with an adaptive security architecture that seamlessly integrates into your existing security ecosystem. To be effective, it must include these five essential products/capabilities:

Security Orchestration and Automated Response (SOAR)

A SOAR product to automate incident response processes, reducing the time between threat detection and mitigation while ensuring consistent handling of security events. Additionally, HRM enabled SOAR can transform real-world threats into training opportunities. By correlating human risk data with security incidents, SOAR platforms can initiate targeted interventions, such as delivering just-in-time training or requiring additional authentication. This seamless integration between HRM and SOAR enhances security resilience, providing security teams with the ability to respond faster and with greater precision.

Integrated Cloud Email Security (ICES)

Advanced email protection that combines AI-powered analysis with user behavior patterns to defend against sophisticated phishing and social engineering attacks. By integrating with HRM platforms, ICES can block malicious emails and provide risk-based training tailored to users who interact with suspicious messages. This proactive approach ensures that employees are not only protected from email-based threats but also continuously educated on emerging attack techniques, strengthening overall security awareness.

Real-Time Risk Mitigation

AI-driven defense agents to provide immediate protection against emerging threats while delivering contextual coaching to users. When risky behavior is detected—such as entering credentials into a suspected phishing site or downloading an unverified attachment—real-time mitigation tools can intervene by blocking the action, issuing a warning, or prompting additional verification steps. Over time, this approach helps employees internalize safe behaviors, reducing their likelihood of falling victim to threats and improving the organization's overall security posture.

Cross-Platform Integrations

Connecting with existing security infrastructure (Microsoft 365, CrowdStrike, Cisco, Netskope, etc.) to share threat intelligence and create a unified security ecosystem. A strong HRM platform doesn't operate in isolation—it enhances and amplifies the capabilities of your broader security stack. By integrating with endpoint detection and response (EDR), identity access management (IAM), and security information and event management (SIEM) products, HRM platforms can provide a comprehensive view of human risk.

Automated Response

Implementing systems that can automatically quarantine threats and remove malicious emails across the organization when identified. Instead of relying solely on manual intervention, automated response mechanisms help security teams contain threats before they spread. When a phishing attempt is reported or detected, the system can instantly remove similar emails from all inboxes, preventing further exposure. By reducing reliance on human response time, automated security actions significantly enhance threat containment and risk reduction.

Continuous Monitoring and Improvement

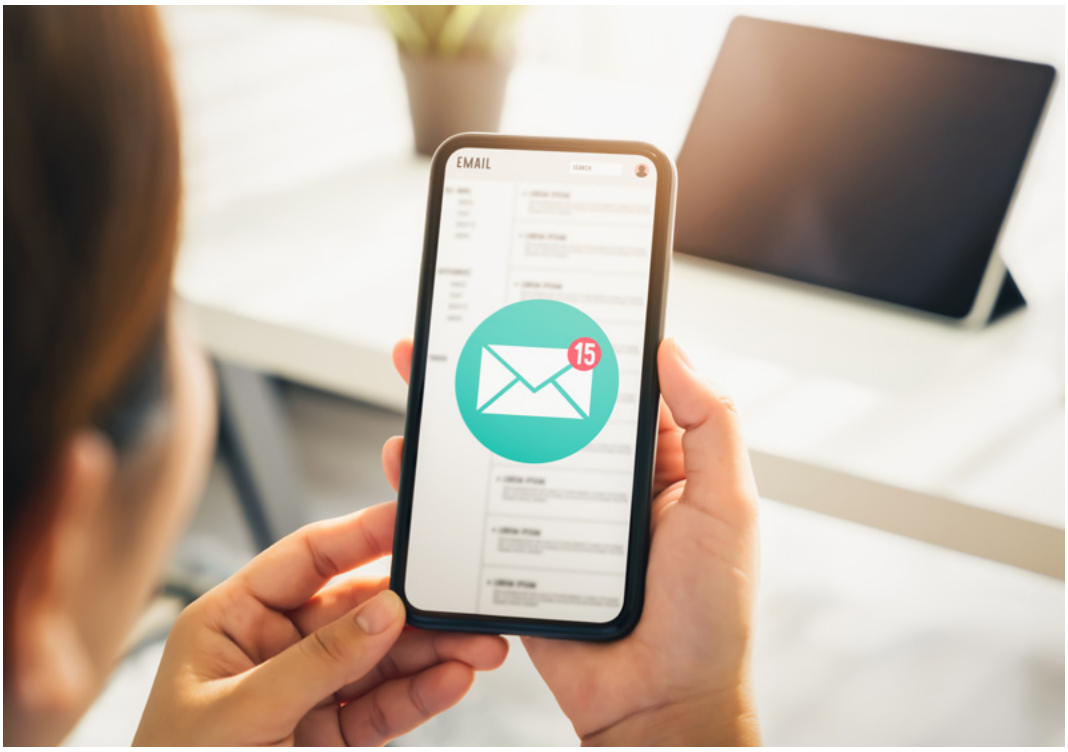
Finally, data-driven insights and adaptive security controls are a must. Human risk is constantly evolving, so your HRM platform should use real-time data to make dynamic adjustments and continuously strengthen your organization's risk management strategy. Here are five essential capabilities that make this possible:

Risk Scoring

Maintaining dynamic risk profiles for each employee, team or department based on their behaviors, training performance and security events. Unlike static assessments, real-time risk scoring adapts to ongoing changes in user activity, ensuring a continuously updated understanding of human risk. This includes monitoring interactions with phishing simulations, engagement with security training, and responses to real-world security events. A strong HRM platform uses this data to segment employees into risk tiers, allowing security teams to prioritize interventions where they're needed most.

Adaptive Security Controls

Automatically adjusting security controls and training requirements based on individual risk levels and behaviors. If an employee demonstrates repeated risky behavior—such as engaging with phishing attempts, failing security assessments, or bypassing security policies—the system can escalate protective measures. This might include enforcing multi-factor authentication (MFA), restricting access to sensitive data, or increasing mandatory training frequency. Conversely, employees who consistently demonstrate strong security awareness can receive fewer training requirements, reducing friction and improving efficiency. By making security controls dynamic and responsive, organizations can create a more personalized, risk-based approach that adapts to each employee's behavior in real time.



Behavioral Metrics and Analytics

Moving beyond simple completion rates to measure actual behavior change. This should include the ability to track comprehensive metrics such as Phish-prone Percentage™, security awareness levels, policy copmliance rates, incident reporting rates (including time-to-detect) and real-time risk indicators.

Regular Risk Reassessments

Conducting periodic evaluations of the organization's human risk profile to identify new vulnerabilities, evolving threats and areas of improvement. This includes assessing how well security controls align with human nature and workflow needs. Cyber threats are constantly evolving, making it essential to regularly revisit training effectiveness, employee engagement and policy adherence. Risk reassessments should incorporate data from phishing simulations, policy violations and real security incidents to ensure continuous improvement. Additionally, by comparing current risk trends with historical data, organizations can measure the effectiveness of their security programs and adjust strategies to address emerging challenges.

Adaptation to Change

Continuously evolving strategies to address new challenges such as remote work, generational shifts in the workforce, new cyber threats and the growing use of AI and automation. As work environments and technology change, so do the tactics of cybercriminals. Organizations must remain agile by updating their security training, communication strategies and risk assessments to reflect new attack vectors and behavioral trends. For example, the rise of AI-powered phishing attacks requires enhanced training on deepfake and voice phishing threats. A truly effective HRM platform ensures that security strategies remain relevant, proactive and responsive to the ever-changing cyber landscape.

A true HRM platform integrates risk assessment, personalized learning, automation, and continuous monitoring to create an adaptive security ecosystem that evolves alongside emerging threats. By leveraging AI and behavioral analytics, HRM transforms security awareness from a static training exercise into a dynamic, intelligence-driven strategy.

Cyber threats are constantly evolving. To stay ahead, organizations must move beyond awareness and focus on measurable behavior change. The right HRM platform will not only reduce human risk but also build a stronger, security-conscious culture—one decision at a time.

Learn more about what KnowBe4 can do for your organization

Visit KnowBe4.com

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit
www.KnowBe4.com

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

01F02K02