KnowBe4

5 Most Frequently Asked Questions About Human Risk Management

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

Human Risk Management (HRM) has emerged as both a “buzz phrase” and an essential enterprise cybersecurity competency. Yet many IT and security administrators are still unclear on what it means for their teams. To help, KnowBe4 has put together concise answers to five of the most frequently asked questions about HRM:

1. What is Human Risk Management (HRM)?
2. Why is now the time for HRM?
3. How can you operationalize HRM?
4. Does HRM replace security awareness training (SAT)?
5. How should you evaluate potential partners?

Question 1: What is HRM?

Falling prey to social engineering schemes. Mishandling sensitive information. Skipping system updates. Relying on weak passwords. These are among the most common ways that humans unintentionally jeopardize an organization's cybersecurity at risk.

For years, organizations have invested in training to increase employee awareness and knowledge about why and how to maintain a strong cybersecurity posture. Such efforts have been and remain worthwhile. Yet now there is an opportunity to embrace a new approach: Human Risk Management.

KnowBe4 defines HRM as a holistic approach for identifying, quantifying and mitigating risks associated with human behavior. Building on legacy SAT, HRM is about forging a comprehensive approach to understanding and managing human-related risks. It requires a strategy and supporting infrastructure that address four pillars:

Risk Identification and Assessment

Systematic identification and assessment of human-related cybersecurity risks within your organization

Personalized Education and Enablement

Delivery of personalized, engaging and continuous learning experiences to your employees

Technology Integration and Automation

Implementation of an HRM platform that leverages the power of AI and machine learning and integrates with your other cybersecurity systems and tools

Continuous Monitoring and Improvement

Ongoing assessment and refinement of HRM strategies using data-driven insights and adaptive security controls

AT A GLANCE: **SHIFTING TO HRM**

That was then	This is now
Focus on providing knowledge to employees	Focus on addressing employees' underlying motivations and behaviors
Static, standard content that can lead to training fatigue or disengagement	Personalized, dynamic content that keeps employees engaged and reflects changes in both security threats and employee behaviors
Training platform siloed from other security systems	HRM platform that integrates with other security systems

Question 2: Why is Now the Time for HRM?

At the core, there are four main drivers behind the shift to HRM:

Social engineering and phishing attacks represent the single largest cyber risk

As cybersecurity defenses have become significantly more effective, attackers are finding that they can't use technology alone. Not surprisingly, social engineering attacks have become more sophisticated and widespread. In fact, according to research, 70% to 90% of cyber attacks now involve some form of social engineering.

AI will keep compounding the problem

Over 95% of cybersecurity professionals believe AI-generated content makes phishing detection more challenging. In the hands of bad actors, AI is fueling a new breed of highly convincing social engineering attacks, including synthetic media ("deepfakes"). Your employees need to be continually educated on how to detect and avoid them.

Traditional employee education is no longer enough

SAT is still critical. But traditional SAT alone is not an adequate defense in today's complex environment. With HRM, you can take employee education and engagement to another level. It enables you to be more proactive than reactive to continually learn from and improve real-world user behaviors.

Regulatory mandates are growing

Organizations face mounting requirements related to cybersecurity posture disclosure and reporting. Governments, regulatory bodies and even insurance providers have all officially recognized that the weakest link in security is often the human element.

Less than 3% of security spending is focused on the human layer. Yet more than 68% of breaches are traced to people. And Forrester has predicted that 90% of data breaches in 2024 would have a human element—up from 74% in the prior year.

Question 3: How Can You Operationalize HRM?

HRM isn't a one-and-done system implementation. It's a strategy, program and supporting infrastructure that you must build and maintain over time. As you work to bring HRM to life within your organization, consider these guiding principles for implementing and executing effective strategies:

Take a human-centric approach

View your people as assets to be empowered, not liabilities to be restricted. Strive to understand human nature so you can work with it (not against it). Make security intuitive and engaging, with systems that make secure behavior the easy choice. All the while, foster safety and community when you report incidents or concerns.

Aim for AI-driven adaptability

AI is making the "impossible" possible. With machine learning, you can identify and predict risky behaviors with greater speed and accuracy. Using generative AI, you can deliver unprecedented personalization within security experiences—including context-aware security coaching. And by harnessing automation for routine security tasks, you can reduce friction and free capacity to focus on other priorities.

Choose an integrated platform

A big-picture view of human risk is critical to your success with HRM. As you implement an HRM platform, unify security awareness, behavior management, and culture initiatives—creating seamless connections between security tools and systems. You need to be able to share threat intelligence across security platforms and to provide consistent user experiences across channels.

Commit to continuous adaptation and evolution

As always, security is an ongoing journey. Your HRM strategy and platform should support regular updates to content and simulations so they reflect the latest trends and threats. You need the ability to monitor and adapt to changing work patterns and technologies among your employee/user base, with constant refinement based on results you measure.

Keep nurturing a security culture

Building security into your organizational DNA has always been important. Your HRM strategy and platform should bolster your workforce's sense of shared responsibility for security. By celebrating security wins and learnings from incidents, you encourage your employees to openly communicate their security concerns.

Question 4: Does HRM replace SAT?

Not at all. HRM is simply the next phase in the evolution of employee education and engagement—and SAT remains a critical element within any HRM strategy.

SAT focuses on educating employees about cyber threats, policies and best practices. While valuable, this approach alone doesn't always translate into behavior change. HRM represents the next evolution by shifting the focus from awareness to measurable risk reduction.

HRM addresses the limitations of SAT operating alone, including one-size-fits-all experiences that may lead to knowledge acquisition without behavior change. It uses data-driven insights to assess individual risk levels by analyzing factors such as phishing test results, real-world security incidents and behavioral trends. HRM also integrates with, and leverages data from, an organization's broader security stack to allow security teams to prioritize risks.

HRM builds on SAT and powers a transition from reactive to proactive and from narrow to holistic. It also incorporates a behavioral focus, helping move from what people know to what they do.

Question 5: How should you evaluate potential partners?

The market has plenty of providers that purport to offer HRM or human-centric security products. In reality, many are technically-focused providers that have acquired smaller security training consultancies. For effective HRM, you need more than a veneer of human centricity.

The crux of cybersecurity risk often lies in human decisions. Thus, when evaluating HRM platforms, it's critical to choose one that genuinely addresses human behavior. Platforms that merely appear to be human centric might focus on superficial metrics or isolated training events—failing to create meaningful, lasting changes in behavior. In terms of capabilities, HRM should bring together SOAR, integrated cloud email security, real-time security coaching, cross-platform integration, SAT, and more, to deliver a data-driven, holistic approach to measuring and mitigating human behavior.

It should integrate education, engagement and reinforcement strategies that align with how people learn and act in real-world scenarios. A robust platform embeds this human element—habits, awareness and decision-making—at its core. In doing so, it transforms your employees into proactive participants, rather than passive liabilities, in your organization's security. Without this depth, you risk investing in tools that provide the illusion of improvement without reducing real-world vulnerabilities. And that can leave you exposed to preventable threats.

Conclusion

In the face of increasing threats, game-changing AI innovations, and burgeoning regulatory requirements, now is the time to get serious about HRM. When building and executing your organization's HRM strategy, consider the advantages of collaborating with a partner that has a clear vision and proven outcomes for human-centric security management.

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