knowbe4

A Strategic Framework for Human Risk Management

What is Human Risk Management and Why Do Organizations Need it?

Whitepaper

WWW.KNOWBE4.COM

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

0825US

It's Not Just About Technology

Despite significant investments in cybersecurity technologies, the human element remains a primary factor in the majority of security breaches, with various industry reports attributing between 68% and 90% of incidents to human action or error.

However, this is not a time to start pointing fingers. Organizations must acknowledge the reality that, inevitably, people make mistakes. In today's work environment, employees are increasingly busy, highly distracted and often remote, so even when they do understand the dangers posed by cyber attacks, they may not have the time to fully comprehend them. This is especially true as the sophistication of social engineering attacks, now amplified by Artificial Intelligence (AI), make attacks more deliverable and that much harder to spot.

How can we expect employees to detect attacks, when traditional detection technology cannot?

Modern stresses in the workplace, combined with advanced social engineering tactics make it clear that traditional, compliance-based security and awareness training is no longer sufficient for mitigating pervasive threats. Therefore, many organizations are left with a critical strategic gap in their security posture. And what better to bridge the gap with than Human Risk Management (HRM) - a strategy that moves beyond simple awareness to systematically identify, measure, and mitigate human-derived risk through a continuous, data-driven process.

This whitepaper outlines the core principles of modern HRM and introduces a conceptual model for its implementation, structured around four key pillars: Defend, Educate, Empower, and Protect (DEEP). A central component of this model is the cultivation of a robust security culture, built upon proven principles of organizational behavior. Finally, it recommends the adoption of an integrated, AI-driven HRM platform as the most effective means of engaging employees. Such a platform provides the necessary tools for risk assessment, personalized education, real-time coaching and automated response, enabling organizations to transform their workforce from a potential vulnerability into a resilient layer of defense.

The Persistent Challenge of the Human Element

Traditional Tools Often Miss the Mark

Cybercriminals are masters of manipulation, playing on our innate human tendencies such as our desire to be helpful, our respect for authority, our fear of missing out or even just a moment of distraction. They are not just hacking systems; they're hacking human nature. This human element is a consistent theme in breaches.

For decades, the answer to human error was "more training!" or "more technology!" However, it has become increasingly clear over time that tick-box training and legacy detection technology will not solve the issue. In recent years, cybercriminals have become increasingly adept at formulating attacks that can easily bypass traditional detection technology such as the secure email gateway (SEG). In addition, security awareness training can often be generic, rarely engaging, and almost never tailored to how that specific individual in that specific role might be targeted.

KnowBe4 has long advocated against the approach of a generic, one-size-fits-all approach to security training, as it is rarely effective.

A New Playbook: The Rise of Strategic HRM

Instead, the focus needs to move away from a siloed spotlight on just training or just technology and include a holistic approach that centres around the human.

Enter the Human Risk Management approach.

This is not just Security Awareness and Training (SAT) with a fancy new name. It is a strategic, continuous process that blends technology, an understanding of why we do what we do, and a commitment to getting better every day.

The shift to HRM is about seeing the bigger picture, about building a resilient organization, and protecting hard-earned reputations by placing the emphasis onto people. This approach can be enhanced with a platform-based approach that helps organizations build cyber resilience by understanding and improving how people interact with technology. The platform combines AI-powered defensive controls, security education, user empowerment, and protective measures to create an environment where secure behavior becomes natural.

It is a process that works with people, not against them.

Mind Over Malware: The Behavioral Science Behind Smarter Security Habits

An effective HRM strategy must be built upon a clear understanding of the problem it seeks to solve. This involves analyzing the limitations of past approaches, the behavioral factors that contribute to human vulnerability, and the defining elements of a strong security culture.

The Inadequacy of Traditional Security Awareness Training

Historically, the primary response to human-related risk has been periodic, often compliance-driven, SAT. However, this approach has proven insufficient for several reasons:

- **Lack of Engagement**
  Traditional SAT often consists of presentations and quizzes that fail to capture employee attention or motivate genuine learning. Instead, employees rush to get through it and see it as a tick-box exercise.
- **Generic Content**
  A one-size-fits-all methodology does not account for the different roles, responsibilities, and threat exposures of individual employees. A financial controller faces different risks than a marketing associate, yet they often receive identical training.
- **The Awareness-Action Gap**
  Knowledge of a security policy does not guarantee its application under pressure. Awareness alone is often insufficient to overcome ingrained habits or in-the-moment cognitive biases, leading to a persistent gap between what employees know and what they do when faced with a real-life threat.

Recognizing Cognitive Biases

Cybercriminals are adept at exploiting predictable shortcuts in human cognition known as cognitive biases. Key biases exploited include:

Authority Bias
A tendency to comply with requests from perceived authority figures, making employees susceptible to emails impersonating executives or government agencies.

Optimism Bias
The belief that one is less likely to experience a negative event than others, leading individuals to underestimate their personal vulnerability to scams.

Familiarity Bias & Illusory Truth Effect
A preference for the familiar and a tendency to believe information that is easy to process and repeatedly encountered. Attackers leverage this by creating phishing messages that mimic legitimate communications, feeling familiar and therefore trustworthy.

Availability Heuristic
The tendency to overestimate the likelihood of events that are more easily recalled. This can lead to hyper-awareness of recent, publicised threats while lowering defences against less familiar attack vectors.

The Core Components of Security Culture

A weak security culture is a significant risk factor. Culture can be defined as the shared ideas, customs, and social behaviors that influence security. When these elements are underdeveloped, employees may lack the intrinsic motivation to act securely, particularly when they believe their actions are not being observed. Therefore, a positive security culture is a powerful mitigator of human risk.

At KnowBe4, a mature security culture is understood to comprise several key dimensions, including security-supportive norms, the quality of security-related communication, awareness of policies, security knowledge, attitudes toward security, and a shared sense of responsibility. Fostering these dimensions is a critical objective of any HRM program.

The Human Risk Management Approach

Addressing the multifaceted problem of human risk requires a new approach that goes beyond the basics.

In a nutshell, the HRM approach is a strategic, human-centric framework to cybersecurity that incorporates technical defences alongside understanding the 'why' behind people's actions. It acknowledges that human behavior is influenced by culture, psychology, and the design of our systems, so instead of just creating rules, HRM seeks to understand the motivations and daily pressures that guide employee decisions.

It must be noted that this is different from a HRM platform, which is the tool that can be used to achieve a meaningful and effective HRM approach. The HRM platform will be covered later in the paper.

Core Principles of a Modern Human Risk Management Approach

An effective HRM approach is built upon several core principles:

Identify Weak Spots
You can't fix what you don't know is broken. A proper risk assessment is your starting point – understanding who's likely to click on what, and why.

Personalization
The approach must be tailored to address the different threats and learning needs of individual teams and roles.

AI and Automation
Leveraging intelligent technology is critical to scale the approach, personalize interventions, and provide data-driven insights.

Continuous Measurement and Improvement
HRM is an iterative process that relies on tracking key metrics to measure behavior change and refine strategies over time.

Making Policy Human
Policies and procedures shouldn't read like legal contracts. If we want people to follow the rules, they need to understand them. That means using plain language, being empathetic to time constraints, and offering real-world relevance.

Human-Centric Design
Security should enable, not hinder, business operations. This requires empathy, clear communication, and processes designed with the user experience in mind.

Leadership Engagement
Executive sponsorship is essential to signal the strategic importance of HRM and foster accountability.

Remembering the Human Touch
Technology is brilliant, but sometimes a quiet word, a bit of coaching, or just making people feel part of the solution can make all the difference.

A Supporting Model: The DEEP Framework

To structure the implementation of the core principles involved in a HRM approach, a conceptual model such as DEEP (Defend, Educate, Empower, Protect) can be incredibly helpful. This conceptual model provides four distinct but interconnected pillars:

1 Defend: Stop attacks reaching people

This is all about technical safeguards. This means proactively reducing the attack surface with technical controls (e.g., AI-enhanced email security) to minimize the number of real-life attacks that reach employees.

2 Educate: Teach threat recognition

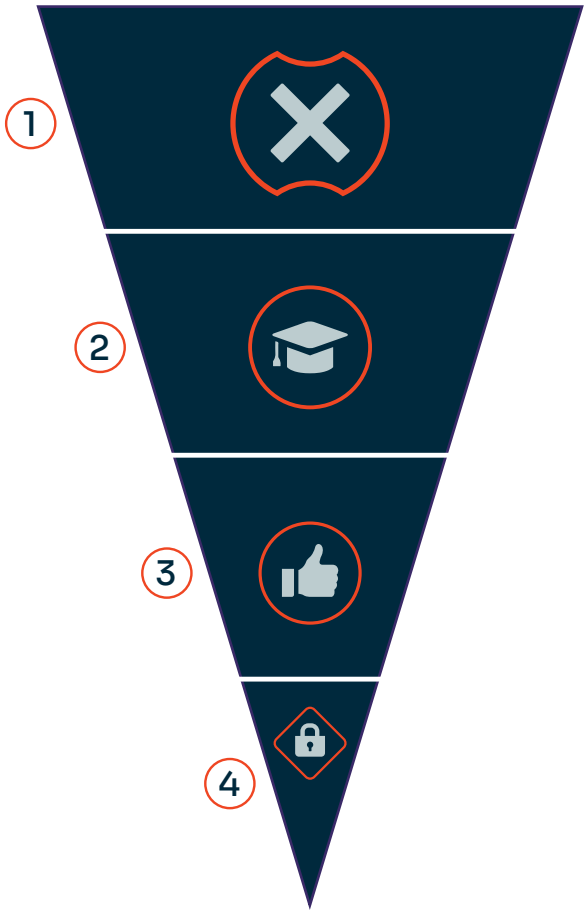
Here, we move beyond neutralizing threats and start building on human understanding. This includes equipping employees with the knowledge and skills to recognize and respond to threats through personalized, adaptive and relevant training.

3 Empower: Create a positive security culture

It's one thing to know what to do; it's another to feel able and supported to do it in the moment. Creating a supportive culture and providing user-friendly tools (e.g. one-click reporting buttons, real-time coaching and interactive anti-phishing banners) that make secure choices easy and intuitive.

4 Protect: Limit fallout from mistakes

No matter how impenetrable a security strategy may seem, unfortunately, mistakes still happen. Therefore organizations need to implement robust response plans to minimize the impact of an incident and use the data from such events to continuously improve the other three pillars.



This is not a rigid or linear process. It's a continuous loop. What you learn from a Protect scenario feeds back into how you Defend, what you Educate on, and how you Empower employees. It's all connected, like a well-oiled (and very secure) machine.

Recommendations: Implementing an Integrated HRM Platform

To effectively execute the strategy, we recommend adopting a modern, integrated HRM platform. This approach provides the scale, data integration, and automation necessary, which is unachievable with fragmented, individual solutions and their separate data sets.

At KnowBe4, we believe that tackling human risk effectively in the modern age requires more than just good intentions and a library of training videos. It needs a robust foundation. This means leveraging the power of AI, smart automation, and the seamless integration of security capabilities to build an intelligent system that learns, adapts, and helps your people become genuinely more secure. This philosophy is the very fabric of our HRM+ platform.

The KnowBe4 HRM+ Platform

KnowBe4 HRM+ is a comprehensive platform designed to put your own strategic HRM strategy into action, directly linked to the pillars of DEEP. It's designed to be personalized, relevant and adaptive, fortifying your organization against sophisticated threats and transforming your workforce from the biggest attack surface into your most valuable security asset.

Key capabilities include:

Security Awareness Training (SAT) & Compliance Plus
A comprehensive library of engaging, localized and personalized training content that serves as the foundation for the 'Educate' pillar.

Cloud Email Security
An AI-powered email security product that uses pre-generative modeling and deep neural networks to 'Defend' against advanced inbound phishing attempts and outbound data breaches over email.

PhishER Plus
A Security Orchestration, Automation, and Response (SOAR) product that automates incident response to 'Protect' the organization and reduce the workload on security teams.

SecurityCoach
A real-time coaching tool that integrates with the existing security stack to 'Empower' users by delivering immediate feedback and guidance at the moment of risky behavior.

AIDA (Artificial Intelligence Defence Agents)
A suite of AI agents that underpin the entire platform, enabling the personalization of training, generation of realistic simulations, and dynamic risk scoring required for a modern HRM approach.

The Role of Individual Risk Scoring

A critical capability of a modern HRM platform is the use of dynamic, individualized risk scores. By analyzing a wide range of behavioral data, including phishing simulation performance, training engagement and real-world security events, AI-driven engines like KnowBe4's SmartRisk Agent™ can generate a nuanced risk profile for each user.

This allows security leaders to:

- **Target Interventions**
  Focus resources and more intensive coaching on the highest-risk individuals and groups.
- **Identify Systemic Issues**
  Use collective risk data to pinpoint widespread vulnerabilities or ineffective processes.
- **Justify Investments**
  Demonstrate measurable reductions in aggregate risk to executive stakeholders.
- **Enable Personalized Journeys**
  Automate the delivery of appropriate levels of training, ensuring the program is both efficient and effective.

What Can Organizations Do to Achieve an Effective HRM Approach?

The persistent and evolving nature of human-related cyber risk necessitates a strategic evolution beyond traditional security awareness training and legacy technology. A comprehensive HRM approach, enhanced by a HRM program, built on principles of behavioral science, continuous improvement, and cultural development, is now a business imperative.

The most effective path to implementing such an approach is through an integrated, AI-driven HRM platform. By unifying capabilities for defense, education, empowerment, and protection, such a platform provides the tools necessary to identify risk, drive meaningful behavior change, and cultivate a resilient security culture.

As demonstrated by independent ROI analysis, this approach not only strengthens an organization's security posture by significantly reducing the likelihood of employee-driven incidents but also delivers tangible operational efficiencies and financial returns. Adopting a strategic HRM approach is a critical investment in organizational resilience, transforming the human element from a potential liability into a robust and reliable layer of defense.

The KnowBe4 Approach

At KnowBe4, our entire HRM+ platform is engineered with CISO-level strategic considerations in mind. We believe in a human-centric approach that is powerfully augmented by AI and automation. Our four pillars – Risk Identification and Assessment, Personalized Education and Enablement, Technology Integration and Automation, and Continuous Monitoring and Improvement – are designed to provide organizations with a comprehensive, data-driven and adaptive system for managing human risk.

Managing human risk is no longer a "soft" skill or a secondary concern. In an era of AI-powered attacks and ever-increasing digital interaction, it's a strategic necessity. And having an intelligent, integrated HRM platform is key to getting it right.

Learn more about KnowBe4's HRM+

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

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

knowbe4

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