knowbe4

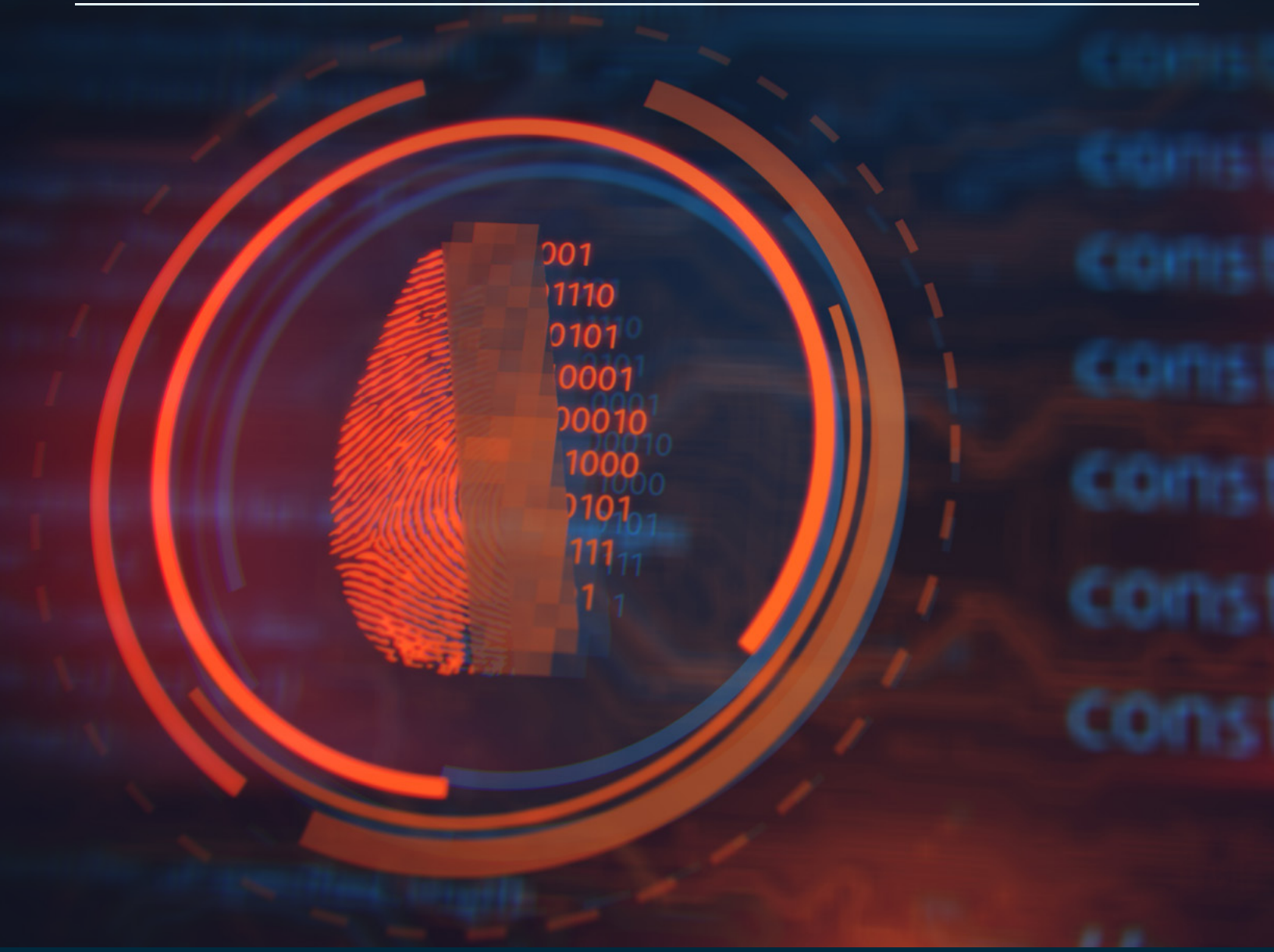
7 Best Practices

For Implementing Human Risk Management

WWW.KNOWBE4.COM

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

0359-C1025



Introduction

In cybersecurity, the biggest and most overlooked threat is human risk. With human error accounting for 68% of data breaches (according to the Verizon Data Breach Investigations Report), managing human risk isn't just important—it's essential. That's why Human Risk Management (HRM) has become a critical part of modern security strategies. Effective HRM goes beyond awareness training by taking a data-driven, behavior-focused approach to reducing human risk.

Implementing HRM effectively requires more than just policies and training—it demands a strategy that blends technology, psychology and continuous adaptation. Here are seven best practices to help organizations build a strong HRM program that drives real behavior change and strengthens overall security.

1 Engage Leadership and Build a Security Culture

HRM initiatives thrive on strong leadership and a culture of accountability. When top executives prioritize cybersecurity, the rest of the organization is more likely to follow suit. Engaging leadership involves:

- **Fostering Executive Buy-In**
  Highlight the financial, reputational and operational risks of neglecting human risk to secure leadership support. Present case studies and real-world examples of breaches caused by human error to underscore the urgency of proactive measures.
- **Cross-Department Collaboration**
  HRM is most effective when it integrates insights from HR, IT, legal and compliance teams. This collaborative approach ensures a comprehensive view of organizational risk, facilitates the implementation of cohesive policies, and avoids gaps in coverage.
- **Promoting Continuous Improvement**
  Leadership should champion ongoing security training and awareness initiatives to encourage a proactive, security-focused mindset across all levels. Regularly reviewing progress and adapting strategies ensures alignment with the latest threat trends.

When leadership sets the tone, it creates a ripple effect, embedding HRM into the organization's values and goals. This not only enhances security but also strengthens overall operational resilience.

"When top executives prioritize cybersecurity, the rest of the organization is more likely to follow suit."

2 Adopt a Culture of Accountability and Transparency

Accountability and transparency are critical to gaining employee trust and ensuring compliance with security policies. To foster this culture:

- **Set Clear Expectations**
  Communicate security policies and procedures in a way that's easy for employees to understand and follow. Regular reminders through newsletters or internal platforms can reinforce key policies.
- **Encourage Reporting**
  Create an environment where employees feel safe reporting potential security issues without fear of retribution. Anonymous reporting channels and clear follow-up processes encourage transparency.
- **Reward Positive Behavior**
  Recognize and reward employees who demonstrate good security practices. Acknowledging their efforts, through incentives or public recognition, motivates others to follow suit.

Transparency also involves openly discussing lessons learned from past incidents, which helps reinforce the importance of collective responsibility in safeguarding the organization. Regularly sharing updates on security efforts and their impact fosters a sense of shared ownership and accountability among employees.

3 Start with a Risk Assessment

A thorough risk assessment is the foundation of any HRM strategy. It allows organizations to:

- **Identify Key Risks**
  Pinpoint areas where employees are most vulnerable, such as phishing susceptibility or poor password hygiene. Incorporate threat intelligence to stay informed about industry-specific risks and emerging attack vectors.
- **Prioritize Efforts**
  Use risk profiles to focus on the most critical threats based on the organization's cybersecurity posture and business objectives. For instance, prioritize protecting high-value assets like customer data or intellectual property.
- **Align with Business Goals**
  HRM strategies should complement broader organizational objectives to ensure seamless integration. A risk assessment that aligns with business goals facilitates executive support and ensures that security investments deliver maximum ROI.

Risk assessments should be iterative, incorporating feedback and evolving with the organization's needs and threat landscape. Behavioral analytics can streamline this process by providing actionable insights into employee activities and potential vulnerabilities/risks. Periodic assessments help maintain an up-to-date understanding of risks and ensure continuous alignment with the organization's strategic objectives.

4 Personalize the Experience

Generic, one-size-fits-all approaches to security training are rarely effective. Instead, organizations should tailor their HRM initiatives to individual employees or groups based on:

- **Risk Levels**
  Employees who handle sensitive data or access critical systems may require specialized training. For example, a finance team might need targeted guidance on avoiding payment fraud scams.
- **Behavioral Insights**
  Leveraging analytics to understand how employees interact with technology and identifying high-risk behaviors. Using tools that flag risky actions, like repeated attempts to access restricted files, can help identify training priorities.
- **Engaging Content**
  Use gamification, microlearning and scenario-based exercises to keep employees engaged and motivated to learn. Simulations that mimic real-world scenarios, such as phishing attempts, enhance retention and readiness.

By personalizing HRM strategies, organizations can address specific vulnerabilities and foster meaningful behavior change. Regular updates to training content, based on evolving threats, ensure employees remain vigilant and well-prepared to combat new challenges.

5 Leverage AI to Automate and Enhance HRM Processes

Artificial intelligence (AI) is revolutionizing HRM by automating repetitive tasks and providing real-time insights. Key benefits of integrating AI include:

- **Behavioral Analytics**
  AI-powered tools can identify risky patterns, such as repeated failed login attempts or unusual data access. These insights enable security teams to intervene proactively and prevent potential breaches.
- **Phishing Detection**
  AI can simulate phishing attacks tailored to organizational contexts, helping employees recognize and report threats. Advanced AI models can also detect and block phishing emails before they reach inboxes, adding an additional layer of defense.
- **Streamlined Processes**
  Automating tasks like log analysis and risk assessments reduces the workload for security teams, allowing them to focus on strategic initiatives. AI-driven dashboards can provide instant summaries of organizational risk levels, empowering quicker decision-making.

AI enhances the efficiency and effectiveness of HRM, enabling organizations to stay ahead of emerging threats. However, it's essential to ensure AI tools are calibrated to align with organizational goals and ethical considerations, preventing biases in data interpretation or decision-making.

6 Measure, Monitor and Improve

Continuous improvement is the cornerstone of a successful HRM strategy. Organizations must:

- **Track Key Performance Indicators** (KPIs)
  Metrics such as phishing simulation click rates, incident response times and training completion rates provide valuable insights into the effectiveness of HRM initiatives. Benchmarking these metrics against industry standards can further highlight areas for improvement.
- **Conduct Regular Testing**
  Simulations and penetration tests help identify gaps and reinforce employee readiness. Frequent testing ensures employees stay alert and reduces the risk of complacency.
- **Incorporate Feedback**
  Use employee feedback and incident data to refine training programs and policies. Conducting surveys and focus groups allows employees to share their experiences and provide insights on improving security practices.

A data-driven approach ensures HRM strategies remain relevant and effective in an ever-changing threat landscape. Periodic reviews and adjustments based on measurable outcomes ensure long-term success and adaptability.

7 Incorporate Human Elements

While technology and analytics are essential, the human touch remains a vital component of HRM. Organizations can:

- **Provide Coaching and Mentoring**
  Pair employees with security champions or mentors to reinforce positive behaviors. Personalized guidance helps employees better understand their role in mitigating risks.
- **Offer Support for High-Risk Employees**
  Address stress, burnout or other factors that might lead to risky behavior. Providing access to mental health resources or flexible work arrangements can mitigate underlying issues.
- **Engage Employees in Security Planning**
  Involve staff in creating security initiatives to boost buy-in and relevance. Collaborative efforts, such as workshops or brainstorming sessions, make employees feel valued and invested in organizational security.

Balancing technical offerings with personal interactions creates a well-rounded approach to managing human risk. Human-centric initiatives foster trust and engagement, enhancing the overall effectiveness of HRM strategies.

Conclusion

HRM isn't a one-time initiative—it's an ongoing strategy that evolves with your organization and the ever-changing threat landscape. Successfully implementing it requires a multifaceted approach that balances technology, behavior and culture. By engaging leadership, conducting thorough risk assessments, personalizing training, leveraging AI, fostering accountability, continuously improving and incorporating human elements, organizations can create a robust HRM strategy.

By following these seven best practices, you can move beyond traditional security awareness training and build a proactive, data-driven approach to managing human risk.

Learn More

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

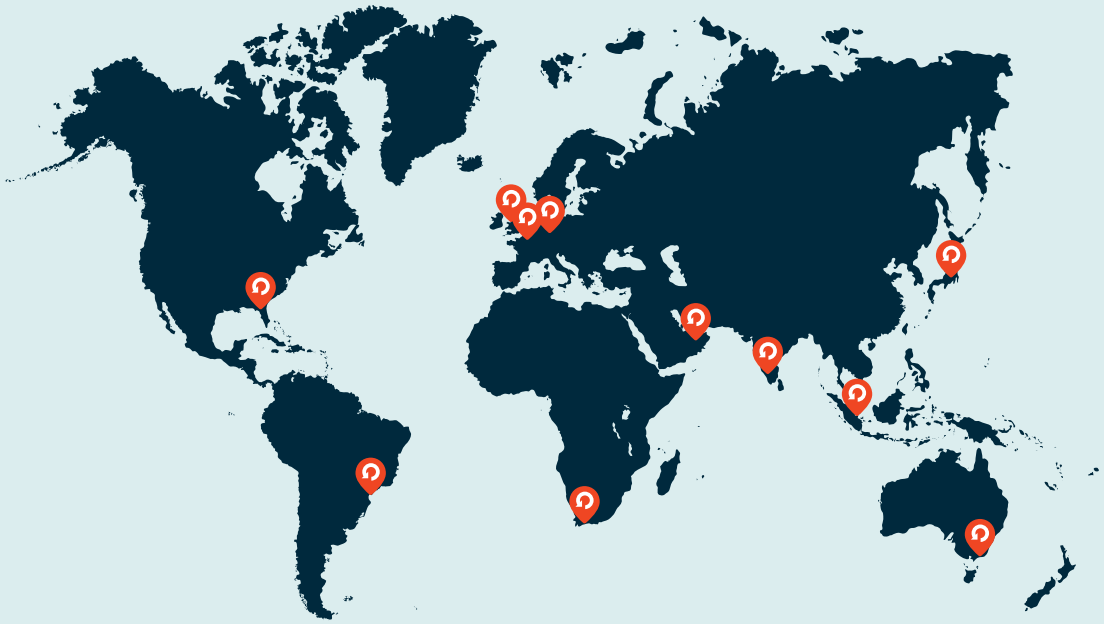
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test

Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 empowers workforces to make smarter security decisions every day. Trusted by over 70,000 organizations worldwide, KnowBe4 helps to strengthen security culture and manage human risk. KnowBe4 offers a comprehensive AI-driven "best-of-suite" platform for Human Risk Management, creating an adaptive defense layer that fortifies user behavior against the latest cybersecurity threats. The HRM+ platform includes modules for awareness and compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense Agents and more. As the only global security platform of its kind, KnowBe4 utilizes personalized and relevant cybersecurity protection content, tools and techniques to mobilize workforces to transform from the largest attack surface to an organization's biggest asset. 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