knowbe4

CISO's Guide:
Top 4 Considerations for Human Risk Management

Is Security Awareness Training Working?

Whether it's amorphic AI-powered attacks or well-known (and might we say dreaded) ransomware, threats are a constant source of change. Amid this chaos, people are simultaneously our greatest security vulnerability and our strongest line of defense. But are we doing everything we can to ensure the latter, minimizing human risk and maximizing protection?

To contain the risk that comes with being human, security awareness training (SAT) has long been the gold standard to improve cyber hygiene. However, it's not a one-and-done fix to thwart social engineering schemes or guarantee that employees won't inadvertently leak sensitive information. Like cybersecurity as a whole, to defend against sophisticated malicious actors, we need to layer defenses.

How Security Sits Within the Organization Has Changed

The alignment between CISOs and leadership is stronger than ever before. It took a while, but executives are waking up to the importance of security in...well...everything. Using real-world examples of breaches caused by human error, CISOs have a strong case on why mitigating human risk is critical for financial, reputational and operational health.

Around **77.6% of CISOs** now include risk assessments in their reports, and nearly **45% prioritize business impact analysis.**[3]

84% of CISOs now report alignment with their board on cybersecurity issues, up from 62% in 2023.[4]

This paints a promising future where decision makers understand how security issues affect the organization beyond compliance checklists. The shift in reporting and analysis suggests that discussions with executives are evolving to incorporate broader risk management strategies, including initiatives like insider risk mitigation and behavioral analytics.

Death, Taxes, and Human Error as a Top Security Risk

74%

of CISOs still view human error as the top cybersecurity risk.[1]

87%

are turning to AI-powered solutions to mitigate human-related threats, reflecting a move toward more proactive risk management strategies.[2]

1 Proofpoint's 2024 Voice of the CISO report
2 Ibid.
3 National CIO Review, CISO Reporting Landscape 2024
4 SOCRadar, CISO 2024 Top 10 Statistics and Trends

Not Just a Buzzword: Human Risk Management

CISOs are increasingly moving beyond traditional SAT and embracing a more comprehensive approach focused on Human Risk Management (HRM). This is not a simple name change. It's the next step in how we think about addressing human risk and a modification in strategy, process and technology.

HRM as a holistic approach for **identifying, quantifying and mitigating risks associated with human behavior.**

Four Pillars of Addressing Human-Related Risk

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 addresses four pillars:

Risk Identification and Assessment

Deepen your understanding of cybersecurity risks within your organization through a systematic approach.

Personalized Education and Enablement

Engage employees in unique and continuous learning experiences designed for behavior change.

Technology Integration and Automation

Improve risk management by joining cybersecurity systems and tools with an HRM platform that uses AI and machine learning.

Continuous Monitoring and Improvement

Regularly assess and tune HRM strategies using data-driven insights and adaptive security controls.

Top 4 Considerations for HRM

The security industry is known for its alphabet soup. But HRM isn't just another acronym. It's worth not only your attention, but consideration from all of your organization's leaders.

CISOs are at the helm of building a strong security culture — which is often already in motion with SAT. However, to turn your workforce into active defenders, you need HRM. Only then can you transform human error into human strength.

In this eBook, we'll help you on your way to HRM, giving you clarity on what it is, including the top four considerations for using it to improve your security outcomes.

1. The Difference Between SAT and HRM

Forrester Research formally retired its security awareness and training nomenclature in favor of a more comprehensive approach to measuring and mitigating human risk.

> If the majority of data breaches include the human element, are our efforts actually managing the threat? HRM makes us dig deeper into how we understand and manage human risk.

One of the greatest challenges with SAT is that knowledge does not always translate into behavior. Phishing simulations and annual training modules will only go so far, especially as threats intensify. Even with the best training, people have moments of weakness, slip up, and can cause security problems. CISOs need a solution to reduce or take away the reliance on humans for decisions that could create or deter a security event.

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
Quizzes and tests that don't take into account employees' security knowledge	Risk-based approach, which considers the individual and what they are exposed to
Training completion and quiz scores informing human risk scores	Rating human risk based on behavioral analytics from integrated technologies
Ineffective training schedules (too infrequent, too often or at random)	Training plus real-time interventions
Training platform siloed from other security systems	HRM platform that integrates with other security systems
Lack of visibility into how training impacts security posture	Demonstrable and quantifiable impact on cyber risk reduction

2. Now Is the Time to Adopt HRM

Timing and buy-in are common concerns for moving from SAT to HRM. As organization leaders look to CISOs for strategic cybersecurity decisions that will have a ripple effect through the business, knowing when to make changes is just as important as the change itself. Now is the time to adopt HRM because of four major drivers:

1. Social engineering and phishing attacks represent the single largest cyber risk.

According to research, 70% to 90% of all successful cyberattacks involve social engineering and phishing.[5] Attackers are a cunning bunch and they understand that our defenses have become significantly better. That's why they use more than technology to dupe us.

2. AI will keep compounding the problem.

AI is an arms race. Over 95% of cybersecurity professionals believe AI-generated content makes phishing detection more challenging.[6] In the hands of bad actors, AI is fueling a new breed of highly convincing social engineering attacks, including synthetic media ("deepfakes"). Employees need to be continuously educated on how to detect and report them.

3. Traditional employee education is no longer enough.

Traditional SAT alone is not an adequate defense today, although it is a critical layer. Much like reactive detection and response has strengthened to include proactive threat hunting, as an example, managing human risk amid the current threat landscape requires education and engagement on another level to improve real-world user behaviors.

4. Regulatory mandates are growing.

Organizations today 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. In response, we are seeing new regulations such as the SEC disclosure law, NIS2, and DORA in Europe requiring HRM as part of governance, risk, and compliance (GRC) frameworks.

For regulated industries, HRM has immediate value, as it provides measurable security outcomes to meet regulatory requirements. And because it is demonstrable, it can even improve cyber insurance eligibility.

[5] KnowBe4, If Social Engineering Account for up to 90% of Attacks, Why Is It Ignored?
[6] LastPass, Social engineering: Combatting an evolving threat, 2024

3. HRM Needs More Than a Human-Centric Veneer

If now is the time to adopt HRM, the natural next step would be to shop around. As HRM matures, many vendors will use the term, but may only have a veneer of human centricity. To get the outcomes you desire, it will be essential for you to be able to spot a true HRM platform.

> HRM transforms employees into proactive participants in your organization's security, rather than passive liabilities.

The Crux of Cybersecurity Risk Often Lies in Human Decisions

Effective HRM addresses human behavior rather than focusing on superficial metrics or isolated training events. These fail to create meaningful, lasting changes in behavior.

Let's take phishing testing as an example. 88% of respondents to a LastPass study think that their organization's phishing testing program is effective.[7] But as the report notes, there is clear cognitive dissonance. Ticking the boxes by sending out phishing tests can leave businesses susceptible to attacks. We've already seen social engineering becoming more sophisticated with AI. Now, employees must be active participants in fighting back against attacks that are meant to manipulate them. Employees must be as vigilant and adaptable as the threat itself.

Avoid the Illusion of Improvement

True HRM integrates education, engagement and reinforcement strategies that align with how people learn and act in real-world scenarios. 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.

[7] https://www.lastpass.com/-/media/483ac1cf3c8c4c80a48865a2b69bf4cf.pdf

4. Key Metrics and ROI for an HRM Program

SAT	HRM
Compliance-driven, training completion metrics.	Behavioral-driven, risk reduction KPIs.

If we look at how we measure SAT, the metrics primarily assess participation and knowledge retention, but they don't necessarily reflect real-world security behavior changes. While SAT is easier to track than HRM, there is an obvious winner for security improvements that align with business objectives. But CISOs need a straightforward way to justify the investment.

A thorough risk assessment is foundational to any HRM strategy and helps prove its ROI. Periodic risk assessments can help pinpoint areas where employees are most vulnerable and use risk profiles to prioritize areas of improvement. By aligning with business goals, and tracking improvements like reduction in credential sharing that could lead to leaking intellectual property, it can help facilitate executive support.

Justifying HRM Costs

While HRM provides long-term security benefits, it requires upfront investments in technology, training and personnel. CISOs may struggle to justify costs to leadership, especially if their current SAT programs already meet compliance requirements. The key consideration here is highlighting that even though the organization is, for example, below the industry benchmark for how many employees click on a simulated phishing attack, it does not account for real-time behavior and does not reduce security risks proactively.

SAT vs. HRM for Phish-prone™ Percentage

Phish-prone Percentage is the percentage of employees that are prone to click on a phishing link. But what if they delete the message and do not report it as phishing? SAT would look favorably on this action. Instead, we need to measure time to report rather than ignoring it. For HRM, we want to see the action rather than inaction because it demonstrates behavioral change. It provides more proof that if a real phishing incident were to happen, your employee would have the experience to spot and report the malicious email.

Metrics at a Glance

HRM focuses on proactive risk mitigation, behavioral changes and continuous monitoring rather than vanity training completion metrics. Because of this, how we measure the two are completely different.

Traditional SAT Metrics	HRM Metrics (Behavioral and Risk-Based)
▪ **Training Completion Rate (%)** – Percentage of employees who complete required security awareness training. ▪ **Phishing Simulation Click Rate (%)** – Measures how many employees fall for simulated phishing attacks. ▪ **Quiz/Assessment Scores (%)** – Average scores on cybersecurity knowledge tests post-training. ▪ **Time Spent on Training (Minutes/Hours)** – Measures how long employees engage with security training content. ▪ **Annual Security Training Participation (%)** – Ensures compliance but does not measure security behavior.	▪ **Human Risk Score (0-100 or High/Med/Low)** – AI-driven risk scoring based on individual employee behaviors, such as phishing susceptibility, login anomalies and sensitive data handling. ▪ **Phishing Resilience Index (%)** – Tracks not just click rates but how many employees report phishing attempts versus ignoring them. ▪ **Real Threat Reporting Rate (%)** – Percentage of employees who correctly report real-world phishing attempts and security incidents. ▪ **Risky Behavior Reduction (%)** – Measures improvement in behaviors like credential sharing, downloading unauthorized software or ignoring security warnings. ▪ **Just-in-Time Security Intervention Effectiveness (%)** – Tracks how often employees change risky behaviors after receiving real-time security nudges or alerts. ▪ **Insider Threat Detection Rate (%)** – Uses behavioral analytics to flag potential insider threats or negligent behavior before incidents occur.

Comfort Level: An Unmeasurable KPI

CISOs are responsible for cultivating an organization's security culture. One of the most important parts of that is how comfortable people feel with security. This may not be measurable, but it's essential.

HRM works to empower employees. If they make a mistake that could cause an incident, you want to know that they will identify the error and then report. In these cases, the security team has the opportunity to contain the mistake before it becomes an incident.

How HRM Identifies, Quantifies and Mitigates Human Risk

HRM takes a data-driven, holistic approach to human security risks. It readies security teams with an effective defense that stitches together insight into employee behaviors, vulnerabilities and daily threats. While HRM platforms vary, key capabilities should create a complete picture to manage human risks and set next steps.

At a glance: Shifting to HRM

AI-Driven Behavioral Analysis

Identify at-risk employees by analyzing user interactions across systems and platforms. Then tailor security training to their specific vulnerabilities.

Security Posture Assessment

Understand readiness through regular, 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.

Adaptive Assessment

Prevent complacency with relevant and challenging training by adjusting difficulty levels and attack vectors based on employee responses and adaptive assessments.

Integrated Threat Intelligence

Surface early warnings of targeted phishing campaigns, credential-stuffing attempts, and social engineering schemes through analysis of data from global threat feeds, dark web activity, and industry-specific attack patterns.

Comprehensive Risk Monitoring

Detect anomalies through continuous monitoring across email, cloud applications, and other systems to analyze communication patterns, access behaviors and device usage.

KnowBe4 HRM+ Personalized. Relevant. Adaptive.

HRM+ is KnowBe4's innovative approach to human risk management. HRM+ transforms your largest attack surface — your workforce — into your biggest asset, actively protecting your organization against cybersecurity threats, strengthening your security culture and reducing human risk.

Learn About KnowBe4's HRM+

knowbe4

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