FORTRA

From Awareness to Action: Embracing Human Risk Management in Cybersecurity

Mitigating the Human Risk Factor

Reducing cybersecurity exposure requires more than tools – it needs a security-focused culture. While solutions like Security Awareness Training (SAT) and Human Risk Management (HRM) are related, they differ in scope, depth, and strategic purpose.

SAT is a program that often includes targeted courses, quizzes, phishing simulations, that educates employees about cybersecurity threats and safe habits. Depending on compliance requirements, most organizations provide annual training for their workforce to improve awareness and knowledge.

HRM is a cybersecurity approach to manage and reduce the risks associated with human behavior in an organization. Through data, behavior monitoring, and integrations, HRM can be tailored to specific individuals thereby creating a security awareness to empower employees.

Having an HRM solution that includes SAT fosters a proactive and adaptive security program by reducing cybersecurity risks related to human behavior.

Mitigating the Human Risk Factor

The Hollywood image of a hacker surrounded by screens, typing methodically to break into a system is not only outdated, but oversimplifies the reality of today's cybersecurity landscape. In an era of AI-powered attacks and increasingly sophisticated automated phishing campaigns, the most significant vulnerability is the human risk factor.

Over 3.4 billion phishing emails are sent every day, and if users are not adequately trained to detect them, it's only a matter of time until one of the users falls victim to one. An up-to-date firewall, strong antiviruses, and strict hardware policies are essential to cybersecurity. But, at the end of the day, the most important element of your cybersecurity strategy is the people in your organization.

Users need the right tools and education to recognize cyber threats and respond effectively, even in uncertainties. Mitigating the human risk factor is about empowering users to work safer and smarter. A people-centric cybersecurity training program aims to lower human risk by fostering lasting behavioral change, cultivating a security-minded attitude among employees, and ultimately building a security-focused culture throughout the organization.

When seeking executive-level buy-in, present human risk management as a valuable benefit for employees. Emphasize the positive aspects of the program, rather than letting it be viewed as a tedious obligation. Reinforce that an HRM program should be presented as a clear demonstration of the employer's care and consideration for their workforce.

The 5-Step Framework for Successful Human Risk Management

Think of SAT as the tactical "what" and HRM as the strategic "how and why." A strong program starts with training but evolves into full HRM to create a resilient security-focused culture. You need both to be successful.

Enterprise-wide cybersecurity awareness may seem like a tall task but can be a simple process once you break it down into an easy-to-implement framework. Categorize the training needs by employee role or department, make sure content is engaging and adapted to the user's reality, and you'll be well on your way to making lasting behavioral changes within your organization.

1. **Analyze:** Assess current maturity, audience segments, risk behaviors, compliance needs, budgets, and resources — a tailored foundation.
2. **Plan:** Build your awareness roadmap by defining team roles, campaign goals, content formats (e- learning, phishing simulation, surveys), KPIs, and stakeholder communication.
3. **Deploy:** Launch with pretesting, then kick off campaigns. Use support materials such as posters, newsletters, and videos, to reinforce messages and boost engagement.
4. **Measure:** Track defined KPIs and metrics. Monitor performance against objectives, demonstrate impact across the organization, and inform next steps.
5. **Optimize:** Analyze results to identify improvements. Adjust content, campaign strategy, and update goals. Hold postmortems to iterate and build resilience.

Choose the Right Partner

A cybersecurity training provider is not just a supplier but should also be a visionary partner. Seek a human risk management solution from a company that utilizes a consultative approach, taking the time to understand your unique situation and anticipate your needs. The right partner has the experience and subject matter expertise to help you plan and execute a security awareness program designed specifically for your organization.

When you bring in a partner, you gain access to an expert team who can assess and analyze your data to help you measure and optimize your HRM program. Remember, you don't have to go it alone!

A visionary human risk management partner will:

- Offer expert advice and coaching to plan and execute your security training program. They also will understand potential roadblocks, anticipate challenges, and be available to you throughout your campaigns.
- Provide expertise and insights to optimize your programs, motivate users, and drive behavior change.
- Work with you to analyze data and provide both results and insights, pinpoint strengths and successes, and identify areas for improvement.
- Use a proven informative approach and methodology for adult eLearning.

Breaking the Social Engineering Attack Chain

Supported by our team of offensive and defensive security experts, Fortra HRM identifies risky actions attackers exploit and reinforces positive behaviors that disrupt them. This empowers users to become a strong line of defense, driving measurable reductions in organizational risk. Fortra breaks the social engineering attack through:

Minimizing Real Human Risk

- Diverse training formats including role-based courses, microlearning, nanolearning, and cybergames that keep users engaged and reinforce key behaviors.
- High-impact learning paths using real insights from Fortra's offensive and defensive security teams, ensuring users develop the behaviors that stop attacks.
- Phishing simulations grounded in emerging social engineering tactics, testing, and reinforcing user behavior based on real-world adversary methods.

Activating Human Defense

- A "Report Phish" button makes it simple for users to easily report suspicious emails.
- Fortra Suspicious Email Analysis, driven by the Fortra security operations center (SOC), delivers rapid triage and disposition of all user-reported emails.
- Timely response is provided to users, closing the loop and acknowledging positive behavior.

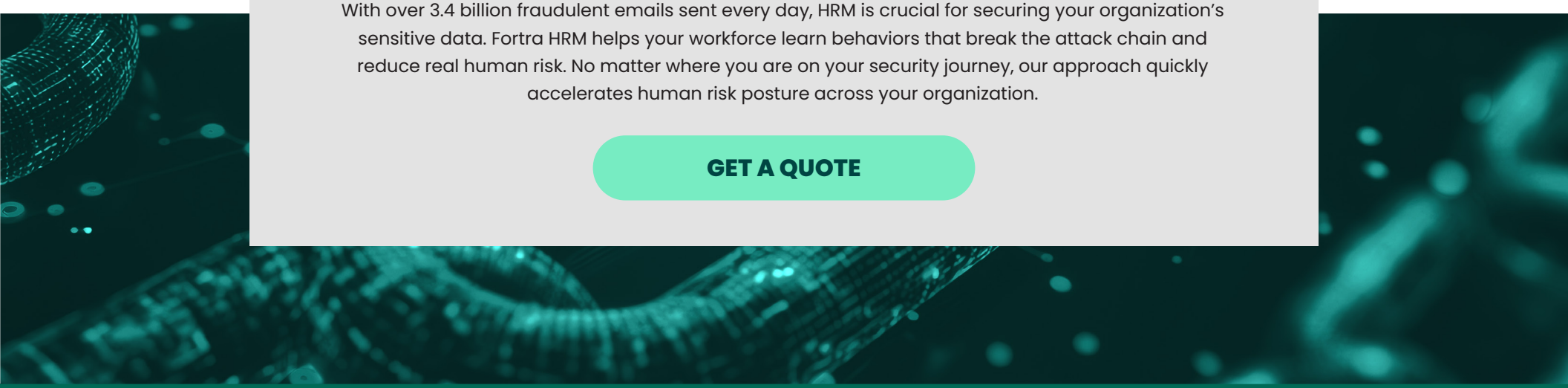
Leveling Up Fast

- Packages and pre-built training plans are available for every maturity level, helping administrators move quickly to improve.
- Our optional Managed HRM, program management by our HRM professionals, allows your internal admins to spend more time on program strategy and leadership instead of day-to-day operations.
- Our optional HRM Advisory Service provides plan customization and expert guidance that helps admins quickly assess their current state and launch strategic initiatives to improve their program maturity.

Break the Attack Chain With Fortra

With over 3.4 billion fraudulent emails sent every day, HRM is crucial for securing your organization's sensitive data. Fortra HRM helps your workforce learn behaviors that break the attack chain and reduce real human risk. No matter where you are on your security journey, our approach quickly accelerates human risk posture across your organization.

GET A QUOTE



FORTRA®

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

fta-corp-gd-0825-r1-vm