



Global Healthcare Leader Launches Scalable Human Risk Program with Living Security's Unify Platform

Challenge

A global leader in healthcare set out to build a human risk management (HRM) program that could scale across a workforce of over 120,000 employees—despite having only 1.5 full-time employees (FTEs) dedicated to security awareness and culture.

Starting with social engineering risks, the organization prioritized identifying segments of the workforce most vulnerable to attack. By combining role data, threat intelligence, and behavioral indicators, contractors quickly emerged as a high-risk group due to consistently low vigilance.

"We needed more than check-the-box training," said their HRM Program Leader at the organization. "Our goal was to identify real human risk and respond with the right message, for the right person, at the right time."

Instead of launching broad campaigns, the team implemented a tailored onboarding process specifically for contractors—addressing key knowledge gaps early and effectively.



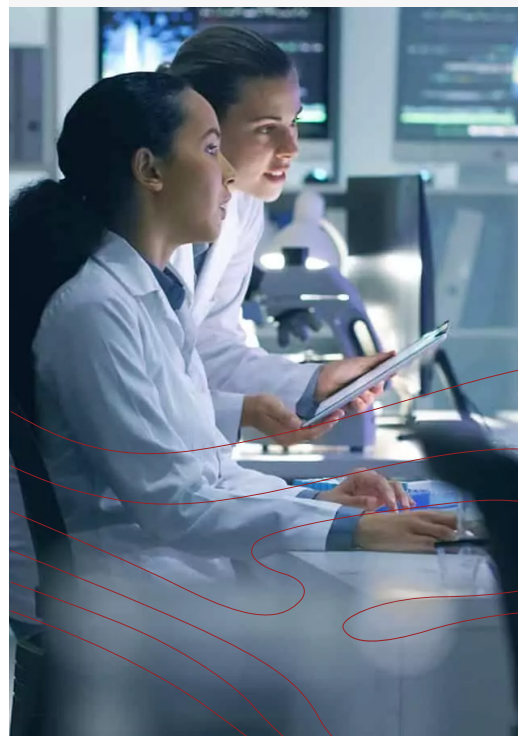
INDUSTRY:
Healthcare & Life Sciences



LOCATION:
Midwest Region



COMPANY SIZE:
120,000+ employees



Solution

Using Living Security's Unify platform, the organization unified and expanded visibility into previously siloed risk data. This enabled a smarter, more targeted approach to training—rooted in real-world behaviors and access patterns.

Their contractor-focused onboarding strategy led to a **2x increase in phishing reports submitted by contractors to the SOC**, converting a traditionally disengaged population into proactive participants in risk reduction.

Building on that momentum, the team next focused on another high-risk group: employees with USB port access exceptions. These individuals were identified, profiled, and enrolled in custom, access-aware training tailored to their unique exposure.

Most recently, the program expanded to include users frequently flagged for travel—closing the loop between HRM and technical security teams to improve safeguards for mobile employees.

Why Living Security

This organization's journey illustrates the power of starting small and scaling strategically:

- 1 Start with visibility:** Use data to reveal real risk before launching training
- 2 Act on insights:** Align interventions to actual behavior, access level, and threat exposure
- 3 Earn support:** Show impact with metrics that resonate across leadership

By partnering with Living Security, the organization moved from a reactive security awareness model to a proactive, data-driven HRM strategy—where risk isn't just monitored, it's meaningfully managed.

Results

In under two years, this global healthcare organization transformed its HRM program from a small, resource-constrained effort into a strategic component of its cybersecurity posture. With measurable results and growing executive support, the team has expanded from 1.5 to 3.5 FTEs, with continued investment on the horizon.

Key outcomes include:

2x increase in proactive phishing reports from high-risk contractor populations

Behavioral segmentation and tailored training for USB users and access exception cases

Cross-functional alignment with technical security teams supporting higher-risk employee groups (e.g., frequent travelers)

Executive buy-in and funding driven by demonstrable outcomes from Unify insights