

Training Effectiveness Proof Uncovered in Unify HROC

A 7,500-employee company sought to prove that their security training program actually improved their overall security posture. Using their Human Risk Operations Center (HROC) via Unify, Living Security’s Human Risk Management platform, they looked at behaviors before and after training deployment. What’s more, their HROC enabled them to uncover this data without any manual reporting.



What is an HROC?

Somewhat similar to a Security Operations Center, or SOC, the HROC by Living Security pulls in data across many cybersecurity technologies and uses it to show risk at the employee level. This helps security leaders prioritize risks and quickly take action among a set of employees.

This one-pane-of-glass view, the HROC, also segments risk by department, role, location, and even a lens into risk specific to those who have elevated access to sensitive data. Looking at risks this way provides important context to surface cybersecurity at the business level. For example, does the marketing team share files too readily to people outside the company? Does the finance department have good MFA hygiene?

The data comes from a company’s existing tools—including Microsoft 365, Proofpoint, Mimecast, CrowdStrike, 1Password, LastPass, Zscaler, Living Security’s phishing and training platforms, and many more—that integrate with the HROC to show a view

into risks with a perspective of human risk. These tools help provide guardrails for security, but the human element is a factor in almost all breaches. The HROC brings all of these factors together to get the best investment out of the tools and cultivate the best, most secure behavior in employees.

Company solves for phishing vulnerability discovered in the HROC

Recently a 7,500-employee company used Unify’s HROC to...

- Prove that training successfully changes human behavior.
- Mitigate risk efficiently by training only the organization’s riskiest employees
- Save hundreds of hours of unnecessary training, keeping employees focused on their jobs
- Reduce hours of manual reporting to surface risk; Unify shows it in one view

Unify proves that phishing training effectively reduces the number of repeat clickers

Via the HROC, the company saw that 126 employees clicked on a recent phishing simulation.

Instead of training the whole organization, they used a pre-built phishing simulation training from Living Security's Training platform to deploy training only to those who clicked on the simulation.

Of those that received the training, 85% of them completed it.

Post-training, they ran a phishing simulation again to the 126 original clickers. Unify indicated that only nine of them clicked the second simulation. Ninety three percent of the original clickers did not click again, signaling that the training had an impact, that behavior was changing.

HROC identifies risky behavior easily, speeding time to mitigation

Unify's HROC pinpoints specific users that show risky behavior, enabling this organization to create targeted action plans. In this case, when an employee clicks on a simulated phishing campaign, they must complete additional phishing training. They use Living Security's Training platform to pre-configure a phishing training campaign that's deployed in a few clicks.

The HROC also surfaces trends in vigilance among those users, indicating that they engaged with the training and then either did or did not click on another phishing simulation or interact with real phishing instances.

Unify's HROC saves hundreds of hours of employee training time

With only a small percentage of employees showing vulnerabilities around phishing, it would not make sense to force everyone to take additional training. Unify enables this organization to target only the employees that need training.

This targeting saved the non-clickers from additional training. Instead of sitting through training they don't need, they stayed focused on their work. If only 20% of the institution's employees show risky behavior and require training, it means that more than 5,500 of employees save hours of time by NOT having to take additional training.

Even the people who needed the additional phishing training saved time; micro-learning and gamification from Living Security keeps training interactive, brief, and effective.



Living Security's HROC saves hours of reporting time

Prior to using Unify, this organization pulled multiple manual reports from the phishing simulation tool and the training tool to understand which employees put the organization at risk. Unify's HROC pulls and shows data from these tools automatically, showing a HROC that pinpoints the biggest risks, helping prioritize projects that will have the biggest impact to mitigate risk.

More integrations bring more efficiencies

This is only the tip of the iceberg for this company. As their training program evolves, Unify will allow them to cross-reference the phishing simulation data with other security behaviors and event monitoring tools, such as identity management and data loss protection technologies. Unify's HROC integrates with most cybersecurity technology, helping CISOs, SOCs, and program owners analyze all security data at the human level on one pane of glass.



To learn more about how Living Security helps organizations quantify their human risk, identify areas to target, and change security behaviors visit www.livingsecurity.com.