RISKY BUSINESS

WHO PROTECTS AND WHO PUTS YOU AT RISK

INSIGHTS FROM 100+ ORGS ON
THE R.O.I. OF MANAGING HUMAN RISK

RISKY BUSINESS

WHO PROTECTS & WHO PUTS YOU AT RISK

Every cybersecurity leader knows that employees represent both their most critical exposure and their most valuable asset. What most don't know is who's who. The challenge lies in understanding which individuals are most exposed, how to identify them, and what, if anything, can be done to effectively manage human risk.

This report meets that challenge head-on with hard data collected from the Human Risk management (HRM) programs of over 100 organizations over the past several years. The HRM dataset extends far beyond phishing clicks and training completions, encompassing over 200 real-time risk signals that span external threat events and a wide variety of user behaviors and attributes.

You'll find honest, analytical answers to the questions listed in the contents. Those answers are guaranteed to change how you think about and manage human risk for the better.

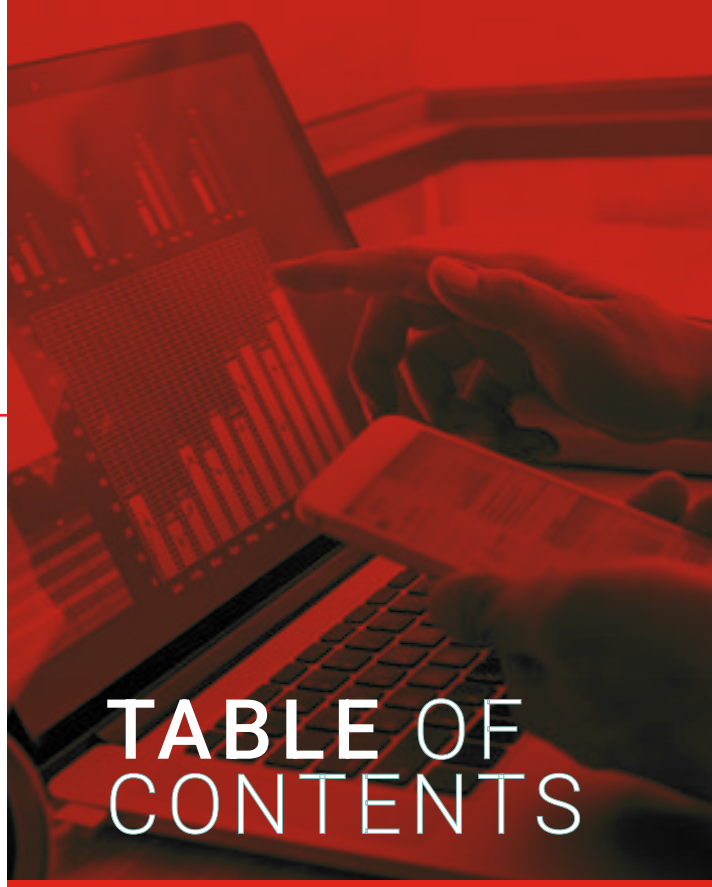


TABLE OF CONTENTS

Key Findings

Human risk is not evenly distributed across the workforce.

- 10% of users account for 73% of all risky behavior within their organizations.
- The riskiest users aren't always who or where you expect. Remote and part-time workers are often less risky than the colleagues you see in the office every day.
- 78% of users actually help to reduce exposure more than they add to it.

Gaining comprehensive visibility into human risk is a challenge.

- On average, firms have the capabilities to detect less than half of all events and behaviors that constitute human risk.
- Visibility into human risk activity drops to 12% for organizations relying solely on security awareness training (SAT).
- Mature HRM programs routinely achieve risk visibility that's 5x greater than SAT alone.

Human risk management isn't a misnomer; it works.

- Organizations using Living Security's Unify platform saw their population of risky users drop by half over the last year (from 43% to 21%).
- After completing action plans, users spent an average of 60% less time in a risky state. That effect is even stronger for risk specific to data loss–98% less time!

What constitutes human risk?

Ask any IT or security pro what comes to mind when you say "human risk," and you'll almost always hear one word: phishing. No surprise—it's the start of every annual training slideshow we half-watch while checking email.

It's also long been a major threat vector. Verizon's 2025 Data Breach Investigations Report (DBIR) found that phishing and other forms of social engineering contributed to 17% of all breaches. But does this capture the sum of human risk? No!

The last few DBIRs have reported that the "human element" plays a role in about three-quarters of all breaches. Their definition not only includes phishing but also intentional misuse by insiders, unintentional actions (e.g., drive-by downloads, misconfigurations), and compromised user credentials. This is certainly a much broader concept than what's covered in most Security Awareness and Training (SAT) programs—but is it broad enough? Again, we say no.

Living Security analyzes over 200 real-time signals—spanning identity access, user behavior, and external threats—to provide a comprehensive, 360-degree view of human cyber risk. Each signal (or insight) is evaluated for its impact and categorized as vigilant, neutral, or risky, offering security teams a nuanced understanding of what truly drives or reduces exposure. This approach helps pinpoint not only who poses a risk, but also who is strengthening security, so organizations can take precise action.

Figure 1: Breakdown of human risk signals in Unify

Living Security categorizes human risk signals as behaviors, events, or attributes. Behaviors include user actions that both raise and lower risk. Events are threats that occur to or around users that aren't their own doing, but nevertheless affect risk. Attributes capture inherent user traits related to role, access, and tenure.

FOUNDATIONAL HUMAN RISK SIGNALS

Every organization is unique, but many human risk programs start with the following signals:

VIGILANT INSIGHTS

- Report phishing email
- Password manager used
- Credentials reset
- Training completed
- MFA active

RISKY INSIGHTS

- Simulated phish clicked
- Poor credential hygiene
- Credentials compromised
- Training overdue
- Malware detected

How visible is human risk?

Visibility is a core concept in HRM and is referenced often in this report. Generally speaking, this refers to an organization's capacity to see all aspects of human risk. Specifically, we measure visibility based on the scope of human risk signals (see Figure 1) that can be detected when tools in an organization's tech stack are integrated into Unify.

What level of risk visibility is typically achieved? Well, that depends. Figure 2 plots a sample of active organizations[1] (represented by dots) along the axis based on the proportion of all observed[2] human risk they're able to detect. On average, firms have visibility into just under half (43%) of risky events and behaviors.

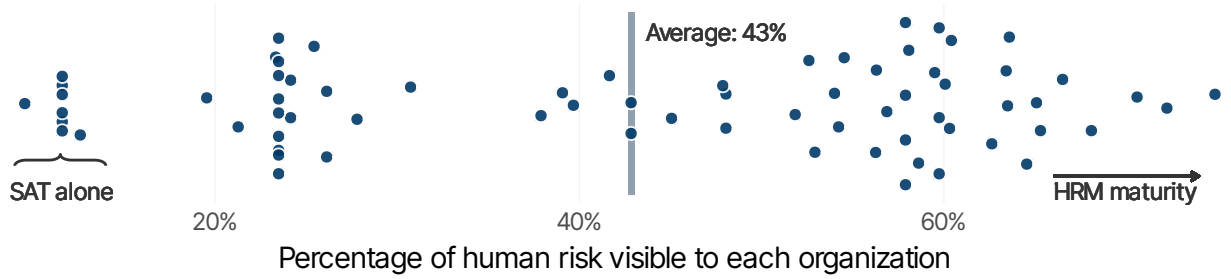


Figure 2: On average, organizations can detect 43% of all human risk activity. Visibility increases dramatically in mature HRM programs.

The "on average" part of that statistic is important because Figure 2 makes it obvious that there's wide variation among organizations when it comes to human risk visibility. Those on the very low end (~12%) have only implemented basic SAT and have low visibility into the broad spectrum of human risk. Visibility levels increase as organizations move forward in their HRM journey. The cluster on the right consists of mature programs that, through diverse integrations, have the ability to detect a large majority of human risk activity that is 5x that of SAT alone.

STREAMS OF VISIBILITY

Risk visibility is based on integrations (or "streams") that enable firms to detect human risk signals. These streams include solutions ranging from phishing simulations to endpoint detection and response (EDR) to identity and access management (IAM).

Based on our data, companies with five or fewer streams can only see 21% of all human risk, on average. Organizations with 16 or more streams into Unify gain the capability to detect two-thirds of all human risk activity.

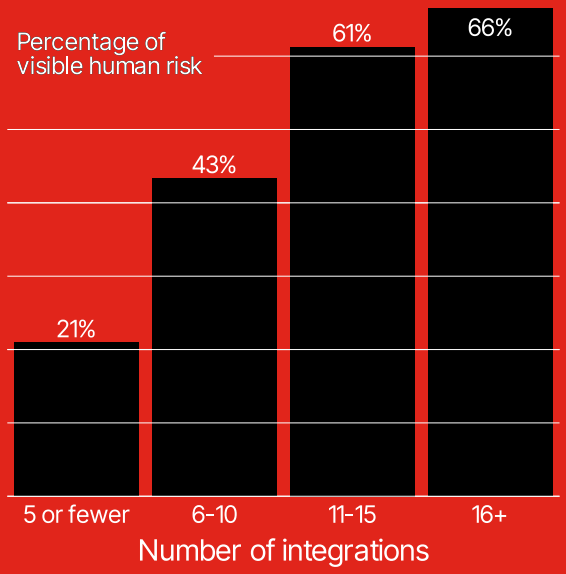


Figure 3 (right): Integrations increase visibility

[1] We've selected organizations that have a sufficient quantity and history of activity in the Unify platform.
[2] "Observed" in this context means the risk signal was actually detected by at least one firm in our sample.

How should we interpret these statistics on human risk visibility? Is being able to see 43% of all observed human risk signals sufficient? That's not something we can fully settle in this report, but we can further explore the concept of sufficiency.

We'll start by measuring the scope of all human risk that is actually detected or experienced by organizations. Figure 4 averages that ratio at 19%, although it ranges from 1% to over 40%. You can compare this directly to the risk visibility stat above. The typical firm can detect 43% of all human risk activity, but actually detects a much lower 19%. In that sense, organizations have more than enough visibility, on average.

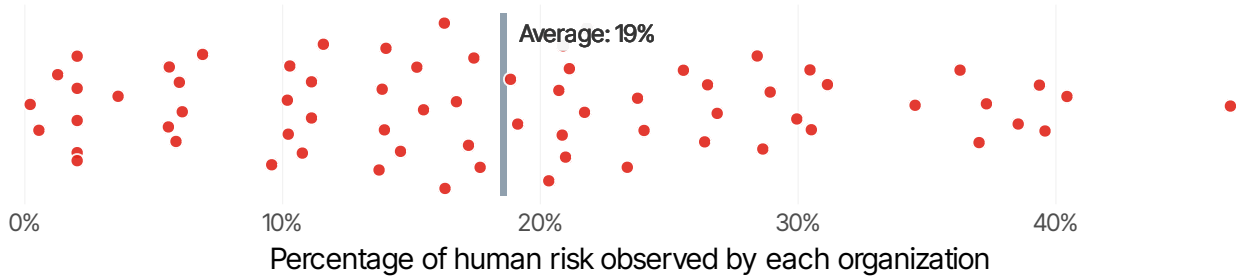


Figure 4: On average, organizations actually detect 19% of all human risk activity.

We can also assess sufficiency relative to each firm's visibility. The axis in Figure 5 has been modified to show the proportion of observed human risk specific to each organization. It asks, "Are we actually detecting everything we're able to see?" Organizations that are at 100% have detected everything their integrations enable them to, which means they're likely missing risky activity they have no means of detecting. Conversely, firms on the other side of the scale likely have ample coverage relative to what they're currently experiencing.

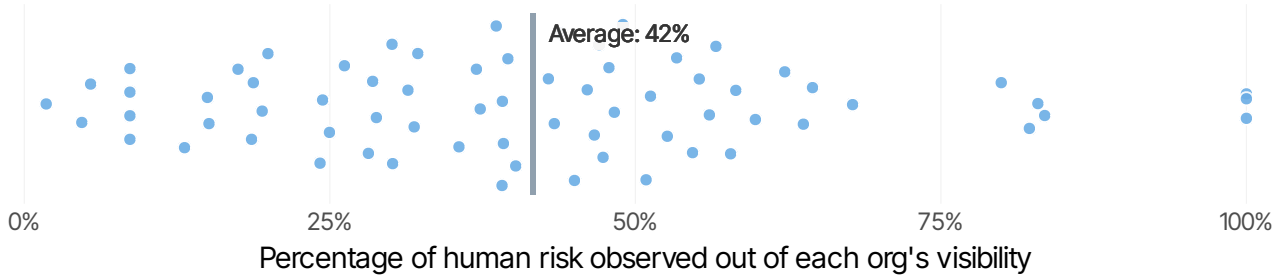


Figure 5: On average, organizations detect 42% of human risk activity they're able to see.

So, where does that leave us in terms of assessing the sufficiency of risk visibility? It could be argued that anything less than perfect visibility means organizations are blind to some potentially critical areas of human risk. Practicality, however, dictates that the optimal level of visibility should be based on each firm's exposure to human risk and its strategy for managing it.

Whatever your perspective, these findings should provide motivation to assess gaps in human risk visibility within your own organization.

How prevalent is human risk?

Now that we've established the broad scope of human risk, you may wonder which types of risky events and behaviors are most common and/or concerning. All risky insights defined in Unify fall into the following high-level categories:

- **TRAINING COMPLIANCE:** Monitor training compliance status for users and segments across the enterprise.
- **PHISHING & EMAIL:** Identify the users most and least at risk of social engineering attacks and protect them.
- **MALWARE THREATS:** Proactively protect users from malware, including viruses, worms, Trojans, spyware, adware, and ransomware
- **DATA LOSS:** Pinpoint when data is at risk of leaving your controlled environment through unauthorized access or malicious intent.
- **IDENTITY & ACCESS:** Get visibility into the most susceptible users for account compromise and mitigate their risk.

The chart below compares the relative frequency of risky events and behaviors in each of these categories. The position of organizations along the axis indicates the percentage of their observed risky insights that correspond to that category. For example, Malware Threats account for 20% to 30% of risk exposure for the majority of companies, but approach 50% for two of them.

In general, risk signals associated with Identity & Access tend to be the most common, while Data Loss is less prevalent. However, there's a huge amount of variation among organizations in each human risk category. Notice how there are a couple of companies with 2% to 4% of their risky insights in the Identity & Access category and another two that exceed 60%. That kind of variation illustrates why it's so important to gain visibility into human risk in your own workforce.

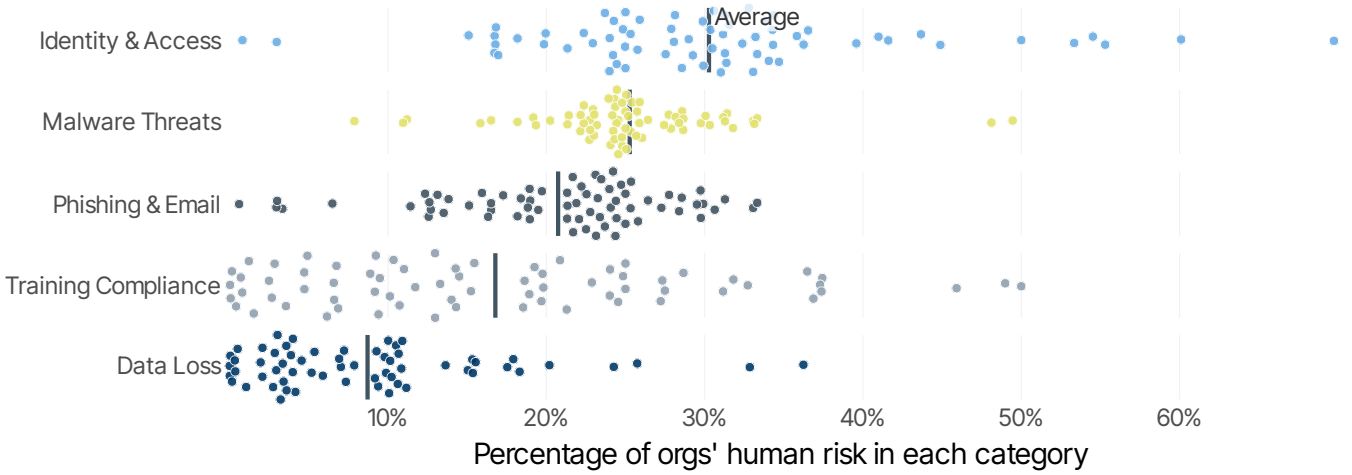


Figure 6: The prevalence of human risk varies widely within organizations and by category

These five categories grant a high-level view of the scope and prevalence of human risk, but not much in the way of specific behaviors or events. That's what the 200+ unique risk insights tracked in the Unify platform provide. Table 1 lists a sample of these insights generally considered more impactful to human risk, along with the percentage of organizations and users that have observed them.

Stats for 20 highest impact insights observed		
	% of orgs	% of users
Simulated Phish Clicked Multiple Times	53%	3%
Phish Clicked	40%	0.5%
Phish Clicked Multiple Times	40%	0.2%
Targeted by real phish with high rate or severity	32%	1%
Action taken on simulated phish website	29%	2%
Malware detected	29%	0.1%
Malicious data detected	24%	0.1%
Opened an attachment to simulated phish	14%	1%
Unauthorized changes made to EDR settings	12%	0.007%
Violated outbound data policy	11%	0.2%
Entered credentials on simulated phish website	8%	1%
Accessed suspicious data	4%	0.008%
Uploaded sensitive data	3%	0.002%
Shared a credit card without encryption	1%	0.2%
Shared social security number without encryption	1%	0.06%
Shared a passport without encryption	1%	0.05%
Shared a bank account without encryption	1%	0.04%
Malicious Website Visited Repeatedly	1%	0.02%
Website Blocks Bypassed Repeatedly	1%	0.001%
Malware installed	1%	0.0009%

Table 1: Sample of risky insights with high impact rating

We say "generally considered" because impact ratings are neither universal nor static. The same insight may be considered high risk in certain contexts or combinations but not in others. Even so, the insights listed here are things you'd likely want to know about if/when they occurred.

Note that the percentages attributed to users who trigger these events are quite low. But those numbers grow much larger at the organizational level.

That's a good reminder of one of the core challenges of managing human risk. It's great if 99.9% of your workforce doesn't engage in risky behavior. But it only takes one to download malware, disclose sensitive documents, or fall for a scam to trigger a major incident.

Therefore it's critical to identify the subset of users who most strongly affect your risk exposure. How big is that subset of uber-risky users? Find out in the next section...

ARE SOME HUMAN RISK INSIGHTS MORE COMMON THAN THESE?

Yes; Table 1 just includes some of the more impactful ones. For example, 73% of users clicked on a simulated phishing email. 46% show failed login attempts. 32% recently completed security training. None of these are likely to sound alarm bells, but taken in aggregate, they (and many others) contribute to a holistic, dynamic view of human risk.

Are some employees riskier than others?

Reviewing the user-level stats in the prior table demonstrates that a small proportion of users trigger these high-risk insights. Based on that, a question arises as to whether the same few users are responsible for a large proportion of risky events and behaviors for their organization. It's a question that's definitely worth answering.

To begin exploring this question, we tallied all insights for each (anonymous) user as a ratio of all insights observed by their organization. Very few employees generate more than 1% of their organization's risky insights. So, there's not one single person who can be reformed or removed to solve your human risk problem.

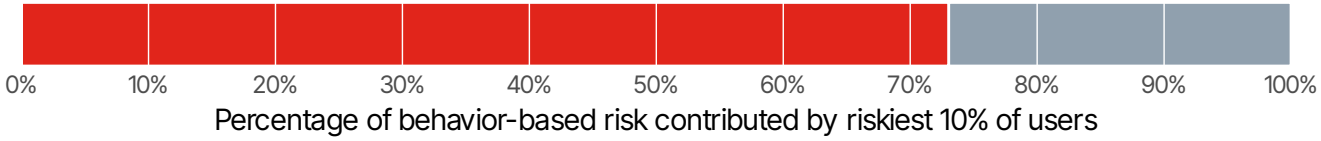


Figure 7: 10% of users account for 73% of all risky behavior within their organizations

That said, risk is certainly not evenly distributed across all users. Just 10% of users are responsible for about two-thirds of identified behaviors and events. If we focus solely on risky behavior (excluding external events over which users may have no control), the distribution of human risk is even more lopsided. The worst 10% of offenders are responsible for nearly three-quarters of all risky behavior observed (Figure 7)!

We can apply that same concept to the five insight categories presented earlier. Data risk is the most imbalanced, but over half of human risk in each category ties back to just 10% of users. That suggests organizations can achieve some quick wins by focusing on action plans and controls specific to those users.

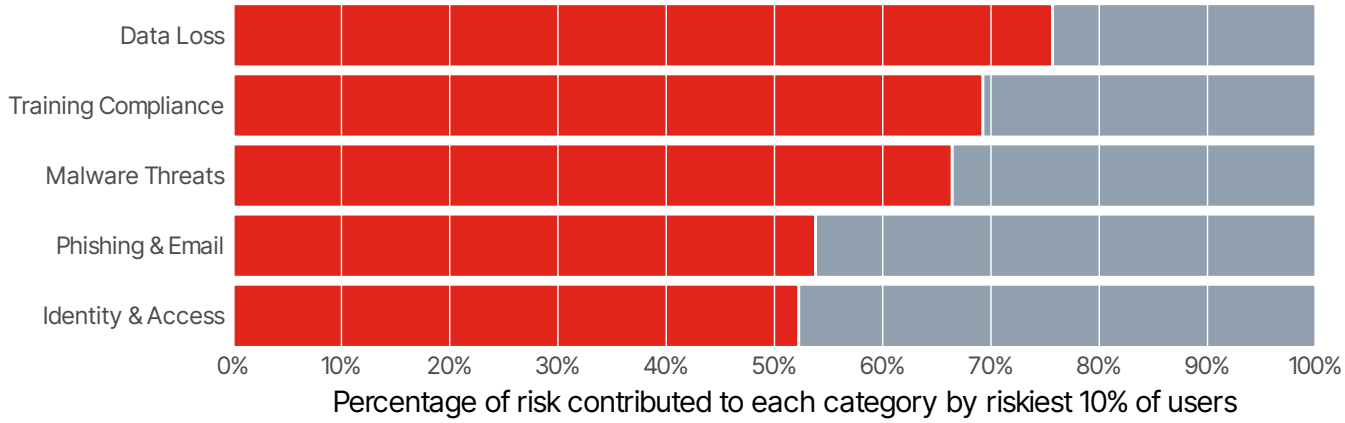


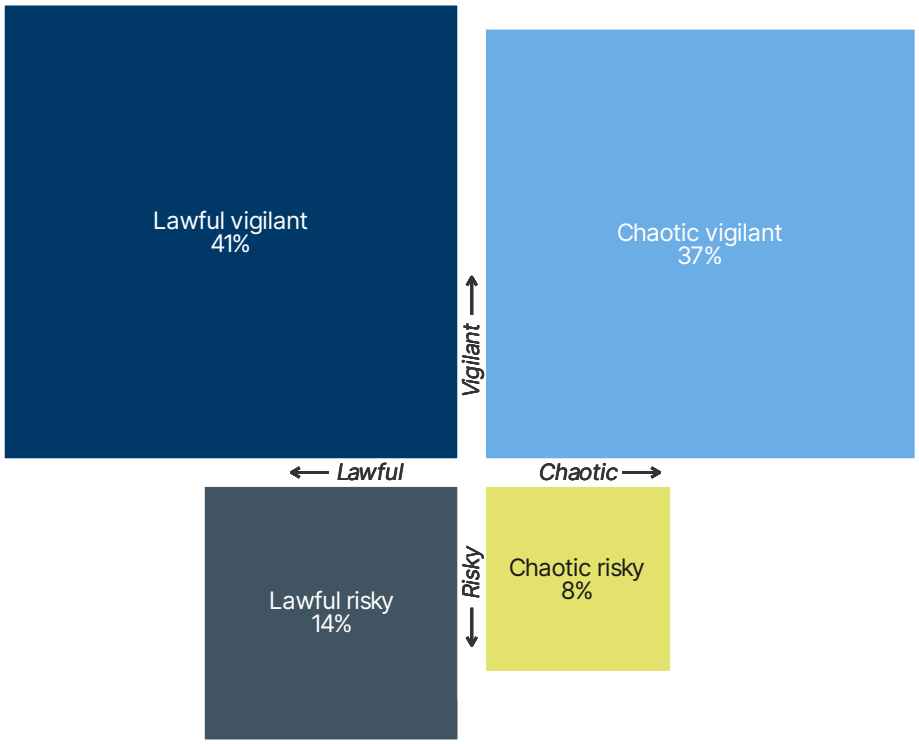
Figure 8: The contribution of the riskiest users varies among categories of human risk

Do users tend to be more risky or vigilant?

We've seen that certain employees contribute to more than their fair share of risk, but are there others out there whose actions serve to reduce exposure? To find out, we're going to ask you to venture with us into the realm of Dungeons & Dragons. Yep—you read that right. Get your D20 ready to roll.

As some of the more nerdy among you may know, characters in the D&D universe have an alignment along the dimensions of good vs. evil and law vs. chaos. Characters are generally required to act in a manner consistent with their alignment; straying too far usually incurs penalties. Do employees exhibit a similar form of alignment in terms of being more risky or vigilant, lawful or chaotic?

The chart below separates users into a simple 2×2 grid based on whether they generate more risky or vigilant insights, and whether the events and behaviors associated with them are repetitive/predictable ("lawful") or highly varied ("chaotic").



78% of users lower human risk more than they add to it (vigilant)

55% of users tend to do the same few things over and over (lawful)

8% of users are all over the place when it comes to risk exposure

Resulting In tailored strategies for each persona for more effective risk management

Figure 9: D&D-inspired breakdown of human risk alignment for users

The results of our D&D-inspired experiment into human risk alignment may surprise some. Almost 4 in 5 employees (78%) generate more vigilant than risky insights. That means the majority of your workforce is helping to reduce exposure more than adding to it!

Chaotic vigilant users are your security champions, engaging in a wide array of positive behaviors. Encourage them to continue and influence others. The lawful vigilant ones are getting the basics right. With a little help to expand their repertoire of vigilance, they could be champions too.

Of course, the alignment chart also indicates that 1 in 5 users is a net risk liability. The "lawful" 14% of risky users are, at least, somewhat predictable. They're routinely flagged for the same few risky insights. The silver lining is that they are good candidates for action plans targeted at those recurring issues.

The 8% of employees with a chaotic risky alignment are the ones who keep security leaders up at night. Their actions (and events involving them) expose the organization to a wide range of risks. Efforts to contain, train, and refocus them are definitely warranted to mitigate human risk.

IS THERE A "NEUTRAL" ALIGNMENT?

D&D fans may wonder why we don't follow the classic 3×3 alignment grid with a neutral option on both axes. That was a choice to simplify the message. But the reality is that about half of all users generate a roughly even mix of risky and vigilant insights and thus could warrant a neutral alignment. In fact, many users fluctuate between risky and vigilant over time (see Figure 14). That's good to keep in mind.

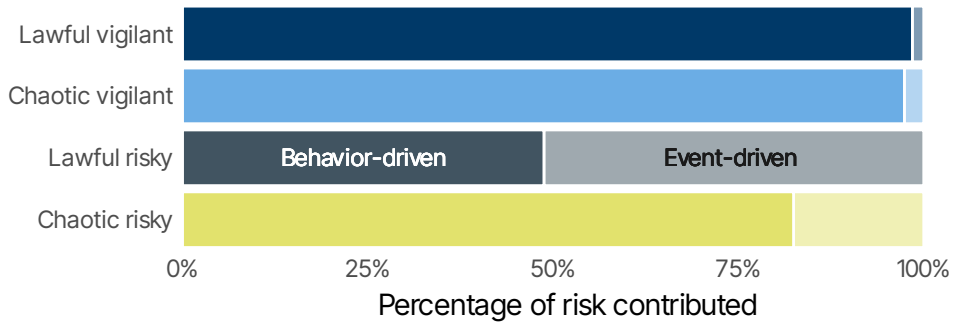


Figure 10: Behaviors vs. events in user alignment

At this point, you might be wondering what makes users more risky. Are they doing risky things (behaviors), or are risky things happening to them (events)? Understanding the difference is key to effectively tailoring strategies to manage human risk.

Figure 10 reveals the ratio of behaviors and events behind the four user alignments in the prior chart. Both vigilant classifications are almost entirely due to behavior. This supports the recommendation to empower and encourage these employees as security champions.

The alignment of risky users also reflects their behavior, but the higher proportion of events indicates that much of their risk profile is not their own doing. They're more targeted by threats, have higher levels of access, and aren't adequately protected, among other issues. This is why training alone can't effectively reduce risk. De-risking these users is much more than just a matter of correcting behavior.

What traits correlate with human risk?

Following the last section, you may be curious to know more about who makes up alignments like "chaotic risky" and "lawful vigilant." That's where the attribute category of risk insights comes in handy (see Figure 11).

Think of attributes as inherent user characteristics that add context about who they are, what access they have, etc. Some of these attributes are featured in the chart below, which gives a breakdown of risk alignments associated with each. It reveals some stark differences among user groups and may challenge some widely held assumptions about risk profiles.

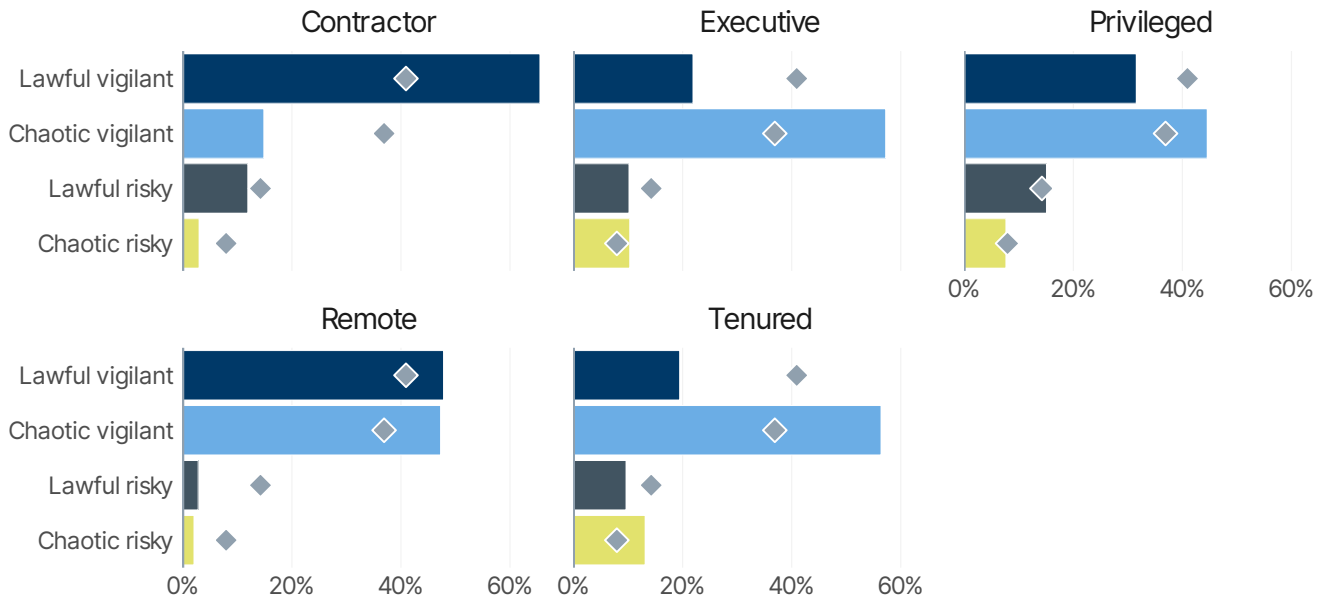


Figure 11: Comparison of user alignment profiles among employee attributes

Contractors and remote employees, often viewed as a security liability, are actually less risky and more vigilant than the overall average (which is indicated by the gray diamond). In the case of contractors, their tendency toward lawful vigilance may stem from policies such as requiring MFA for all access and mandatory training to maintain active status.

Executives and tenured employees show an abnormally high proportion of security champions (chaotic vigilant). That's an encouraging finding because such employees generally have high levels of influence across the organization. At the same time, the elevated ratio of chaotic risky users among them shouldn't be overlooked.

We can do a similar comparison along industry lines in Figure 12. It's clear that each sector has a unique profile when it comes to the breakdown of human risk alignments. The data used for this analysis is completely de-identified, so we can't contact them to inquire about internal factors that might be behind these profiles. But we can offer some hypotheses based on general knowledge about these sectors.

The Business Services category is fairly broad, encompassing legal services, holding companies, travel agencies, etc., so it's hard to ascribe shared tendencies to the whole lot. However, the fact that the chaotic risky alignment is higher in this sector than in any other suggests looser policies, controls, and risk visibility (see Figure 13 and callout).

The very high rate of lawful risky users in the Education sector isn't terribly surprising. EDUs are known for less centralized security controls and more open policies. It's not hard to see how users could repeatedly engage in the same few high-risk behaviors in such an environment.

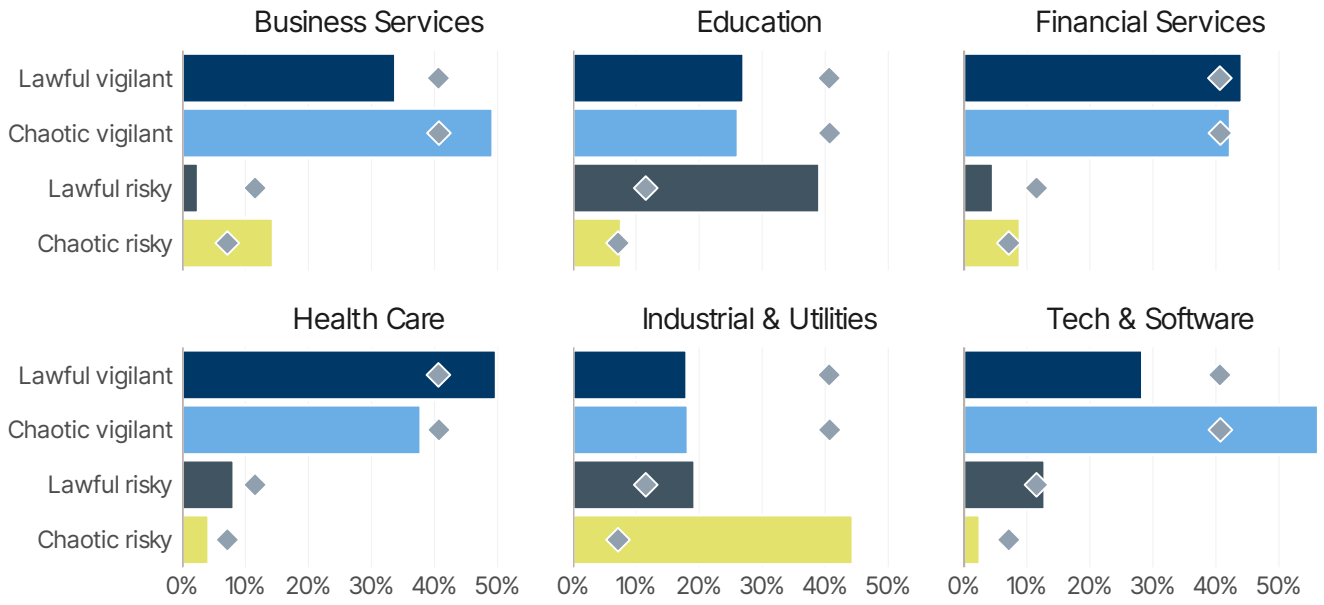


Figure 12: Comparison of user alignment profiles among industry groups

The Financial Services and Health Care sectors are traditionally highly regulated and tightly controlled. We'd hope to see fewer risky users and a higher degree of vigilance, which is generally what Figure 12 shows. The Tech & Software group shows a similar pattern.

RISK VISIBILITY CONTRIBUTIONS

Variation in risk visibility may contribute to the user alignment profiles observed among sectors in Figure 12; therefore, revisiting this topic here seems useful. The main standout is Business Services, with significantly lower visibility. It's also rather surprising to see Financial Services lower in the list, and perhaps even more so that Industrial & Utilities sits on top.

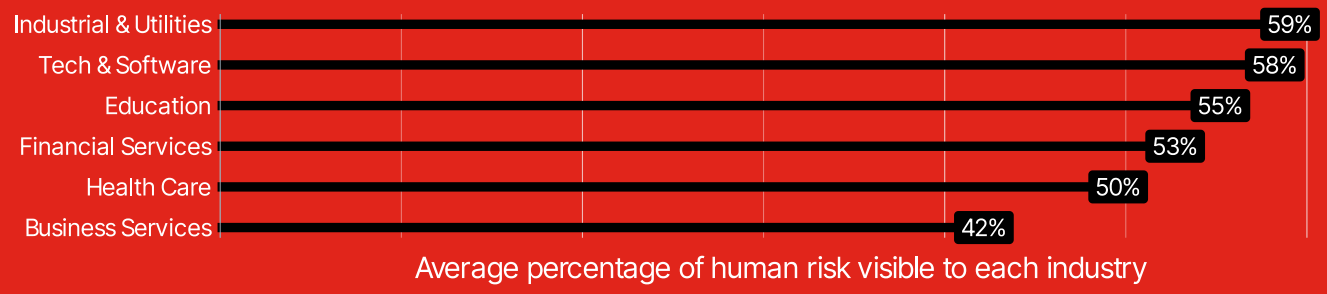


Figure 13: Human risk visibility is highest in Industrial & Utilities; lowest in Business Services

Can human risk actually be managed?

Everything covered thus far ultimately leads to this key question. Indeed, assessing and improving your visibility into human risk is an important step. It's helpful to know which types of risky behaviors and events are most common. Identifying your riskiest users—and budding security champions—is definitely worthwhile. But if nothing can be done to actually reduce human risk exposure for your organization, then the value of these insights is limited.

In this section, we'll prove it's not all for naught. We have solid evidence from many organizations that have seen their workforce become both less risky and more vigilant over time. That's a big claim, so let's look at the data.

The lighter lines in Figure 14 trend the percentage of users in each organization who are classified as more risky than vigilant over the last year. The shifting of those trendlines indicates that the human risk surface is far from static. Changes in the workforce, what they can access, the controls around them, and the external threat landscape all conspire to drive risk up and down over time.

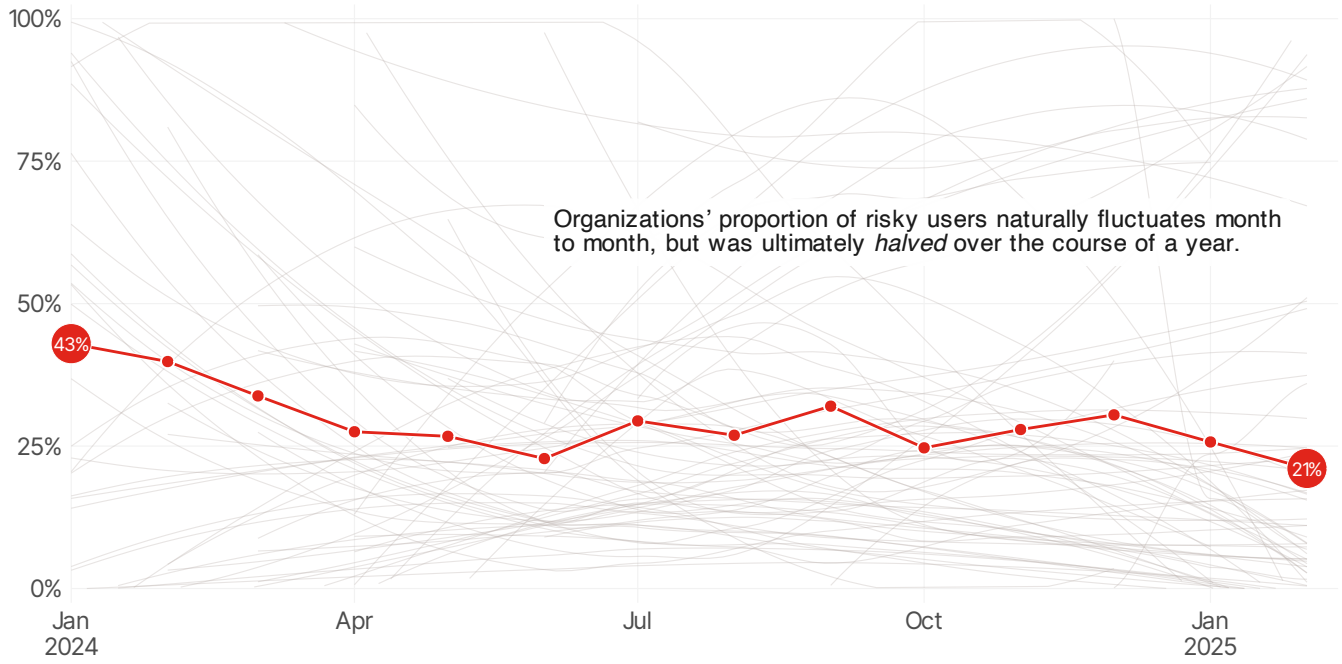


Figure 14: On average, the population of risky users in organizations dropped by half.

Amid the fluctuations for individual firms, the overall trend is one of decreasing risk. Organizations using Living Security's Unify platform saw their population of risky users drop by half over the last year (from 43% to 21%). And if that weren't enough, the ratio of vigilant users rose from 57% to 79%!

At this point, some may be wondering something like "Okay—but what's actually causing users to be less risky?" That's certainly the question we (Cyentia Institute) were asking when this finding emerged from our analysis. The Living Security team hypothesized that the risk-to-vigilance trend stems from action plans assigned to users to curb risky behavior. We're suckers for testing hypotheses, so we dove back into the data to see what it had to say.

Testing the efficacy of action plans requires that we not only establish a correlation between assigned plans and outcomes, but also link those together temporally. To do this, we compared the amount of time users spent in a risky state over a 90-day period before and immediately after completing action plans. This essentially measures the changing window of human risk exposure.

The results of these tests were quite convincing. Overall, we observed a 60% decrease in the amount of time users spent in a risky state. The change is most pronounced in the Training Compliance and Data Loss categories, resulting in a 98%+ reduction in exposure time. That's intuitive for Training and Compliance because once requirements are met, "at risk" status is lifted for a time (it's also a low rate to start with). The drop in Data Loss (which is not a low starting point) largely stems from curtailing unnecessary access or excessive permissions, which greatly reduces the propensity for exposure.

	% of days in risky state...[1]		
	Before action plan	After action plan	Decrease
Data Loss	23%	0.4%	98%
Identity & Access	4%	2%	51%
Malware Threats	4%	2%	54%
Phishing & Email	3%	1%	62%
Training Compliance	1%	0.007%	99%

[1] Recorded in the 90 days before and after the action plan.

Users spent an average of **60% less time** in a risky state after completing action plans.

Table 2: On average, action plans cut the window of user risk exposure by 60%.

Conclusion & Recommendations

This report reveals a clear and compelling reality: human cyber risk is measurable, unevenly distributed, and, most importantly, manageable. Across over 100 organizations and thousands of users, the data shows that just 10% of users are responsible for the vast majority of risky behavior—yet nearly 80% of employees are actually helping reduce risk more than they contribute to it.

HRM programs that move beyond basic training to incorporate real-time behavioral signals and broad integration streams gain significantly greater visibility—up to five times more than training alone. That visibility enables targeted, data-driven action plans that work: organizations using Living Security's Unify platform cut their risky user population in half and reduced time spent in a risky state by 60%.

The takeaway for security leaders is this: human risk isn't an intractable problem. With the right data, tools, and focus, it's possible to identify your riskiest users, empower your most vigilant ones, and drive real reductions in exposure.

The resources below have been curated to help you get started in that endeavor. On the next page, you'll also find recommendations from our experts for evaluating and building a successful HRM program.

RECOMMENDED RESOURCES

1. HRM Taxonomy[3]: A foundational tool that brings clarity and precision to human risk management by mapping observable user behaviors and exposures to real-world security threats. This resource helps you translate insight into action—enabling risk assessments, prioritization, and mitigation efforts that are aligned with leading frameworks like NIST CSF and Mitre Attack and tailored to your workforce.

2. How to Turn Human Risk Data into Actionable Intelligence: This guide explores how to contextualize human risk, integrate risk management strategies into daily operations across teams, and how to enhance security efficiency and resilience.

3. Forrester Wave™ for HRM: Evaluates nine HRM vendors and names Living Security a Leader, highlighting our advanced, data-driven approaches to human-centric risk scoring and real-time behavioral interventions.

4. HRM Buyers Guide: The Human Risk Management Buyer's Guide highlights three key areas and associated elements every robust Human Risk Management platform must have.

5. Human Risk Management Maturity Model: The new approach in changing human behaviors to protect organizations from cyber threats.

6. Risk Quantification in Human Risk Management: Explore how Living Security's Unify platform quantifies human cybersecurity risks by analyzing user behaviors and providing actionable insights to mitigate vulnerabilities.

[3] Comming Soon!

Recommended Next Steps for Evaluating HRM Programs

Whether you're just starting your human risk management journey or looking to evolve a mature program, the following steps can help your organization evaluate and enhance its approach:

- **CONDUCT A HUMAN RISK ASSESSMENT:** Begin by measuring your current visibility into human risk. How many risk signals can you detect today? Are you relying solely on SAT, or have you integrated additional data streams?

- **IDENTIFY HIGH-IMPACT RISK SIGNALS:** Focus on behaviors and events that most strongly correlate with breaches or incidents. Target categories like identity & access and data loss first for measurable impact

- **SEGMENT AND PRIORITIZE USER GROUPS:** Not all users pose an equal risk. Segment your workforce to identify top contributors to risk (the riskiest 10%) and recognize security champions (vigilant users). Tailor interventions accordingly.

- **DEFINE AND LAUNCH ACTION PLANS:** Develop and implement targeted interventions for at-risk users. These should include both behavioral nudges and technical controls and be informed by real-time insights.

- **MEASURE CHANGE AND ITERATE:** Track shifts in user alignment and time spent in risky states to quantify improvement. Use these metrics to refine your strategy and demonstrate ROI to stakeholders.

- **BENCHMARK AGAINST INDUSTRY PEERS:** Use the data in this report to compare your organization's performance with that of peers across industries and employee segments. Pay close attention to your risk distribution and visibility gaps.

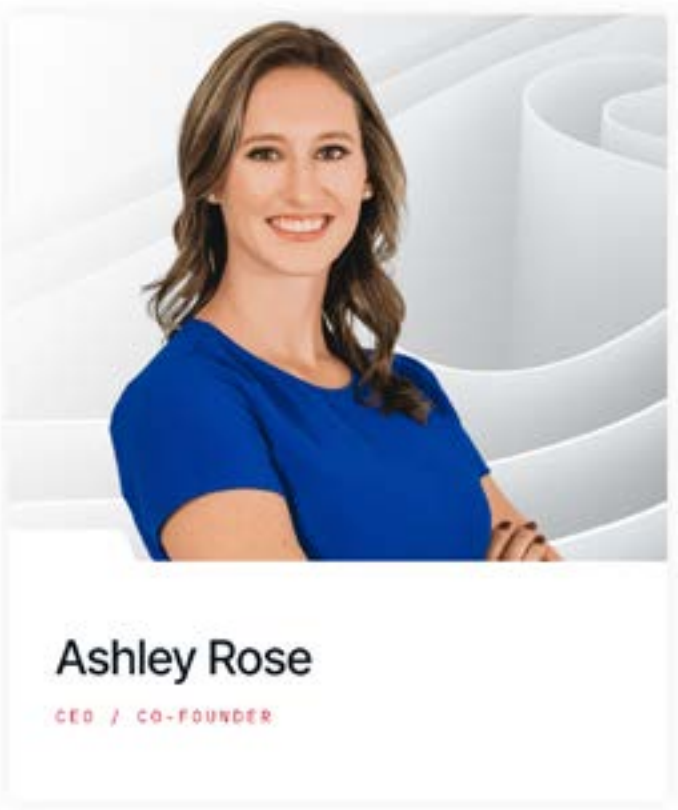
- **ALIGN WITH A STRATEGIC HRM PARTNER:** Consider working with a trusted platform like Living Security, which has demonstrated success in reducing human risk through visibility, analytics, and behavior change at scale.

A View to the Future

Over the past five years, the security industry has made meaningful, measurable strides in reducing human cyber risk. Through behavioral insights, adaptive training, and targeted interventions, organizations have turned the so-called "weakest link" into a strength. The data in this report demonstrates how Human Risk Management (HRM) is delivering tangible ROI—and transforming enterprise resilience from the inside out.

➤ BUT THE HUMAN WORKFORCE IS NO LONGER ALONE.

A new class of digital worker—autonomous, adaptive, and non-deterministic agents—is emerging across enterprises. These agents don't just support employees; they act on their behalf, make independent decisions, and operate at machine speed. In doing so, they expand the workforce—and the attack surface—exponentially.



While agents promise immense operational value, they also introduce the same kinds of behavioral risk we've spent years learning to mitigate in people: overreach, data exposure, shadow access, and policy violations. These agents behave less like software—and more like humans.

As pioneers of Human Risk Management, Living Security is uniquely positioned to apply the same governance principles to this new digital workforce. We envision a future where enterprises manage risk across a blended workforce of humans and agents with shared frameworks, shared visibility, and shared accountability.

This report celebrates the progress we've made on the human side. And it signals the beginning of what comes next. The future of cyber resilience isn't just about managing human risk—it's about managing behavioral risk, everywhere it originates.

➤ MORE TO COME.

livingsecurity

Living Security is the global leader in Human Risk Management (HRM), providing a risk-informed approach that meets organizations where they are—whether that's starting with AI-based phishing simulations, intelligent behavior-based training, or implementing a full HRM strategy that correlates behavior, identity, and threat data streams.

Living Security's Unify platform delivers 5X more visibility into human risk than traditional, compliance-based training platforms by eliminating siloed data and integrating across the security ecosystem. The platform pinpoints the 10% of users who pose the greatest risk and automates targeted interventions in real time—reducing exposure to human risk by over 90%. Powered by AI, human analysis, and industry-wide threat telemetry, Unify transforms fragmented signals into intelligent, adaptive defense.

Named a Global Leader in Human Risk Management by Forrester and trusted by enterprises like Unilever, Mastercard, Merck, and Abbott Labs, Living Security helps security teams move from awareness to action—driving measurable behavior change and proving impact at every stage of the journey.

Because when security teams can see clearly and act precisely, they can finally stay ahead of tomorrow's threats.

119 Cyentia INSTITUTE

The Cyentia Institute is a widely respected research and data science firm, working to advance cybersecurity knowledge and practice. We accomplish that goal by collaborating with security companies to publish data-driven reports like this one and through analytic services that help organizations manage cyber risk.