Culture AI

Time to Adapt:
The State of Human Risk Management in 2024

www.culture.ai

CultureAI commissioned Opinion Matters to survey 200 UK-based SOC and cyber security teams at organisations with 1000+ employees within FinTech, Tech, Oil & Gas, Law, Finance, and Logistics about their approach to managing human risk.

This research was carried out independently and seeks to unpack how far training can go in improving behaviours and reducing risks, evaluating whether investments of time and money offer substantial returns or if resources could be better spent elsewhere.

Definitions

We define Security Awareness and Training (SA&T) as:

A company-wide programme aiming to educate employees on cyber security threats and practices. The success of which is measured through training completion rates, content engagement, and assessments. It can be implemented for various reasons, including compliance and insurance requirements.

We define Human Risk Management (HRM) solutions as encompassing the following functions:

1. **Monitor:** Analyses real-time data to identify risky or positive employee security behaviour.
2. **Reduce:** Utilises teachable moments for timely, targeted coaching to prevent reoccurrence of risk.
3. **Fix:** Secures the organisation through strategic, automated interventions and nudges which resolve the identified risk as quickly as possible.

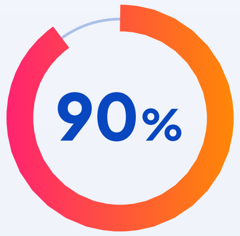
Table of contents

People make mistakes

It's to be expected; to err is human. But that doesn't make the implications of these errors any less catastrophic. Just one click on a malicious email can be all it takes to give hackers access to sensitive data, leaving it vulnerable to exploitation.

The average ransomware payment is a staggering **$2.2 million,** while the typical BEC attack costs an organisation **$125,000[1,2].** However, the repercussions extend far beyond financial losses. A data breach can severely damage a company's reputation and erode customer trust. A staggering 66% of consumers admit they would not trust a company that suffers a data breach[3].

Forrester predicts that:

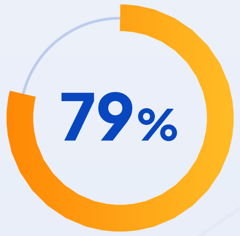


of data breaches will include a **human element in 2024[4]**

Making this the **top cyber security risk** for organisations

This is the new normal

Employees face an increasing range and volume of risks as they go about their daily tasks; with the widespread adoption of SaaS, GenAI, and collaboration tools opening more vulnerabilities for cyber criminals to exploit.



of companies we surveyed reported a human-related data breach in the **last 12 months**

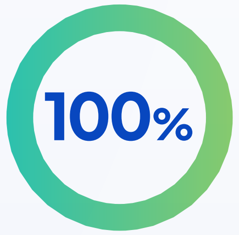
To counter this, companies are pouring more and more resources into their cyber security programmes hoping to improve their security posture and protect their key assets.

Yet, breaches are still happening at an alarming rate. In order for companies to strengthen their defences they need to turn more attention to **quantifying and managing human risk.**

But, how should they do this? Many organisations have invested heavily in security awareness and training (SA&T) programmes, aiming to shift employee behaviours and prevent breaches. **Yet, is sporadic, compliance-driven training truly effective?**

Realistically, with the constant emergence of new threats and vulnerabilities, expecting employees to constantly be on the lookout for threats isn't a feasible solution.

Even the most well-trained employees occasionally make mistakes, and malicious actors will always be ready to exploit these errors.

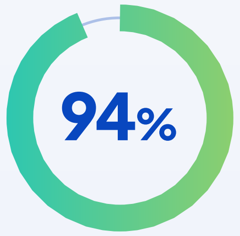


of organisations are carrying out some form of SA&T

How can we better tackle the issue at hand?

As the threat landscape evolves, so must defences. Organisations must take a proactive approach, embracing innovative interventions and technologies. To outpace threat actors, companies need to be adopting an adaptive, data-driven approach to human risk management.

The good news? A significant number of companies are beginning to and are seeing positive results.



of organisations have adopted one or more HRM capability

Key areas of exploration for this report include:

- **Evaluating the value of security awareness and training:** Is it worth the investment, and can a positive return on investment (ROI) be achieved? Does SA&T effectively meet its objectives in enhancing security practices?
- **Understanding human risk management:** What role does HRM play in strengthening organisational security, and how can it be effectively integrated into existing security frameworks?

Evaluating the value of Security Awareness and Training (SA&T)

What are organisations hoping to achieve with SA&T?

The SA&T market has historically been driven by compliance demands, but here's the issue: treating it as just a box-checking exercise typically means putting in minimum effort. And relying on regulatory compliance alone won't truly secure your company.

However, a shift in attitudes is emerging.

According to those surveyed, their primary motivation for providing training today is:

51% to change behaviours and equip employees to handle any risks

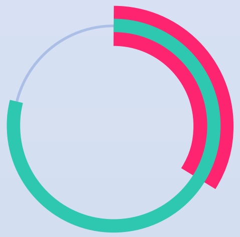
25% for compliance reasons

24% to prevent breaches

The results show that security teams are increasingly striving to exceed minimum requirements. However for those seeking to engage employees and improve behaviours, there are unfortunately few examples of what good looks like. Organisations eager to do better often default to more training, unsure of alternative solutions.

But is this the best approach? Whether training aims to change behaviours or prevent breaches, the stark reality is:

79% of organisations suffered cyber breaches due to **human error**



with **34%** experiencing **multiple breaches**

This trend aligns with global data, like the Verizon Data Breach Investigations Report, which found that in 2024, **68% of breaches involved a non-malicious human factor,** such as falling victim to social engineering or making errors[5].

While Gartner reported that **69% of employees admitted to intentionally ignoring or bypassing their company's cyber security guidelines,** regardless of training[6].

All of this data underscores a significant issue: while organisations strive to equip employees to manage risks, transform behaviours, and prevent breaches, **training alone falls far short of these high expectations.**

SA&T: Investment vs reality

Implementing a security and awareness training programme is a time-consuming commitment.

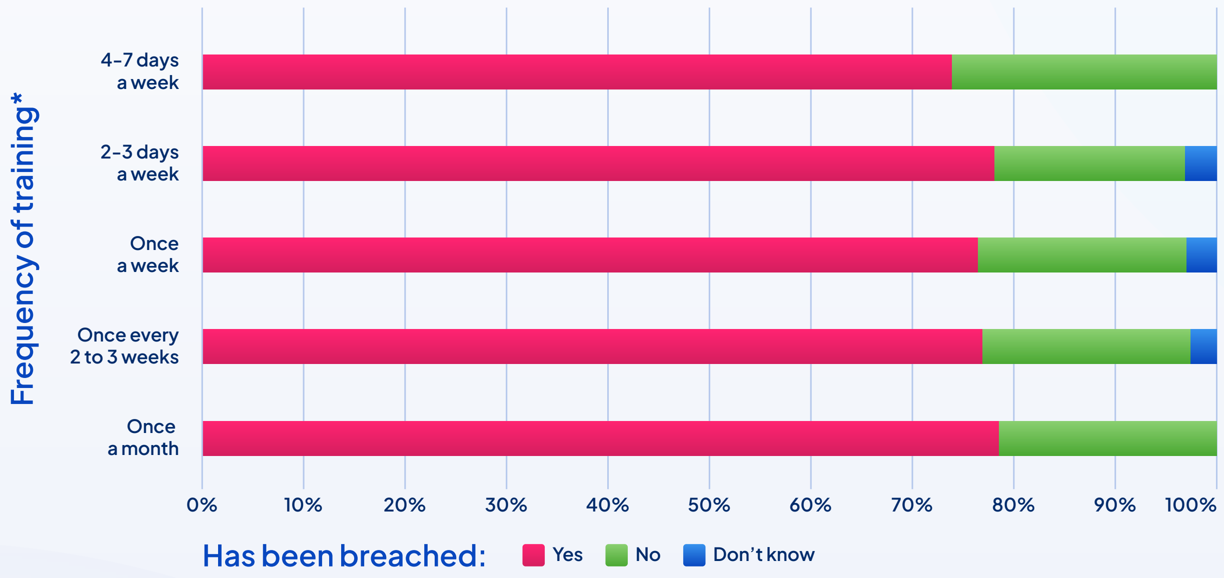
78% of our respondents conduct employee training **at least monthly**

with **45%** doing so **weekly or more**

Unfortunately, despite these efforts, human-related breaches remain prevalent. **The research suggests that the frequency of training does not strongly correlate with breach prevention.**

Regardless of whether organisations conducted training twice a week or once a month, 79% reported experiencing at least one breach.

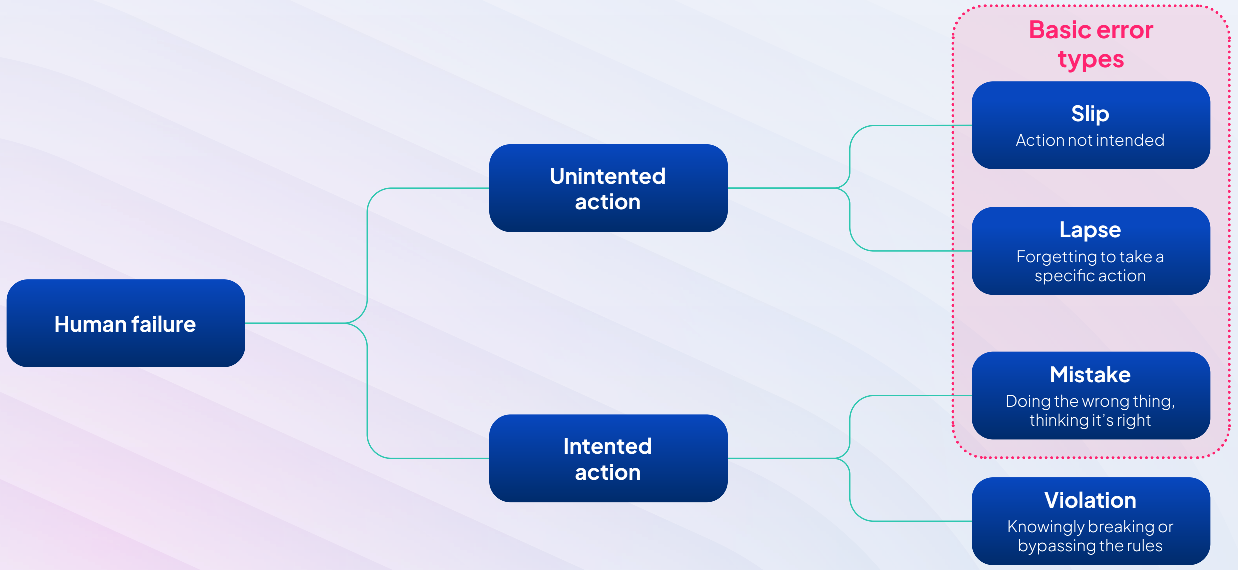
While the frequency of training suggests a significant time investment and is higher than we expected, the incidence of breaches due to human error suggests that this investment is not effectively aiding employees in managing risks or preventing breaches.



This fits well with James Reason's model of human error (see below), which suggests that while training can address mistakes, it has a limited impact on slips and lapses — the errors cyber criminals often exploit[7].

These criminals target System 1 thinking — a fast, automatic, and unconscious way of thinking — knowing that people frequently default to it, even after training.

As a result, the training has little impact on addressing risk.


Human failure
Unintented action
Intented action
Basic error types
Slip
Action not intended
Lapse
Forgetting to take a specific action
Mistake
Doing the wrong thing, thinking it's right
Violation
Knowingly breaking or bypassing the rules

* Combines options '4–6 days a week and Every day.'

The conclusion? Beyond a certain point, further training becomes unproductive, especially when it requires a time commitment from employees who already exhibit positive security behaviours. It also may be that only a small fraction of the workforce is contributing to most of the risk.

Wouldn't it be more effective to identify these high-risk employees and implement technical interventions, and free up the security team's time for more strategic projects?

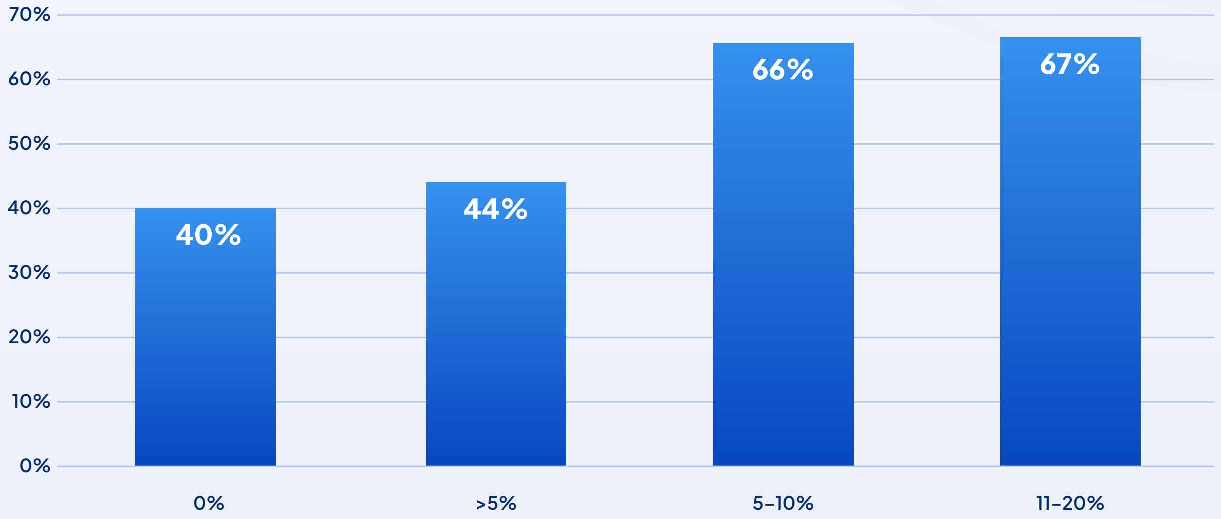
Overspending, underdelivering?

Time isn't the only resource being spent; financial investments are also being made. **63% of respondents currently spend 5% to 10% of their security budget on training with another 33% reporting that they spend 11% to 20%.**

This is more than we anticipated, as in 2023 Gartner reported 60% of teams spend 5% or less on awareness activities (people, processes, and technology all included)[6].

Although these figures may seem modest compared to technology spending, the increase is signalling a desire to spend more on human-focused solutions.

Perceived effectiveness of training by SA&T budget



Among those spending 11% to 20% on training, **80% experienced a security breach in the past year.** This suggests that allocating up to 20% of the budget to training alone could be a missed opportunity, especially as increased spending shows only marginal gains.

While training has a place, it has its limits. Instead of sinking funds into single-focus platforms, why not embrace a comprehensive approach to human risk management? Enabling the identification of key workplace risks and the ability to tackle them head-on.

In a time of tight security budgets and scrutiny, consolidating platforms and functionalities can streamline resources and increase efficiencies.

Training is effective… isn't it?

It's clear that a lot of time and effort is spent on security awareness training — 96% of respondents allocate between 5% to 20% of their security budgets to security training. And 78% trained at least monthly.

Given this investment, it is encouraging to see that 70% of organisations consider their training somewhat or very effective. However, this average does conceal significant variations across sectors. For instance, 84% of finance firms rated their training as somewhat or very effective, whereas only 56% of law firms reported the same level of satisfaction.

The higher rating from finance firms may be attributed to more stringent cyber security regulations placed on the industry, such as the GDPR, PCI-DSS, NIS2 Directive, and specific FCA mandates. These regulations heightened threat awareness and ensured preventive measures were implemented.

Consequently, finance firms, which typically receive more cyber attacks than most other industries, gained valuable insights into effective practices and adapted their approach for maximum effectiveness[8].

We asked "How effective do you think your training is?"

7%	24%	36%	34%
Not effective at all	Not very effective	Somewhat effective	Very effective

Delving into the various job roles also turns the spotlight onto a few key differences in how they view the effectiveness of the training. Surprisingly, it's the security awareness professionals — those usually tasked with implementing SA&T programmes — who often feel the training falls short.

Only 18% consider their training highly effective, while 78% rate it as either not very effective or only somewhat effective. This perception might be due to security awareness professionals setting higher expectations for the training they offer.

The SANS 2024 Security Awareness Report sought to understand the challenges that security awareness professionals were contending with when building and managing an effective security awareness programme[9].

According to SANS[9], security awareness professionals identify their primary challenges as:

41%	37%	29%
Lack of time	Staff shortages	Lack of budget

Security awareness professionals are expected to deliver results, often with limited resources. Many spend significant time on manual training and reporting, but automation can help move the needle.

Utilising just-in-time training and real-time data visualisation can significantly boost efficiency and impact. By adopting automated tools for coaching, phishing simulations, and interventions, security teams can also streamline their operations, ultimately saving valuable time.

High engagement does not guarantee behaviour change or risk reduction

Against this backdrop, we question why organisations label their security awareness training as "very effective" if those responsible for it doubt its efficacy. A deeper examination of the research shows a significant link between perceived effectiveness and employee engagement. Among those who consider their training highly effective, 82% report positive employee engagement.

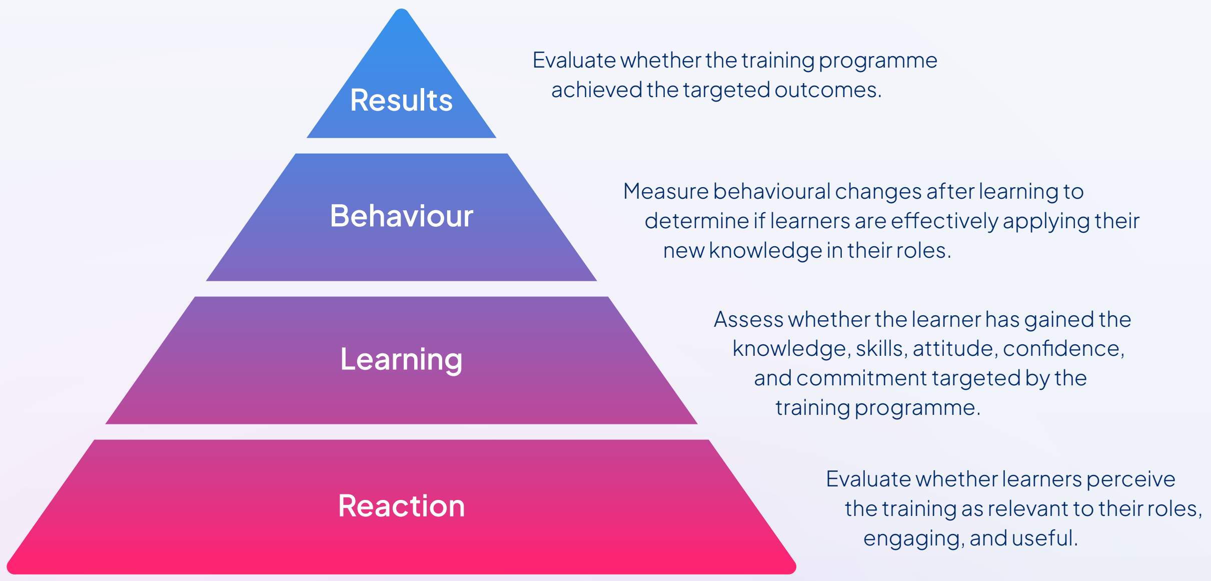
This is expected, as **training success is frequently gauged by completion and engagement rates rather than actual behavioural change.** Gartner reports that only 43% of awareness programmes consistently measure employee behaviour, and 10% never do[6].

But how to evaluate?

The Kirkpatrick model (see below) for evaluating training suggests that there are four ways to evaluate training, increasing in effectiveness and therefore return on investment[10]. The lowest is Reaction — how did the training make the trainees feel? That's usually where engagement is measured.

Far more usefully, the levels above look at Learning, Behaviour, and ultimately Results. Engagement may be important, but without consistent learning or behaviour change, is it valuable?

Kirkpatrick evaluation model


Results
Evaluate whether the training programme achieved the targeted outcomes.
Behaviour
Measure behavioural changes after learning to determine if learners are effectively applying their new knowledge in their roles.
Learning
Assess whether the learner has gained the knowledge, skills, attitude, confidence, and commitment targeted by the training programme.
Reaction
Evaluate whether learners perceive the training as relevant to their roles, engaging, and useful.

Digging deeper into the segment that rates their training as 'very effective' uncovers an interesting pattern:

of these organisations **experienced breaches in the past 12 months**

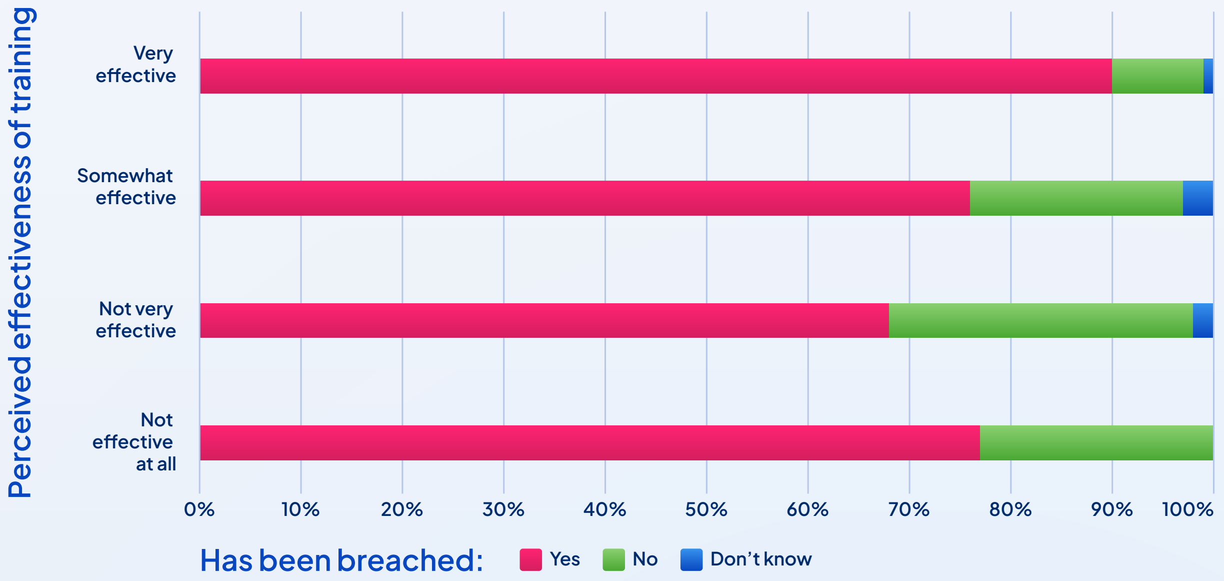
This highlights that while training and testing can boost employee engagement and knowledge acquisition, **it doesn't tackle the issue that is on top of so many security teams' priority list: human-related data breaches.**

The true measure of effectiveness needs to be the outcomes, not the activity itself. It's essential to measure success by results rather than mere participation.

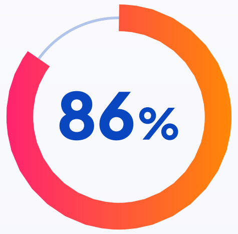
To accurately assess these outcomes, organisations need real-time visibility into employee security behaviours.

Are employees reusing passwords, logging into unapproved software, or oversharing sensitive data in platforms like ChatGPT? How does this change over time when targeted coaching and interventions are introduced?

Perceived effectiveness vs breaches



Customised training: Not quite hitting the mark



of respondents say their training is either fully or partly customised to their needs

Despite the costs and considerable effort required to develop such programmes, **there is no significant difference in perceived effectiveness based on the level of customisation.**

Among those providing generic training, **72% said it was somewhat or very effective.** For those using customised training, **70% reported similar effectiveness.**

This begs the question: is investing in customisation truly worthwhile?

The answer? It depends. We believe there is an important distinction between “customised” and “targeted”. Customised training programmes are often tailored to the needs of an organisation, modifying the content, delivery methods, or assessment techniques.

Whereas targeted coaching aims to address specific vulnerabilities within an organisation by leveraging behavioural data and advanced analytics.

This approach quantifies risks and provides clear, actionable insights directly to individuals at the point of risk — precisely when they need it most.

By prioritising efficiency and precision and concentrating resources on the most critical areas where improvement is needed, this type of targeted coaching can be effective. **But it is still only one piece of the puzzle.**

Understanding Human Risk Management (HRM)

A shift in mindset

Human risk management (HRM) has become a more established category in recent years, representing a much needed change.

A shift in mindset, process, and technology that aims to overcome the critical shortcomings of SA&T. The overarching goal? To enable security teams to more effectively quantify and manage human risk.

This approach enables organisations to understand the real-world risks caused by and affecting humans; implementing the necessary interventions to counter these risks.

While companies may continue to implement SA&T training to satisfy regulatory requirements, they will see more significant impact on their overall risk profile by taking a HRM approach. Cyber criminals are continually embracing new tools and tactics, so it’s imperative companies do the same.

HRM helps businesses get increased value from their current security and technology tools as it leverages data from multiple platforms and helps security professionals remediate and take action off the back of this knowledge.

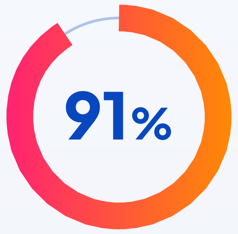
> “Our human risk management platform aims to provide a single source of truth for employee behaviour, offering access to real-time metrics and data from a variety of sources.
>
> Enabling us to identify weaknesses and address risks with targeted coaching and interventions. We had no visibility of these risks before utilising a HRM platform.”
>
> — **Security GRC Manager, Technology organisation**

Companies are driving down risk with HRM

When asked about HRM, companies are beginning to use some techniques to drive down risk. However, while 94% of organisations were using at least one HRM capability, there is still room for growth, as only 22% of respondents were using three or more different capabilities.

There is a notable correlation between the number of HRM solutions utilised and the incidence of human factors-related breaches over the past year.

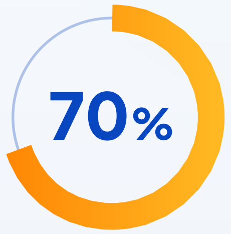
Specifically:



of organisations with **only one capability** experienced a breach

VS

organisations utilising **four capabilities**



While total risk elimination is impossible, it is reasonable to expect a further reduction in risk with the addition of more solutions.

Upon examining the respondents who reported no data breaches, we discovered a preference for more technical HRM functionalities.

The most popular choices were:

45%	37%	37%	32%
Human risk triage	Coaching based on risk level	Nudges triggered by risk	Automated interventions

A further benefit of HRM solutions is that they can also deliver quick time-to-value, leveraging data from internal communication tools, secure email gateways, authentication systems, and cloud storage platforms to provide enhanced insights.

By anlaysing and correlating this behavioural data, HRM platforms offer real-time visibility into a wide range of risks and automate risk response. While automated coaching workflows can be configured in advance and require minimal ongoing attention, allowing security teams to focus on strategic priorities.

> “We were using a well-known security awareness training platform, but it required significant administrative effort for setup, management, and monitoring each month. We spent an entire week setting up the platform.
>
> By contrast we set up a human risk management platform in two hours, with only a couple more days to configure automations and interventions.”
>
> — **Head of IT, Professional services organisation**

It’s an evolution, not a revolution

The evolution towards comprehensive HRM is underway, aligning with **Gartner’s forecast that 80% of enterprises will have established HRM programmes by 2030[11].** While this shift won’t happen overnight, the momentum is undeniable.

The challenge can lie in knowing where to start; however, organisations are already integrating HRM elements, often without explicitly labeling them as such. Encouragingly, those who have embarked on this journey are witnessing tangible benefits.

An effective HRM platform should offer a comprehensive 360° view of employee-related risks, pinpointing their locations, and analysing the behaviours that cause them.

It should empower organisations to prioritise their focus and equip them with the tools to swiftly and effectively mitigate these risks. Furthermore, it should leverage real-time teachable moments for employees to prevent the recurrence of risks.

By embracing these strategies, organisations can not only meet the predicted shift but exceed it, cultivating a more resilient and security-conscious culture.

Top takeaways

Human risk needs to be taken seriously

Human risk continues to be a major vulnerability for most organisations. To tackle this issue, businesses need to be focusing their attention on more adaptive forms of human risk management. This strategy helps identify employees exhibiting the riskiest behaviours and provides targeted coaching and interventions at the point of risk.

Don't overinvest in training

Adopting a HRM approach doesn't mean organisations need to give up on training altogether, especially if it is required for compliance purposes. That said, it is crucial not to overinvest in refining these programmes. Our research shows that extra time, resources, and customisation do not deliver the results hoped for. It's key to understand the limits of training.

SA&T isn't going to stop breaches

While can be useful in helping employees pick up the basics, and many of the organisations surveyed deemed it 'effective'. It's not alleviating the risk of breaches. 79% of surveyed organisations reported a human-related data breach in the last 12 months, even though 100% reported undertaking security awareness training.

Plan for slips and lapses, not just mistakes

Training addresses gaps in education and knowledge, but cyber criminals exploit gaps in attention and perception to achieve their goals. Effective use of technical interventions and psychological nudges can help close those gaps.

Technology needs to protect people

Not the other way around. Real-time detection of risky employees behaviours is crucial. Securing the organisation with technical interventions and leveraging real-time teachable moments can prevent future occurrences. This approach reduces the burden on employees to be equipped to handle any risk.

References

1. Sophos. (2024). *The State of Ransomware 2024.*
2. FBI IC3. (2023). *FBI Internet Crime Report 2023.*
3. Security Magazine. (2024). *66% of consumers would not trust a company following data breach.*
4. Forrester. (2024). *The future is now, introducing human risk management.*
5. Verizon. (2024). *2024 Verizon Breach Investigations Report.*
6. Gartner. (2023). *Security Awareness Efforts Fall Short! Now What?*
7. Reason, J. (1990). *Human Error.* Cambridge: Cambridge University Press.
8. Stiftung Wissenschaft und Politik. (2024). *European Repository of Cyber Incidents (EuRepoC).*
9. SANS. (2023). *SANS 2023 Security Awareness Report: Managing Human Risk.*
10. Kirkpatrick, D. L. (1959). *Techniques for Evaluation Training Programs.* Journal of the American Society of Training Directors, 13, 21-26.
11. Gartner. (2023). *Eight cyber security predictions for 2023–2024.*

Want to carry on the conversation?

As we transition to a new era and beyond, the landscape of human risk management continues to evolve, bringing new challenges and opportunities.

We invite you to dive deeper into these findings with our team of experts and explore how these cutting-edge strategies can transform your organisation's approach to risk.

Get in touch

About CultureAI

The innovative CultureAI Human Risk Management Platform empowers security teams to instantly identify workforce security risks, coach employees in the moment, and automate fixes.

Whether organisations want to enhance resilience against phishing, improve SaaS security, reduce data loss through generative AI, or ensure compliance with personalised security coaching. CultureAI's comprehensive platform encompasses multiple solutions which enables businesses to effectively and efficiently quantify and manage the risks caused by and affecting humans.

Trusted by leading organisations globally, CultureAI is a UK-based company with offices in Manchester and London.

About Opinion Matters

Opinion Matters is an award-winning insight agency. Their consultants create bespoke market research solutions for businesses, organisations, and agencies worldwide. They are experts in creating concepts, implementing and managing projects, analysing results and reporting.
The agency operates internationally, offering highly targeted niche panels that are more pertinent to specialist audiences and media requirements.

Opinion Matters abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Opinion Matters is also a member of the British Polling Council.

The research was conducted by Opinion Matters, among a sample of 200 18+ SOC and cyber security teams at organisations with 1,000+ employees.

Sectors: FinTech, Tech, Oil & Gas, Law, Finance, and Logistics.

The data was collected between **18.07.24–24.07.24.**

Opinion Matters abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Opinion Matters is also a member of the British Polling Council.

Learn more at

www.culture.ai