



Cyber Resilience in 2025:

Futureproofing AI Adoption

CONTENTS

3

Foreword from Rob Demain,
CEO, e2e-assure

4

Introduction

5

AI: The Achilles' Heel of Cyber Resilience?

6

The Truth about Human Error

8

Empowering Employees to Build
Collective Resilience

9


Understanding the Wider Tension

10

Tackling the Problem in 2025

13

Talk to us



In this year's independent research, e2e-assure has investigated the cyber resilience landscape in the UK and drilled down into how AI is set to impact UK businesses' cyber defences. We've widened the net to understand the frustrations of not only cyber risk owners when it comes to cyber security, but also general workers. The intention? To see where there's discrepancies when it comes to perception and understanding, and where the priorities lie for both parties.

We're glad we did, especially knowing now that the majority (73%) of cyber risk owners agree that most cyber attacks come from a lack of employee diligence.

What's clear is that the fragmentation of technology, which encompasses this year's stratospheric rise of AI, hasn't helped when it comes to building cyber resilience. In fact, AI could be about to unravel everything that's been so hard fought for, putting UK businesses at risk.

The threat of AI comes from all types of threat actors – including state and non-state, skilled and less skilled – who are, according to a [National Cyber Security Centre report](#), already using it to varying degrees. But, as this report reveals, the adoption of AI from those inside your organisation is a disaster building in the shadows. The reasons for this are more complex than just poor diligence. They stem from a worrying misalignment.

This might feel like another roadblock in the endless pursuit of cyber resilience. Encouragingly, our new research does reflect that positive headway has been made. Last year, e2e-assure surveyed 500 CISOs and cyber security decision makers (cyber risk owners) across multiple sectors, to understand their frustrations when it came to cyber security, and how resilient they were feeling. The majority (61%) described themselves as only 'somewhat resilient'. This year, we can see that those who have made investments in strong processes, technology and training, report feeling far more resilient. But more on that later.

This report also reveals where the gaps are in employee knowledge, even when investments have been made, so cyber risk owners can maintain a positive trajectory.

With so much in the balance, it's important that cyber risk owners understand that although they must be in control, navigating new challenges is a collective responsibility. Building resilience must be holistic, built from the ground up and with the right assistance.

Research Methodology

The research was conducted by Censuswide in two parts. Part A was among a sample of 1,000 General Office Workers in the UK. The data was collected between 7.08.2024-15.08.2024. Part B was among a sample of 503 UK CISOs/ IT Security Decision makers (50/50 split) with at least 50% from businesses with 500-2500 emps (18+). The data was collected between 06.08.2024 - 16.08.2024. Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Censuswide is also a member of the British Polling Council.



Rob Demain
CEO @ e2e-assure

INTRODUCTION

Cyber incidents are now the number one threat to businesses in the UK. e2e-assure's latest independent research has found that 90% of cyber risk owners, from SMEs to enterprises, have experienced a cyber attack. This is up 15% compared to when we asked the same question last year.

90%

of cyber risk owners said they worked at an organisation that had experienced a cyber attack, compared to 75% last year

Organisations are improving resilience

Cyber resilience has risen to the top agenda item for most cyber risk owners (49%), shooting up from 36% last year. It has overtaken speed, which remains at 43% like last year, followed by control (33%) and cost (30%).

Cyber risk owners have made positive changes to improve their resilience in the last 12 months with 29% of organisations confident that they are resilient, up 7% on last year.

It's also encouraging to see that cyber risk owners are happier with the provision of their cyber security. 26% said their in-house team or provider was 'exceeding their expectations' (up from 17% last year), over half (54%) said their cyber security was 'ok – but there was room for improvement' (up from 42% last year), and 17% said it was 'underperforming and they were looking to make changes'.

Where have organisations invested?

Our data indicates that individuals who regard themselves as resilient have invested more in robust processes, technology, and training compared to those who do not. The biggest impact has been made through a combination of human and technology investments such as training (+18%), clearer

communication paths (+16%) and implementing Managed Threat Protection (+13%).

While organisations have continued to use a variety of operating models to protect their most valuable assets, we have seen a significant increase in those utilising Managed Threat Detection (48% up from 33% last year).

- 48% use Managed Threat Detection services, 39% use an outsourced SOC provider, 36% have their own SOC in-house, and a further 38% then work with an MSSP to augment their in-house SOC provision.

Worker AI usage of at least once per week across sectors:

49% of 'resilient' respondents have invested in Managed Threat Protection from their vendor vs 36% 'not resilient'

49% 36%

39% of 'resilient' respondents have invested in an MSSP to augment their inhouse SOC versus 29% 'not resilient'

39% 29%

40% of 'resilient' respondents have invested in training, versus 22% 'not resilient'

40% 22%

38% of 'resilient' respondents provide clear communication and policies, versus 22% 'not resilient'

38% 22%

resilient
not resilient

Resilience gains are under threat

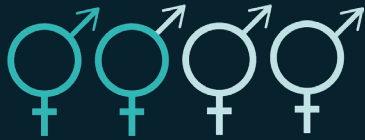
It's no secret that human error and insider threats are one of the biggest threats to an organisation's cyber security. Our research shows that while this remains the case, there is another, more alarming threat on the horizon, the adoption of AI. The combination of insider risks and AI represents a dual threat that organisations must urgently address to stay secure. Despite years of moving in the right direction, this hard work could be on the brink of unravelling with AI becoming the 'Achilles' Heel of Cyber Resilience'.

AI: The Achilles Heel of Cyber Resilience?

AI adoption is gathering serious pace

The last 18 months have seen a significant shift in the adoption of new technology within organisations, notably AI, with our research showing that 62% of workers have used ChatGPT or Copilot in some capacity. Our research shows some surprising trends, especially around frequency, with a significant 41% using one of these tools at least once per week. We can also see trends emerging per industry, with Professional Services being the keenest to adopt.

ChatGPT or Microsoft Copilot are used
6 times per month on average



Collectively, 41% of workers say they use ChatGPT or Copilot at least once per week



46% of women never use ChatGPT or Copilot
vs 27% of men



19% of men, and 12% of women, use ChatGPT or Copilot 2-3 days a week



41% of workers in
Financial Services



29% of workers in
Healthcare



56% of workers in
Manufacturing



65% of in
Professional Services

This new, rapidly evolving technology is often being adopted by employees without permission, attracting employees with promises of increased efficiency—but we must ask ourselves, at what cost?

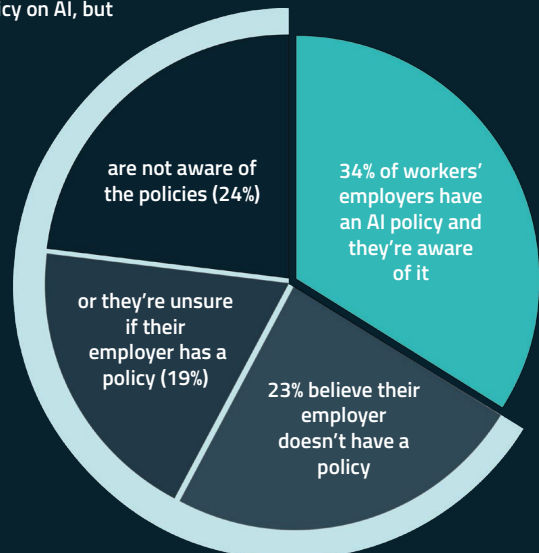
The effectiveness of AI policies

Although 81% of cyber risk owners are either very concerned (24%) or somewhat concerned (57%) about AI, they are feeling confident about the success of the policies they have put in place around it (29% are very confident, and 56% are somewhat).

But this confidence could be their undoing. Our findings show that these policies have failed to resonate with the employees for whom they're in place.

The AI blind spot

More workers either said their company has a policy on AI, but



Gender split; 41% of men say they're sure of company policies on AI, versus 29% of women. Just 12% of men say they are unsure, versus 25% of women.

The mismatch between cyber risk owners and employee knowledge around AI policies is extremely dangerous. The lack of knowledge or awareness of AI policies leaves cyber risk owners with a large gap in their coverage. With employees using unauthorised technologies, UK-based companies face challenges in gathering a complete picture of their cyber risk.

But worryingly, they don't seem to be aware of this blind spot and are putting their confidence in their policies and employees. This potentially results in the unravelling of years of cyber resilience investment.

The Truth About Human Error

Employees are victims of cyber attacks, too

43% of employees we spoke to said they have personally been a victim of a cyber attack at work, and half of those (23%) have experienced an attack in the last 12 months.

51% of workers aged 18-24 have been the victim of a cyber attack (20% in the last 12 months)



44% of workers aged 25-34 have been the victim of a cyber attack (24% in the last 12 months)



54% workers aged 35-44 have been the victim of a cyber attack (29% in the last 12 months)



34% of workers aged 45-54 have been the victim of a cyber attack (18% in the last 12 months)



18% of workers aged 55+ have been the victim of a cyber attack (5% in the last 12 months)



56% of men vs. 32% of women

■ victims of cyber attack ■ in the last 12 months

Therefore, adding an array of fast-faced open-sourced generative AI tools into this mix of employees who are unaware of, and are not using, clearly laid out policies, creates a high level of concern.

According to [Gartner](#), 69% of employees have bypassed cyber security guidance in the last 12 months and 74% said they would be willing to do this if it helped them achieve a business goal. Employees wanting to achieve more, faster, combined with the advent of new technology, has created the perfect storm.

Our findings support this theory, with cyber risk owners seeing employees as a high-risk factor

(73% agreed most cyber attacks come through a lack of employee diligence) and noting the use of unauthorised software as a key concern (30%).

73%

agreed most cyber attacks come through a lack of employee diligence

The engagement gap

Cyber risk owners have been communicating security policies and offering employee training for some time, but it's apparent that as well as an AI blind spot, UK businesses are facing an engagement gap.

84% of cyber risk owners believe employees are engaged in cyber security training. But, in reality, 73% of workers describe themselves as either only 'somewhat engaged' in cyber security training (53%) or 'not engaged' (20%).

Do as I say, not as I do

To add to this concern, there's also a discrepancy between what employees say they would do if they saw a colleague breaching security practices (25% said they would report it to IT) versus what employees are actually doing (21% are advising their colleagues on what to do next time and educating them on best practice).

This suggests UK businesses do have an issue with getting their employees engaged in a security culture. Employees may think they would report the incident, but when it really comes down to it, they are often inclined to keep things among themselves.

Groups most likely to do nothing when they see a cyber practice breach, because they wouldn't want to break a colleague's trust:

Those aged 35-44 (11%) most likely, followed by those aged 18-24 (8%)

Men (9%) vs. Women (6%)

Awareness increases resilience

The vast majority (76%) of our 'resilient' cyber risk owners agree most cyber attacks come through lack of employee diligence, compared to only 49% of those who describe themselves as 'not resilient.'

In the name of efficiency and productivity employees are taking technology adoption into their own hands, and the task to engage and educate them is ongoing. But positively, there is clear evidence that cyber risk owners who are facing up to the truth of human error and proactively tackling it feel resilient compared to those who are not.

40% of 'resilient' respondents have invested in training, versus 22% 'not resilient'



38% of 'resilient' respondents provide clear communication and policies, versus 22% 'not resilient'



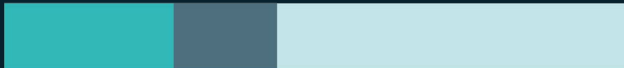
31% of 'resilient' respondents integrate into daily routine versus 22% 'not resilient'



31% of 'resilient' respondents have leadership sponsorship versus 29% 'not resilient'



30% of 'resilient' respondents deploy internal marketing versus 18% 'not resilient'



28% of 'resilient' respondents host clinics versus 22% 'not resilient'



Unsurprisingly, all of those that said they do nothing for engagement are 'not resilient'

resilient not resilient

Plugging the gap

While cyber risk owners look to reduce these risks from human error, they should be looking to plug the gaps with Attack Disruption methodology. This is defined as the immediate containment of an endpoint that minimises the spread of malicious activity.

This form of detection and response acts as a "safety net" for when the inevitable occurs on a company's infrastructure. The best approach to long lasting and sustainable cyber resilience, is a holistic approach, and the right provider can be crucial to this.



"At the point at which an organisation is attacked, it's arguably too late to do anything about it – something cyber risk owners who find themselves falling victim are increasingly conscious of."

"A lot of traditional services function by responding to the actual encryption or ransomware events. That's far too late to make a meaningful difference. By the time that's happened, it's too late to fix it. So, what we should be doing is looking for the spark, which is what we call initial access techniques."

Rob Demain
CEO @ e2e-assure

Empowering Employees to Build Collective Resilience

Building a 'one team' mentality

To relieve frustration and fatigue for cyber risk owners, and build resilience from the ground up, an organisation needs to have a "one team, one dream" mentality. There needs to be a strong narrative in place, positioning cyber security as a collective responsibility, driving an internal cyber security culture to ensure employees are engaged with training and policies.

To help build the trust that is required, cyber risk owners need to listen to employees and give them what they want when it comes to training.

76% of workers said concerns to personal online safety would likely engage them with training, as well as if it was more clearly communicated (75%) or involved real life scenarios that workers could apply (also 75%).

Training that takes place online at a pre-arranged time that is suitable for the worker, is also popular (72%).

Workers would also be more likely to engage if training was short but regular (53%) over long but less regular (23%).

Training and accountability

When an employee is responsible for a cyber attack, cyber risk owners are most likely to offer training.



When employees were asked about the consequences of falling for a cyber attack, over half (59%) said they either receive training and risk disciplinary if they cause another breach (32%) or they are required to attend training (27%).

Clearly, training is happening but what works for some people, doesn't necessarily work for others. Less than a quarter (24%) of employees would describe themselves as 'very engaged' in cyber security training.



Long but less regular training is only helpful for 10% of workers



Clearer communication is most likely to help: workers aged 25-34 (35%), and workers aged 35-44 (32%)



Short but regular training is most likely to help: workers aged 45-54 (35%) and those aged 55+ (42%)



Real life scenarios are most likely to help men (30%) and clearer communication is most likely to help women (34%)

When we train employees in the different skills required to do their job, we take into consideration their learning styles e.g. visual, listening, watch and learn. Cyber risk owners should also take this approach, especially when it comes to the urgent training required around the threat of AI, and the company's AI policies.

Employee engagement that resonates


What does seem to resonate for the majority is the threat to personal online safety.

Understanding the Tension

To reduce the risk from human error and ultimately maintain the resilience of their organisations – cyber risk owners need to understand where the tension lies between them and employees.






Following cyber risk owners' frustrations with use of unauthorised software (30%) such as AI, top frustrations all reflect apathy, or a lack of care, from employees.

Cyber risk owners' top 5 frustrations

-  Use of unauthorised software (30%)
-  Resistance to training (26%)
-  Falling for phishing attacks (26%)
-  Ignoring security protocols (26%)
-  Failure to report incidents (26%)





When we look at what the frustrations are for employees, we can see a pattern of overwhelm, and fatigue.

Workers' top 5 frustrations

-  Complex password requirements (23%)
-  Slow system performance (22%)
-  Training fatigue (22%)
-  Excessive alerts and notifications (20%)
-  Lack of clear communication (18%)

Cyber risk responsibility

Another tension point comes from a lacking sense of responsibility from employees. When asked about who was responsible for the security of the organisation's data, employees placed the IT team first, and themselves third.

-  IT team (42%)
-  Everyone in the organisation (40%)
-  Myself (21%)
-  CIO (14%)
-  CISO (12%)

Those aged 55+ are the most likely to see everyone in the organisation as responsible (70%) and are the least likely to think the responsibility lies with the IT team (26%) and themselves (11%).

Gender differences

Men are more likely to think the responsibility is theirs (25%) than women (18%) and women are significantly more likely to think it's the responsibility of everyone in the organisation, than men (50% vs 30%).

A significant proportion of both men and women think the responsibility lies with the IT team (47% of men and 38% of women). Overall, men are more likely to pinpoint blame on one option (even themselves), whereas women view the responsibility as a collective one.

A lack of understanding around who is responsible could come from a lack of knowledge about what the consequences are, or complete lack of consequences, should they fall for a cyber attack. When asked, almost a third said they either didn't know what the consequences were (22%) or that there wasn't any (6%). Which may also explain employees' keenness to adopt new unauthorised software.

Tackling the Problem in 2025

With the evident challenges cyber risk owners are facing with employee risk, it's clear why cyber resilience sits at the top their agenda this year. Although, as a whole, organisations are feeling more confident in their resilience than last year; these results show it's vital for cyber risk owners to start looking at their resilience picture from the ground up.

The biggest discrepancy is around the strength and understanding of AI policies, creating an Achilles' Heel in cyber resilience. These conflicting views, between employees and cyber risk owners, pose the biggest threat to years of resilience investments.

So where do we start and how do cyber risk owners implement a ground up approach?

1. Keep employees at the centre of the security strategy

There are clear signs of fatigue across organisations, with all parties expressing a level of frustration, but inevitably all trying to achieve the same goal. Business growth and enablement.

Therefore, by keeping employees and their needs at the centre of security strategy, cyber risk owners can collaboratively work with them to create training and policies that enable them to secure their business.

Although a long-term goal, there are proactive steps cyber risk owners can take now:



Create a culture of security awareness

Cyber security should be a shared responsibility, and an understanding of this, across the organisation, is crucial to gaining respect for how and why policies are being implemented. A great way to achieve this is through manager buy-in and taking the time to acknowledge staff who follow best practice. If team managers are on your side, they can help foster a security culture and integrate it into day-to-day practise



Don't write policies from behind closed doors

Get employees involved, understand what software they need to achieve their business goals and monitor these to ensure you have full visibility of potential risk



Improve communication

Bridge the gap between security teams and staff by ensuring that security measures are explained clearly. Employees need to feel like partners, not hurdles. Regularly collect feedback and adapt training and security measures based on that input, to ensure the security strategy evolves with the organisation's needs



Tailor training

Not all staff have the same level of exposure to threats. Customise training based on an employee's role and potential vulnerabilities, as well as their learning style

2. Keep security for end users simple

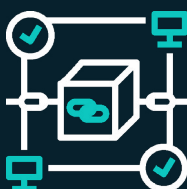
Our findings suggest that employees are frustrated with the complexity of security. Understandably, with the clear rise in threats from employees, cyber risk owners won't have the risk appetite to remove policies/procedures, or give employees the green light to use whatever software they please. But with the correct configuration of technology, it is possible to enable teams with the technology they need, while keeping security at the core of business operations.

Depending on your current set up, this can be a quicker fix by implementing the following:



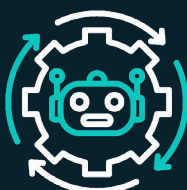
Use role-based access controls (RBAC)

Ensure employees only have access to data and systems relevant to their roles, minimising exposure if an account is compromised. This keeps the overall risk level of each employee to a minimum, but still enables them to get their work done.



Validate supply chain access

There must be some give and take, between cyber risk owners and employees. So, it is a fair trade to ask employees to help clearly define which third-party contacts have legitimate access to your systems and data to reduce risk from phishing attacks.



Use automation to reduce human error

Implement automatic Attack Disruption systems that can temporarily disable compromised accounts or network access when a phishing attempt is detected, offering a safety net for human mistakes. As a result, giving companies more confidence in their resilience and therefore trust in their employees.



Leverage user behaviour analytics

Understand normal user patterns to detect anomalies that may signal compromised accounts. Alert tuning based on real behaviour reduces false positives and business disruption.

Note: This is most effective when all systems are monitored, so working closely with employees to understand what tooling they wish to use is important first. Moving forward, companies should use and continually test playbooks and simulation exercises to improve accuracy and reduce false positives.

3. Have the right provider in place

We've discussed core ways of implementing change to negate the risks covered in this report. But your core set up will fundamentally impact a company's ability to put these suggestions into action.

As a result, a crucial factor cyber risk owners need to consider is the partner they collaborate with, and that partner's ability to provide expertise and guidance.

There are two areas we suggest cyber risk owners focus on when choosing and reviewing their provider:

A. Specialist expertise

Cyber defence is not a simple task. Technologies alone will not fill the gap of people and process as those that are poorly configured will provide very little value. It's imperative that companies outsourcing their cyber defence seek a partnership with a specialist that has dedicated resource focused solely on Threat Detection & Response.

What to look out for:



Smaller service portfolio

Spreading resource too thinly across multiple services or "testing your own homework" through in-house pen testers can result in unnecessary service gaps



Clear communication pathways

Amid a potential incident, you need to have confidence that you can communicate quickly and easily with your provider. Ideally look for live chat options such as the e2e-assure SOC Channel App via Microsoft Teams



Evidence of continual service improvements and investments

We all know cyber threats and TTPs are constantly changing and as a result so should your cyber defence tactics. This doesn't always mean the newest and shiniest of technologies. Continual procedural improvements are evidence of a provider who prioritises the protection of their customers

B. Flexible commercial agreements

Agility in ongoing cyber defence is no longer a luxury, but a necessity. Last year's research showed us that cyber risk owners want shorter contracts (43%) and more flexible contracts (50%) and this year's findings exasperate this need further.

What to look for:



Modular service offering

Every business has unique technological and monitoring needs and it's critical this be considered in commercial options. A key benefit of outsourcing is having the ability to easily increase or decrease monitoring requirements, which should be an option through a modular service approach



Options for shorter or rolling contracts

Old, stagnant contracts that don't allow for service amendments leave businesses with large monitoring gaps, which is unacceptable in 2025. These options may be slightly more expensive but mid-contract amendments can come at an extortionate cost



Technological autonomy

Often providers will lock customers in by owning their technological licensing, with the promise of cheaper technology options. This cost saving is a great benefit, but having technological autonomy is often an overlooked advantage that puts the control back into the hands of the customer

The journey to cyber resilience will never be over. Yet there are clear, immediate next steps cyber risk owners can take to strengthen their foundations. Employees are the bedrock of those foundations. Keeping their needs at the centre of cyber security, and simplifying their experience, will help that bedrock from becoming porous.

For the inevitable moments employees do let their guard slip, the right provider can act as an underlying layer of armour that transforms an organisation from resilient to battle-ready. They can protect the Achilles' Heel, building cyber resilience that is truly holistic.




e2e-assure: Specialists in Threat Detection and Response

If you're looking for an independent specialist for guidance or support in building out your holistic approach to cyber resilience, get in touch.

We abstract away all unnecessary complexity from communication channels and empower your teams with clear, understandable and actionable knowledge, giving you the advantage in protecting your business against cyber threats.

Talk to us

Contact Information

 www.e2e-assure.com

 info@e2e-assure.com

 [e2e-assure](https://www.linkedin.com/company/e2e-assure)

For all PR inquiries please contact our PR agency directly:

 e2e-assure@ambitiouspr.co.uk