advania

Building core resilience

Mid-market tech challenges report

Second edition

www.advania.co.uk

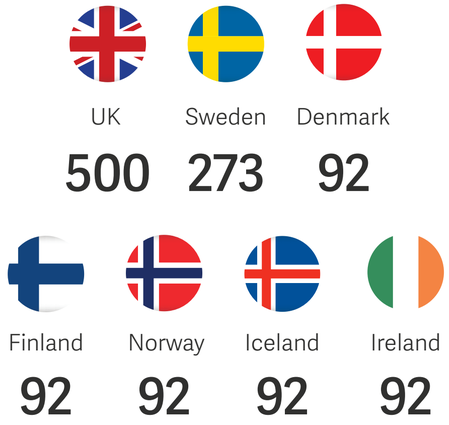
Contents

Methodology

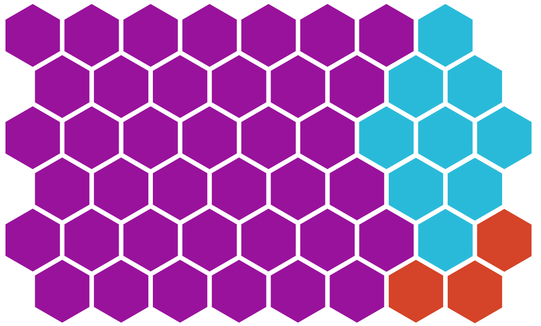
Independent research company, Censuswide, surveyed 1,236 mid-market IT decision-makers across the UK, Sweden, Denmark, Finland, Norway, Iceland and Ireland with responsibility for purchasing software, hardware and cyber security services.

The research aimed to uncover technology challenges holding back the mid-market, and serves as the second edition of Advania's "Engage the core" research report - which surveyed 951 respondents from the UK, Sweden, Denmark, Finland, Norway and Iceland.

Respondents by country breakdown



Business type



Privately owned	76%
Public owned	18%
Family owned	6%

Executive summary

Advania's latest research reveals a decisive shift among Europe's mid-market organisations: a growing move toward technological self-reliance, fuelled by distrust of external vendors and the transformative potential of Artificial Intelligence (AI). While this newfound confidence is enabling greater agility and innovation, it also risks creating a "bunker mentality" that leaves businesses vulnerable to evolving external threats.

More and more mid-market IT leaders now manage cyber security strategy internally as external cyber spending falls, with many expressing high confidence in their own defences - despite rising global cyber threats and a sharp decline in cyber security and cloud spending.

AI is a crucial component in making this possible, and is widely seen as a net positive in enhancing cyber security and customer satisfaction. Yet, while AI tools empower internal development, they also bring new challenges, such as compliance complexity to the accumulation of AI-generated technical debt.

Cost commitments remain a consistent priority despite fiscal caution, in areas as diverse as cloud to ESG. However, tightening budgets have led to cutbacks in key technology investments, and approaches to achieving net-zero vary significantly by region.

Overall, the research highlights a mid-market sector capable and eager to harness innovation for its own independence. But it is in danger of isolating itself from the external expertise needed to stay resilient in an increasingly complex threat landscape.

Hege Støre, Advania Group CEO

Cyber resilience reliant on internal expertise

Overconfidence and the internal trap

Despite recent evidence of the real-world costs of cyber security failure for European enterprises, the mid-market retains a concerning preference for cyber strategy self-reliance. Advania's previous survey detected a similar reluctance among mid-market IT leaders to seek out expert external advice, a trend which has accelerated more recently.

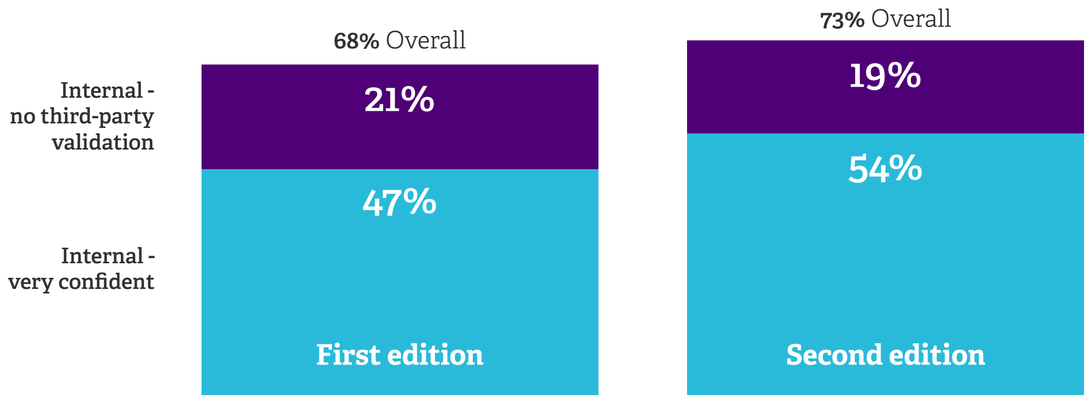
Certainly, confidence remains high, with 73% of mid-market IT decision-makers retaining their own cyber security strategy up from 67% in our previous survey. This figure includes those who feel "very confident" of their effectiveness, and those whose cyber strategy has "no third-party validation".

A small but nevertheless concerning 4% of mid-market organisations describe their cyber strategy as a simple 'tick-box exercise'. Their lower target profile as mid-market companies may have spared many of them from disaster until now, but this relaxed approach contrasts sharply with the growing frequency and sophistication of major cyber incidents.

Mid-market IT teams lack large, specialised cyber teams. Even enterprises with in-house expertise have recently proved to be not up to the task. It is brave then of mid-market organisations to take on the mammoth challenges of modern cyber defense.

This overconfidence on internal resources may prove costly. Particularly when considering that reputational/brand cost from an attack is the most important factor for justifying their ROI (Return on Investment) from cyber spending according to 44% of IT leaders.

Which of the following best describes how your current cyber strategy has been developed?



How do you calculate ROI (Return on Investment) on cyber spend?

1st Reputational/ brand cost from a breach/attack

2nd Communication costs saved by not needing to inform external parties of breach/attack

3rd Legal costs associated with breach/attack

Cyber risk spreads from the inside

Internal concerns outweigh external threats

Cyber attacks on mid-market IT teams are relentless and evolving. Emerging cyber threats remain the single most recognised concern - up 6% from our last report to 44% now.

Adding to the cyber threat landscape is a significant new anxiety: the use of AI by threat actors. A third of respondents see AI as a risk to their cyber resilience, rising to as high as 41% in Denmark and 45% in Norway.

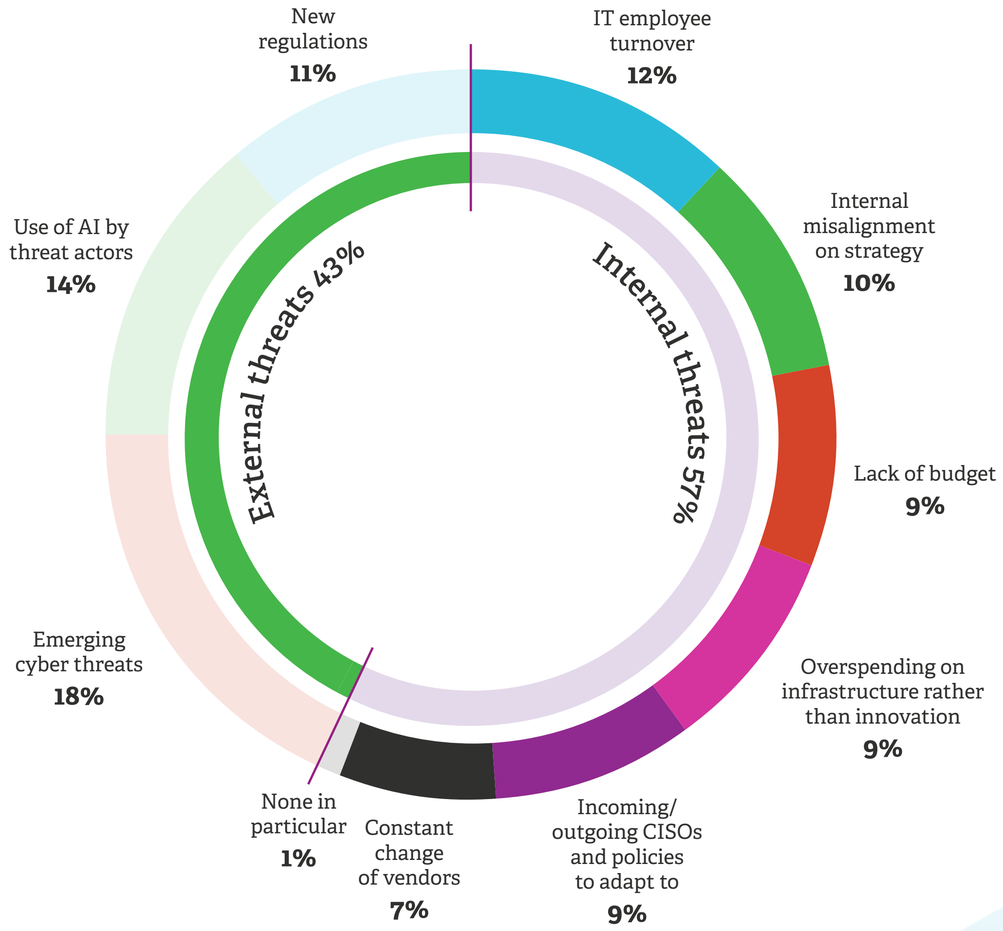
However, the greatest cyber threat IT leaders perceive, despite their growing sophistication, are not external hackers.

While not diminishing the severity of outside attacks, IT Employee turnover, with its ensuing knowledge gaps, often leads to inconsistent security practices - a factor cited by 21% of IT leaders. Asked to define the biggest disruptors of IT cyber security strategies, respondents' concerns broke down as:

- **43% pointed to threats from outside the organisation**
- **57% pointed to factors within their own walls**

Communication is critical in optimising an organisation's cyber-resilience. Internal misalignment on strategy is a prominent hurdle for 25% of respondents. If a cyber strategy is not understood, bought into, or properly resourced by all key departments - from the C-suite down - it is doomed to fail.

What do you believe are the biggest factors for disruption in your IT cyber security strategy?



Cyber training up, defences still down

Increased training is not a clear strategy

In response to the clear rise in social engineering attacks, mid-market organisations have stepped up their training efforts. However, when we look at the most common and costly attack vectors, Phishing and Business Email Compromise (BEC), the majority still aren't doing enough to keep their staff safe and supply chain protected.

When respondents were asked how frequently their company repeats cyber security training, our research found only 11% of organisations deliver this critical training more than once a month - on average once every 41 days. Interestingly, organisations delivering monthly training has increased from 22% previously to 32% in this survey.

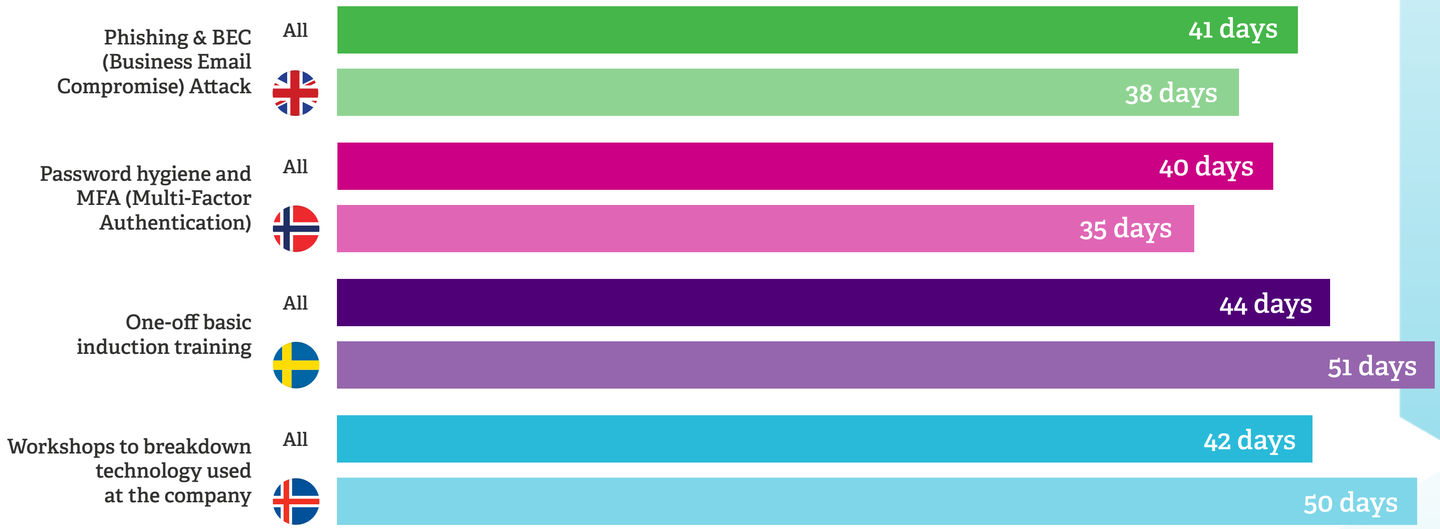
While positive, it still means two thirds of workforces receive this vital training less frequently than monthly. With spear-phishing and BEC attempts becoming daily occurrences for many organisations, training that is delivered quarterly or, worse, annually, simply cannot build the "muscle memory" required to recognise and deflect threats in real-time, especially when those threats are evolving.

While this trend is consistent across Northern Europe, there are clear leaders and laggers based on country. Ireland leads with 53% offering training monthly, or more frequently, and Iceland at only 34%. The UK leads on Password Hygiene and MFA training with 53% of respondents implementing this monthly - or even more frequently. It also leads on workshops to break down company specific tech training at 47%.

"Awareness is not a one-off event but a consistent, ingrained aspect of the company culture. If you are not testing your people frequently, your employees are being trained by the criminals instead."

- Pravesh Kara, Director for Security & Compliance, Advania UK

What types of cyber security awareness training does your company offer and how frequently is it repeated?



Vendor trust is down across the board

The widening credibility gap

With so many organisations turning inward for answers to cyber threats, one external factor emerged as an unexpected issue - a clear and growing distrust of software vendors among mid-market IT decision makers.

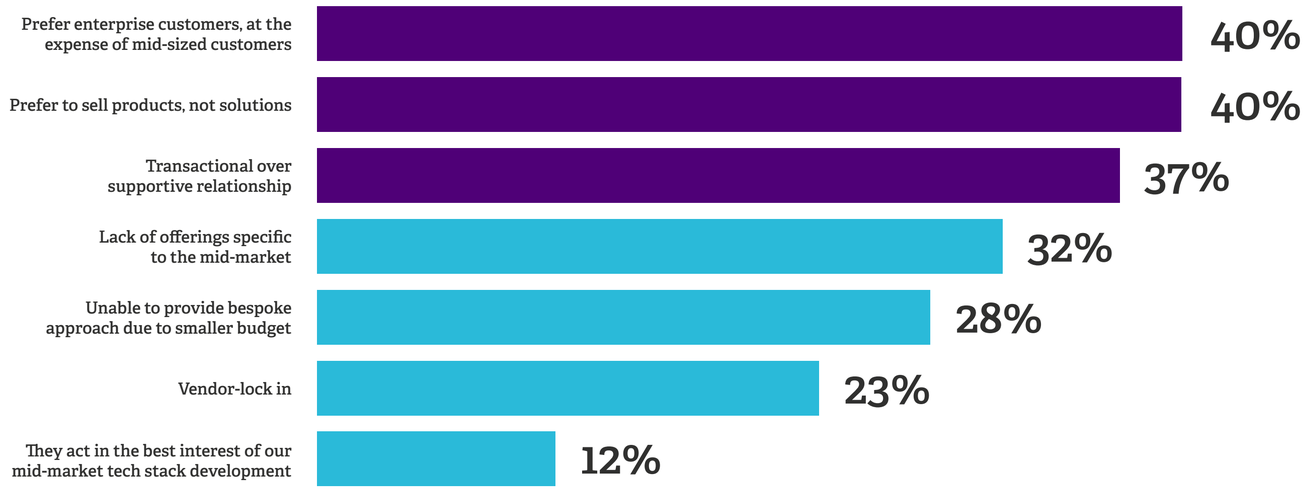
The perception that vendors do not operate in the best interest of mid-sized organisations is more widespread than ever, with nearly every reason for distrust being felt more acutely than the year before.

- The most prominent grievance is the belief that vendors favour larger clients. This feeling of being sidelined has increased significantly, with 40% now believing vendors prefer enterprise customers over mid-sized customers - a rise of 9%
- This is compounded by a growing frustration with fragmented sales models, with 40% of IT leaders feeling vendors “prefer to sell products, not solutions” - a jump of 12%
- 36% feel the relationship is overwhelmingly transactional, not supportive, a 13% increase from last time

These figures point to a credibility gap. Mid-market organisations feel their unique needs - for tailored, integrated, and supportive solutions - are being ignored in favour of box-selling and enterprise-focused strategies. Only a small minority of respondents, 12%, believe their vendors genuinely operate in the best interest of their company and tech stack.

This lack of faith makes a strong case for seeking to work with right-sized partners focused on the mid-market and explicitly dedicated to understanding mid-market customers’ needs with solutions, which can flex up and down as market volatility remains.

Why do you believe that vendors do not act in the best interest of the development of your mid-market tech stack?



50%

Have firewall and antivirus (for basics)

6%

Average decrease across all other actions

AI impact seen as a net positive

Believing in potential, lagging in action

No mid-market IT decision-maker can escape the impact of artificial intelligence. However, most see AI as overwhelmingly positive, with 71% of respondents reporting that it has had a beneficial impact on their organisation.

Only 28% of IT leaders view AI as negative, and only 8% of IT leaders see AI adoption as a threat to their own headcount, running counter to the general perception of AI as a direct threat to jobs. A mere 1% believe there are "no benefits" in the short term.

The AI imperative

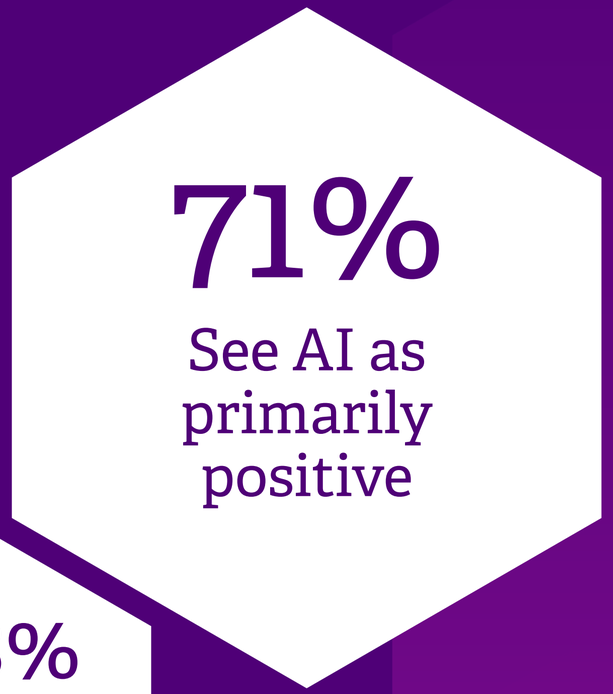
The positive impact most anticipated by those embracing AI is improving cyber security, cited by 27% of respondents. This highlights a growing belief that AI will be the critical tool in the ongoing battle against AI-enhanced cyber threats. However, the rapid adoption of AI is not without its concerns, with the main apprehension being AI will "Increase the complexity of compliance," an issue cited by 12% of respondents.

Awareness vs. action

Despite this generally positive outlook, 76% of mid-market organisations are not recognising AI's potential to improve productivity. This is despite 71% claiming to see a positive impact, suggesting productivity alone may not be the best metric for measuring AI success. At least not in the IT team.

On the skills side, a third of mid-market organisations admit their tech stack isn't future-proof due to a "lack of knowledge in AI", and only 19% expect AI to help build the technical skills needed for long-term growth, up slightly from 16% in our previous research.

What do you see as the key impact of embracing AI for your organisation?



AI code proliferating at pace

AI reopens the build vs. buy software debate

Under the hood of in-house IT teams, the rapid adoption of Artificial Intelligence (AI) and generative coding tools has fundamentally disrupted the traditional choice of 'custom-built' versus 'off-the-shelf' software in the mid-market. The results show a seismic shift towards AI-assisted and AI-generated code, effectively opening the floodgates on customisation for mid-market organisations.

The total proportion of custom-built code, either internally or outsourced, remains significant. But a substantial portion of this is now directly influenced by AI.

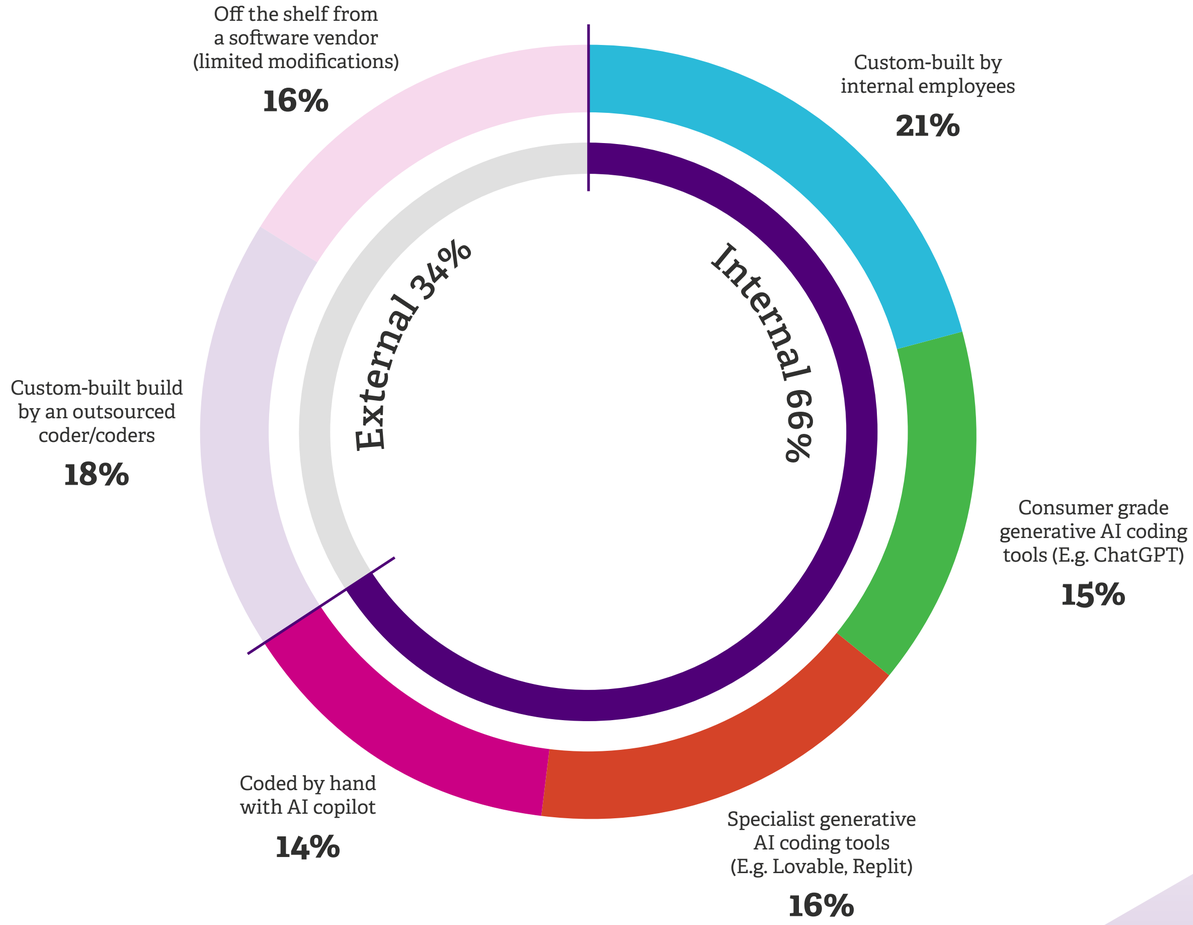
The new coding landscape

Internal code development accounts for approximately 66% of all code, and with a full 30% of that being "vibe coded" or produced with copilots. For a concept which a few years ago was rarely used, let alone trusted, AI-derived code now accounts for 47% of organisations new code indicates remarkably swift adoption by the mid-market.

In fact, this reliance on AI to accelerate internal customisations may help to explain the turn away from external resources. Off-the-shelf software, with just limited modifications, has seen a notable drop, falling from 50% to just 16% in this survey, indicating the European mid-market now believe they can create better solutions faster internally rather than relying on generic, off-the-shelf solutions.

AI can be a double-edged sword. AI-generated code, especially when "vibe coded" can introduce significant technical debt and complexity. Over the long-term code quality needs to be managed - a problem which compounds over time without the oversight that a concrete AI strategy demands.

What percentage of your company's code is derived from the following sources?



Real-world impact of AI

AI's impact goes beyond cost-cutting

To win in tight markets against larger, more efficient rivals, or even fast-moving startups, mid-market organisations need the competitive edge of productivity. But many organisations believe they can achieve productivity by cutting roles.

Only 29% reported "headcount savings" as key, reinforcing that IT leaders do not view AI as a strategy for wholesale labour replacement. In fact, organisations are holding on to top talent more effectively, with excellent IT staff staying in roles for an average of 13 months, up from 11 months - boosting continuity and reducing the disruption of staff turnover.

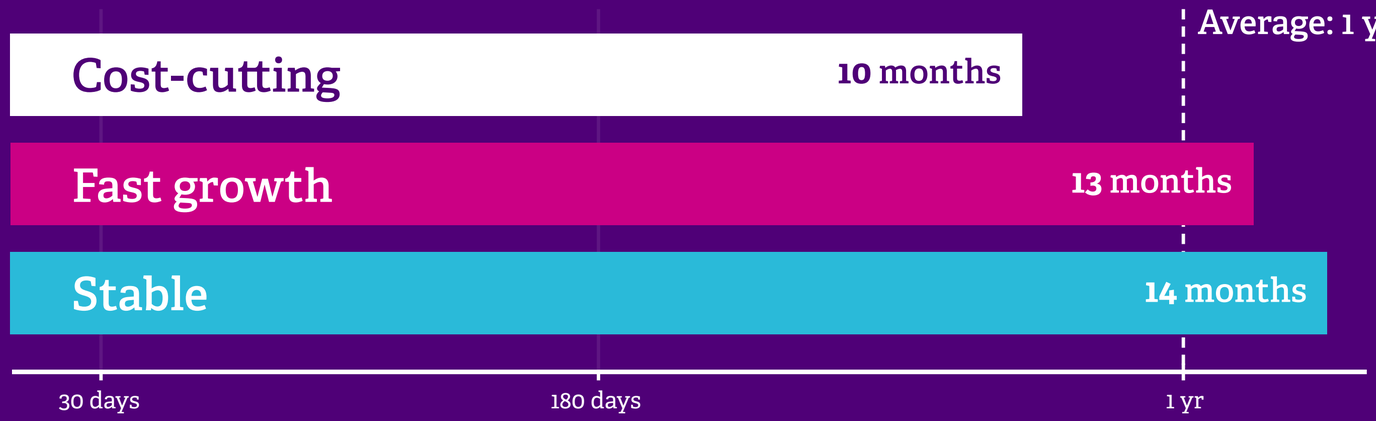
Productivity puzzle unlocked?

This research proves that when deployed skilfully, AI can augment human performance and elevate customer outcomes, not just replace headcount. This is where the mid-market can win. The top two metrics for measuring AI's impact were neck-and-neck at the top of the list:

- **Higher customer satisfaction rating - 48%**
- **Time saved overall organisation - 47%**

We can see the goal for mid-market leaders is not just to do things faster, but to reuse saved time to deliver better customer experiences. Mid-market companies are framing productivity not just in terms of internal efficiency but directly in terms of external business value.

Tenure of "excellent" IT staff in mid-market organisations



"Measuring impact by value, not just effort, is the new standard, and it's how we ensure AI delivers tangible, sustainable growth."

Chris O'Brien, Products & Services Director, Advania UK

How are you measuring AI's impact on IT productivity?

48%
Measure higher customer satisfaction

2%
Do not anticipate AI improving productivity

Who is dictating AI Policy?

Regulators join the list of top influencers

Who dictates AI policies within organisations is often subject to push-pull between C-suite and IT decision makers within mid-market organisations. On the wider international and political stages, however, some leaders are now edging ahead in their impact on mid-market AI strategy.

Mid-market IT leaders are watching closely

Mark Zuckerberg and Meta narrowly topped the most influential figure poll with 12.9%, virtually neck and neck with traditional AI figureheads like Sam Altman of OpenAI on 12.7%, narrowly edging out Elon Musk of xAI with 9.9%.

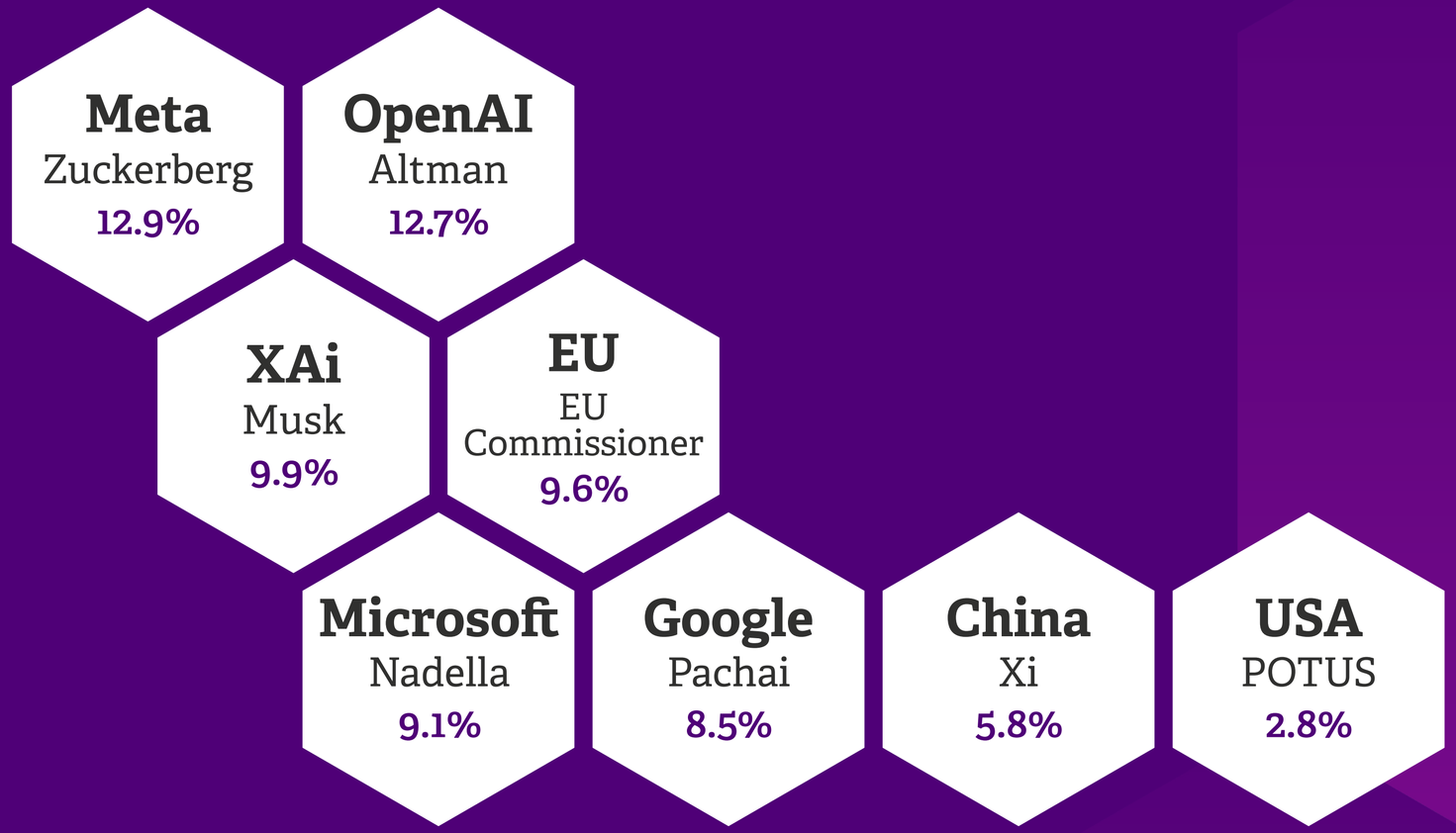
Demand for open models: This reflects a growing market desire for open, customisable models that businesses can run and tailor independently.

Vendor lock-in: The high influence rating for Zuckerberg and the lower-than-expected influence for Satya Nadella of Microsoft (9.1%) and Sundar Pichai of Google (8.5%) suggests a latent concern about vendor lock-in with proprietary platforms like Microsoft Copilot or Google Gemini. As with its' turning inward on cyber security, the mid-market is actively seeking control over its AI destiny.

The politicians of AI

The EU Commissioner's emergence as a significant influencer with 9.6% of the vote, ahead of both national leaders on 5.8% and the POTUS on 2.8%, is perhaps unsurprising given the markets surveyed, but does indicate a fragmentation of AI influence along regulatory lines. For the mid-market companies of Northern Europe the global landscape of AI is being shaped by those who provide the more accessible technology, and by those with the greatest regulatory power to enforce the rules.

Most influential figure/regime impacting AI strategy



Penny pinching pauses progress

Short-term caution undermines long-term growth

Budget constraints in the mid-market are a fact of life, but for many IT decision makers this time feels slightly different. We're in the middle of a period of fiscal caution influenced by macroeconomic pressures like inflation and high interest rates, which when combined with technological shifts has led to a dramatic reprioritisation of spending away from two previously dominant areas.

As a percentage of budget:

- **Cloud Services spending has dropped by 13%, from 23% last time to just 10% now**
- **Cyber security budgets have halved, from 24% last time to 12% now**

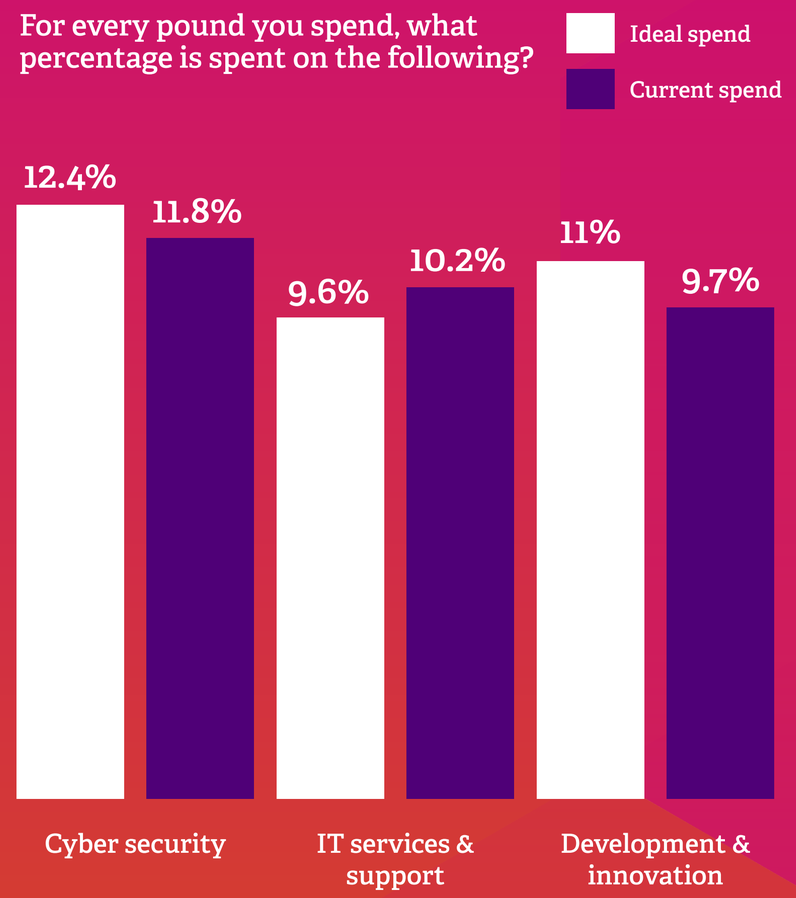
This sharp decrease could stem from several factors: The need to divert funds to cover higher operating costs (energy, labour, software licensing), a forced budget squeeze or even the post-COVID stabilisation period where companies are re-assessing large cloud and security investments made between 2020 and 2023.

Confidence hits budgets

The penny-pinching directly links to a crisis of confidence in long-term readiness. The failure to future-proof the IT environment is directly attributable to the very areas where spending has been cut or constrained:

- **Financial Constraints:** Budgetary restrictions on 33% and accumulated Tech Debt at 32% are key barriers, preventing the necessary capital expenditure to modernise and scale
- **The AI Readiness Gap:** Critically, 37% of respondents cite a lack of AI knowledge as a barrier to future-proofing

This highlights a skills concern that, coupled with reduced spending on development and innovation, prevents organisations from capitalising on the transformative power of AI and building an environment capable of handling scalability plans for the next five years.



Expectations go up even as spend goes down

Rethinking “essential” costs

The dramatic drop in spending on cloud services and cyber security can be explained by the feeling mid-market IT leader’s feeling they are being significantly overcharged. This results in budget pressure for major investments in cyber security and cloud.

The licensing headache

Licensing fees are the number one budgetary pain point. Almost half believe they spend too much on licenses. This significant finding replaced the previous top-rated expense, “Generic products not in use,” at 39% - now in third place. “Additional cloud services” now ranks as the second-highest budgetary concern at 42%.

Declining cloud spend provides a clear reason for organisations to re-evaluate their cloud-first strategies and seek opportunities for cost optimisation.

Mid-market companies expect help with:

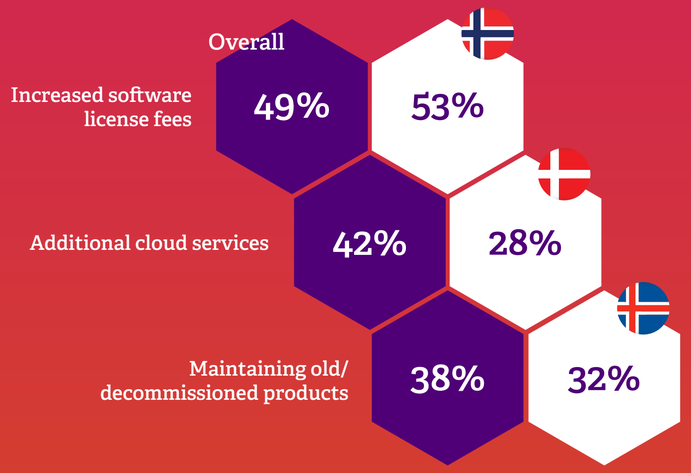
- **Coverage for data recovery - 55%**
- **Cyber security consultancy to fix issues - 51%**
- **Refunds after cryptojacking - 44%**

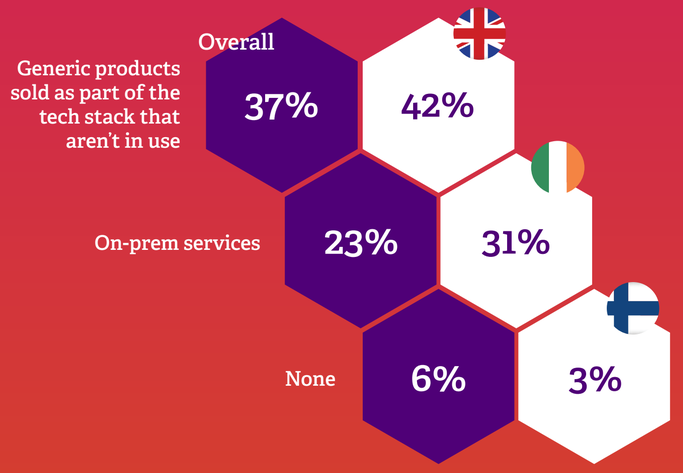
Under most agreements, these expectations are not covered. Certainly not by the vendor. Cloud Service Provider (CSP) contracts typically limit liability to service credits, capped financial amounts, or are restricted by the SRM (Shared Responsibility Model). This disconnect highlights an urgent need for the mid-market to partner with a trusted MSP that can fill this gap, providing the contractual clarity and responsibility that others cannot.

The cloud liability gap

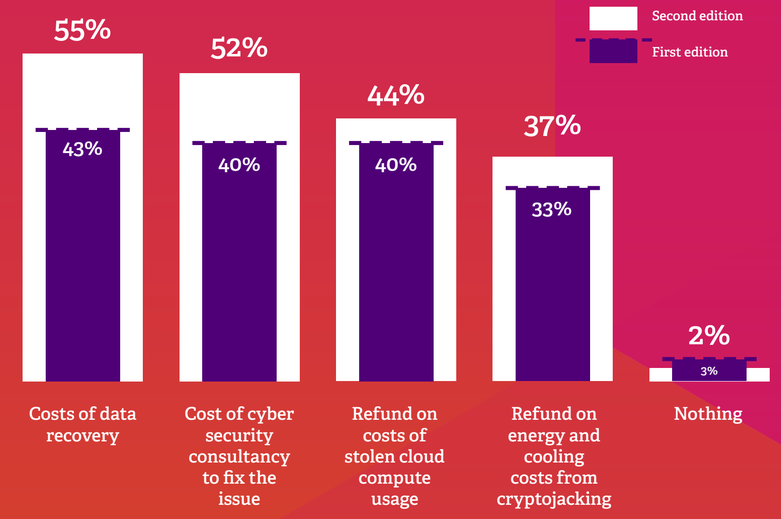
Despite feeling the financial squeeze, the expectations of what cloud providers should cover have risen year-on-year, creating a clear perception gap between what customers want and what contracts deliver.

What aspects of your IT tech stack, do you believe you are spending too much of your budget on?





After a data breach, what is your cloud providers liability?



Paying down tech debt at last

Deferred no more

Decoupling from big spending commitments, like cloud, has left the door open to tackle the mid-market IT leader's biggest chore, the one many delay; paying off their technical debt.

Deadlines drive modernisation

With major platforms, like Windows 10, reaching end of life, the commitment to modernisation has seen a marked acceleration. A strong majority, 67%, is now proactively addressing tech debt by regularly reviewing and replacing legacy systems. This represents a massive 24% jump from the previous survey's 43%.

Proactive automation

This increase in removal is supported by a fundamental and proactive shift in practices: 59% now use automated testing, up sharply from 39% previously. Others are leveraging AI for code analysis and testing in an effort to speed up and systematically identify, prioritise, and eliminate future technical issues for new technical solutions.

A key example of proactive tech debt pay down is the Windows 10 end of life event. Mid-market organisations are nearly there with almost half, 47%, already upgrading their devices to Windows 11. Others are demonstrating readiness and strategic planning.

- **38% are migrating some or all users to virtual desktops, such as Windows 365 or Azure Virtual Desktop**
- **40% have audited their device fleets for Windows 11 compatibility**
- **Fewer than 1% have yet to act**

While most are modernising now, a substantial 34% still plan to rely on Microsoft's Extended Security Updates (ESU) which addresses immediate security needs. It is not a long-term solution to the underlying tech debt.

How do you identify, prioritise and remove technical debt?

67%
regularly review and replace legacy systems
First edition 43%

59%
have automated testing
First edition 40%

32%
wait for bugs and glitches to arrive
First edition 26%

Inconsistent net-zero strategies

Net-zero is case-by-case

Despite the financial constraints and budget tightening seen across the mid-market, commitments to ESG (Environmental, Social, and Governance) strategies, limiting carbon emissions and the journey to net-zero have not been forgotten. The survey data proves ESG remains a strategic priority, though the approach is often a geographically varied mix of initiatives.

Mid-market organisations are tackling emissions with diverse focus areas:

Norway scores the highest on average, demonstrating the most comprehensive and concerted effort across the board to reduce carbon emissions. Conversely, Iceland scores the lowest, indicating that its companies are currently doing the least to reduce carbon emissions.

The high adoption of refurbished IT equipment in the UK, 38%, is a positive sign, showing that resource efficiency is being embedded into procurement practices, moving towards a circular economy model. Similarly, the focus on remote working, 38% in Norway, is a pragmatic step to reduce the carbon footprint associated with daily commuting.

This variety highlights that organisations are embracing practical, achievable measures based on their national context and operational structure. While the strategy may need work, the collective effort confirms that ESG and net-zero aspirations remain an important component of IT strategy, presenting a clear opportunity for IT leads to offer a unified, sustainable IT framework that brings structure to these diverse initiatives.

The three most common ESG strategies that organisations are utilising to contribute towards Net Zero goals, by country

(Of 15 options provided)

	1st	2nd	3rd
	Using environmentally friendly or refurbished IT equipment **38%**	Implementing sustainable procurement policies **32%**	Switching to renewable energy providers **32%**
	Switching to renewable energy providers **29%**	Using environmentally friendly or refurbished IT equipment **28%**	Green building improvements or energy-efficient office design **25%**
	Encouraging remote or hybrid work to reduce commuting emissions **28%**	Switching to renewable energy providers **25%**	Implementing sustainable procurement policies **20%**
	Green building improvements or energy-efficient office design **33%**	Switching to renewable energy providers **25%**	Encouraging remote or hybrid work to reduce commuting emissions **25%**
	Encouraging remote or hybrid work to reduce commuting emissions **38%**	Implementing sustainable procurement policies **36%**	Green building improvements or energy-efficient office design **34%**
	Green building improvements or energy-efficient office design **20%**	Encouraging remote or hybrid work to reduce commuting emissions **20%**	Implementing sustainable procurement policies **20%**
	Green building improvements or energy-efficient office design **33%**	Switching to renewable energy providers **32%**	Implementing sustainable procurement policies **25%**

advania

The tech company *with people at heart*

w advania.co.uk
e hello@advania.co.uk
t 0333 241 7689