

CYBIT

WHAT 2025 TAUGHT US: FOUR PREDICTIONS FOR 2026





EXECUTIVE SUMMARY PURPOSE AND WHY READ THIS



Cybit's 2026 Technology Trends & Predictions gives UK mid-market leaders a guide on what to watch for when looking to enhance customer experience and loyalty with AI, adopt sovereign-ready hybrid cloud, achieve accountable IT service and support, make business decisions based on a data first strategy and ensure resilience across the organisation.





Rob Hankin

Chief Technology
Officer

[C]

FOREWORD FROM ROB HANKIN, CHIEF TECHNOLOGY OFFICER

2025 has made something clear for technology leaders: the gap between ambitious technology strategies and operational reality has widened, and it's proving costly for UK organisations.

As CTO of Cybit, a leading UK technology solutions provider, I spent much of 2025 in conversations with my leadership peer group across both private and public sectors. What struck me wasn't the challenges they faced (VMware licensing changes, cloud cost overruns, identity breaches) but how predictable these problems were. The right questions just weren't being asked. The organisations that have struggled over the past year, weren't those lacking ambition or investment. They were those who'd built impressive technology stacks on foundations that simply could not handle real-world pressure. When vendors changed licensing models, when cloud providers raised prices, when attackers shifted tactics – these weren't technology failures. They were planning failures.

Success in 2026 won't belong to those chasing the latest AI model or newest cloud service. It will belong to those asking harder questions: Where exactly is our data? Who controls it? What happens when our primary vendor becomes unaffordable? The predictions here aren't speculation. They're based on patterns already visible in how leading organisations are rebuilding: hybrid cloud with genuine resilience, identity governance acknowledging modern attacks, AI initiatives based around data quality rather than market hype.

This is the conversation UK technology leaders need right now. Not transformation for its own sake, but systems built to survive what 2025 taught us.

ABOUT ROB HANKIN

Rob Hankin (CTO) has 25 years of IT leadership, including a decade in a multi-national manufacturing environment. Over the past 15 years, Rob has worked with leading technologies, vendors and distributors including Microsoft and AWS. He leads Cybit's technology partnerships, supporting private & public sector customers across the globe. Rob's expertise is highly valued by key industry players, where he has served on Partner Advisory Councils and Product Advisory teams. As a trusted advisor, he helps organisations from small enterprises to global industry leaders unlock opportunities through technology.

Rob Hankin

Chief Technology
Officer



WHY RESILIENCE REPLACED TRANSFORMATION AS THE TOP TECHNOLOGY PRIORITY

If there's one thing 2025 taught UK organisations, it's this: technology plans that look great on paper can fall apart very quickly in the real world. Last year, costs jumped without warning, cloud platforms went down when we needed them most and identity mistakes turned into headline-making breaches. AI moved faster than governance could keep up. And political pressure started shaping technical decisions in a way many teams weren't prepared for.

Now, as we step into 2026, the industry has shifted a little. No one is talking about "digital transformation" in vague terms anymore, but

business want resilience, clarity and control. The next 12 months will not be about chasing shiny new tools but about preparing solid technology foundations that can survive unpredictable economics, fast-changing threats and increasingly complex regulatory expectations.



STATUS:
TECHNOLOGY RESILIENCE
PRIORITISED

FOCUS:
RESILIENCE FIRST

REALITY:
STABLE SYSTEMS
READY FOR 2026

1.

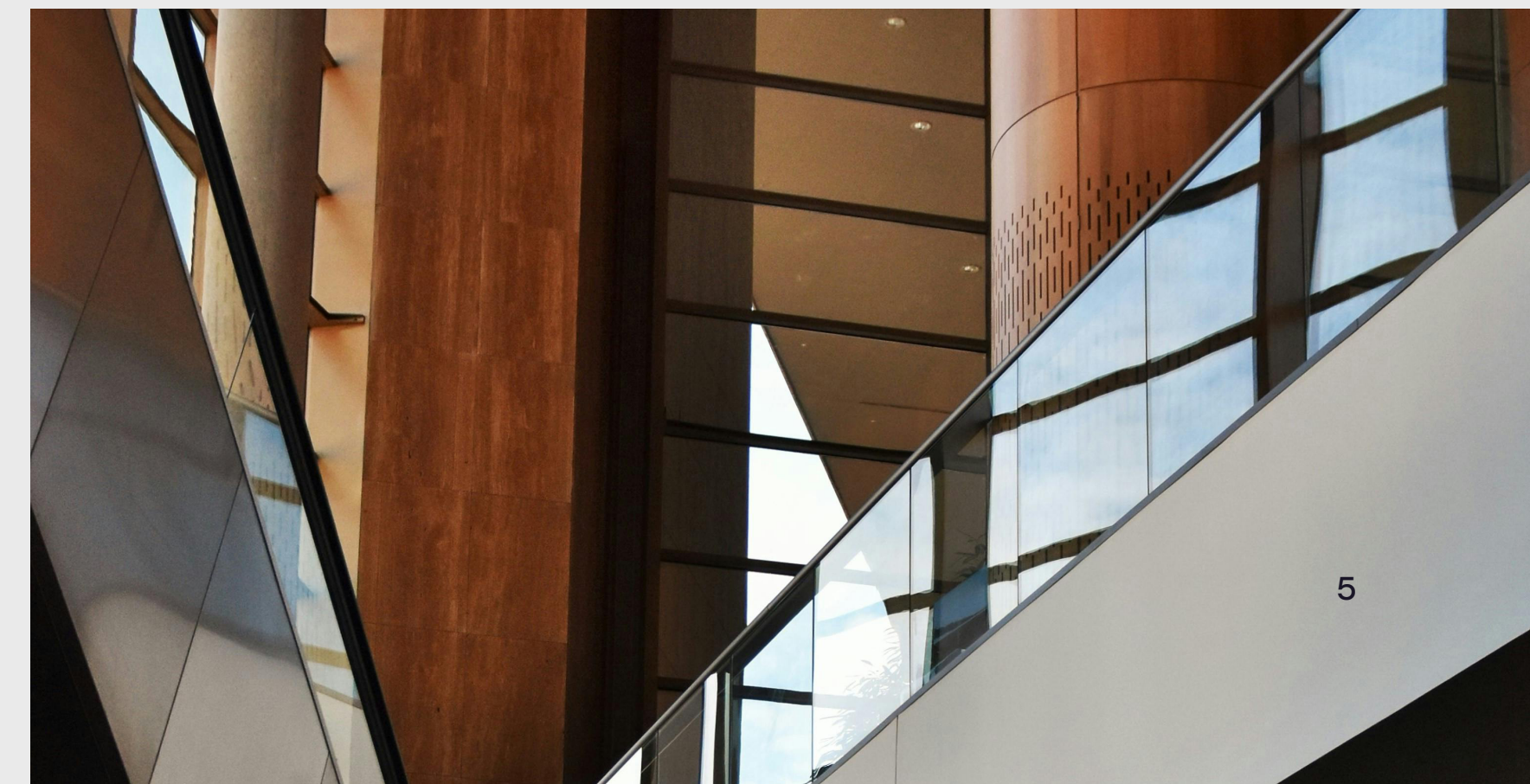
LESSONS FROM 2025, PREDICTIONS FOR 2026

2025 showed that how fragile many cloud and virtualisation strategies really were. VMware's licensing changes blindsided a lot of UK businesses, forcing them to rethink their whole virtualisation strategy.

And with AWS launching its European Sovereign Cloud, plenty of teams began asking: Is our data still safe from political shifts? Is our cloud still the right place for everything?

At the same time, US tariffs pushed up hardware costs and cloud providers raised their own prices. It became clear that cloud wasn't just a technical choice, but also a financial one. These events reveal where the market is heading.

In 2026, more organisations will move away from VMware due to ongoing cost pressure. Confidence in single cloud providers is already weakening, pushing buyers toward multi-cloud and hybrid architectures that offer local resilience when the cloud wobbles. In addition, cloud customers will likely demand stronger sovereignty guarantees as political risks increase. And as providers continue to increase prices, FinOps is moving from a "nice idea" to a business necessity.



2.

STATUS:
CUSTOMER EXPERIENCE
ENHANCED

FOCUS:
PEOPLE FIRST DIGITAL

OUTCOME:
SIMPLER JOURNEYS
STRONGER TRUST

THE MODERN WORKSPACE – TIME OF TECH CONSOLIDATION

Microsoft increased prices across M365 and Teams, which pushed organisations to finally clean up their licences and eliminate waste. Meanwhile, cyberattacks on UK retailers and councils showed that workplace tools are only as secure as the identities behind them and many seemed to have weak identity governance.

Some companies simplified their remote collaboration tools, as using four apps that do the same job doesn't make sense anymore. And with Windows 10 reaching end of life, a lot of organisations realised they weren't ready for the pace of device upgrades.

Looking ahead, this is only going to accelerate. Licence optimisation are likely to become a core



discipline as M365 pricing shifts will continue. Identity protection will top workspace roadmaps because attackers now target tokens and sessions. Additionally, collaboration stacks will shrink as organisations cut duplicated tools. And with US tariffs lifting hardware costs, device refresh cycles are already beginning to slow.

3.

CYBERSECURITY – NO MORE GREY AREAS FOR MSPS

Attacks on Jaguar Land Rover, M&S, Co-op and Harrods made one thing very clear: operational downtime costs more than data loss. When operations stop, the impact is immediate, public and expensive.

At the same time, 2025 saw governments and regulators become more active. Cyber Security and Resilience Bill was proposed to increase security expectations from the UK businesses. Meanwhile, the ICO started handing out bigger penalties for weak vendor oversight. Cyber criminals shifted tactics – tokens, sessions and identity loopholes became

the easiest way in. Customers held MSPs to higher standards, asking exactly who's responsible when something goes wrong. The days of vague contracts are ending.

In 2026, supply chain due diligence will tighten considering major UK breaches involved third parties. Faster breach reporting will become part of compliance. At the same time, we anticipate identity-focused detection will grow as token-based attacks rise. Public bodies will increase resilience spending. And MSP contracts will need explicit breach responsibility clauses.



4.

HYPE VS REALITY: AI AGENTS, DATA GOVERNANCE AND MORE

OpenAI, Anthropic and Google all pushed out major new models in 2025 and expectations only went up. However, many UK organisations quickly found the same problem: their data just wasn't ready. Meanwhile, the Data Use and Access Act added new requirements for anyone handling sensitive or large-scale data.

Factors such as poor quality, missing lineage, confused ownership only slowed down automation projects. At the same time, conversations around "AI bubble" only made leaders more cautious, especially with GPU costs still high.

As we go further into the new year, we'll soon see AI agents handle multi-step operational tasks, but only for organisations with strong data governance. Investment in data quality and lineage will grow as auditors demand evidence, not promises. At the same time, public bodies will shift to smaller, controlled models that meet regulatory expectations. Meanwhile, GPU cost control will matter as concerns about an AI market bubble will make boards cautious.



THINGS BUSINESSES NEED TO FIX URGENTLY IN 2026

In the beginning of 2026, companies should:

- ✓ Re-check all major vendor relationships
- ✓ Build proper multi-cloud resilience
- ✓ Understand where data is stored and who controls it.
- ✓ Tighten identity governance as stale accounts were behind many breaches
- ✓ Track Microsoft 365 usage closely; waste now hits budgets hard
- ✓ Create an AI adoption policy
- ✓ Invest in data quality as AI will not be effective without solid data
- ✓ Strengthen vendor oversight
- ✓ Make breach responsibilities explicit in supplier contracts
- ✓ And yes, finish the move to Windows 11

STATUS:
2026 READINESS CHECK

FOCUS:
CONTROL THE BASICS

PRIORITY:
SECURITY
COST
ACCOUNTABILITY

THE TAKEAWAY

2025 reminded us that technology isn't only about innovation, but also about stability, control and readiness. Businesses that thrive in 2026 won't be the ones chasing the flashiest new tool – but those who build smarter, more resilient foundations.

CYBIT

Equinox House
Silver Fox Way,
Cobalt Business Park,
Newcastle Upon Tyne,
NE27 0QJ

03300 577350
hello@cybit.com

