INDEPENDENT PUBLICATION BY

Raconteur

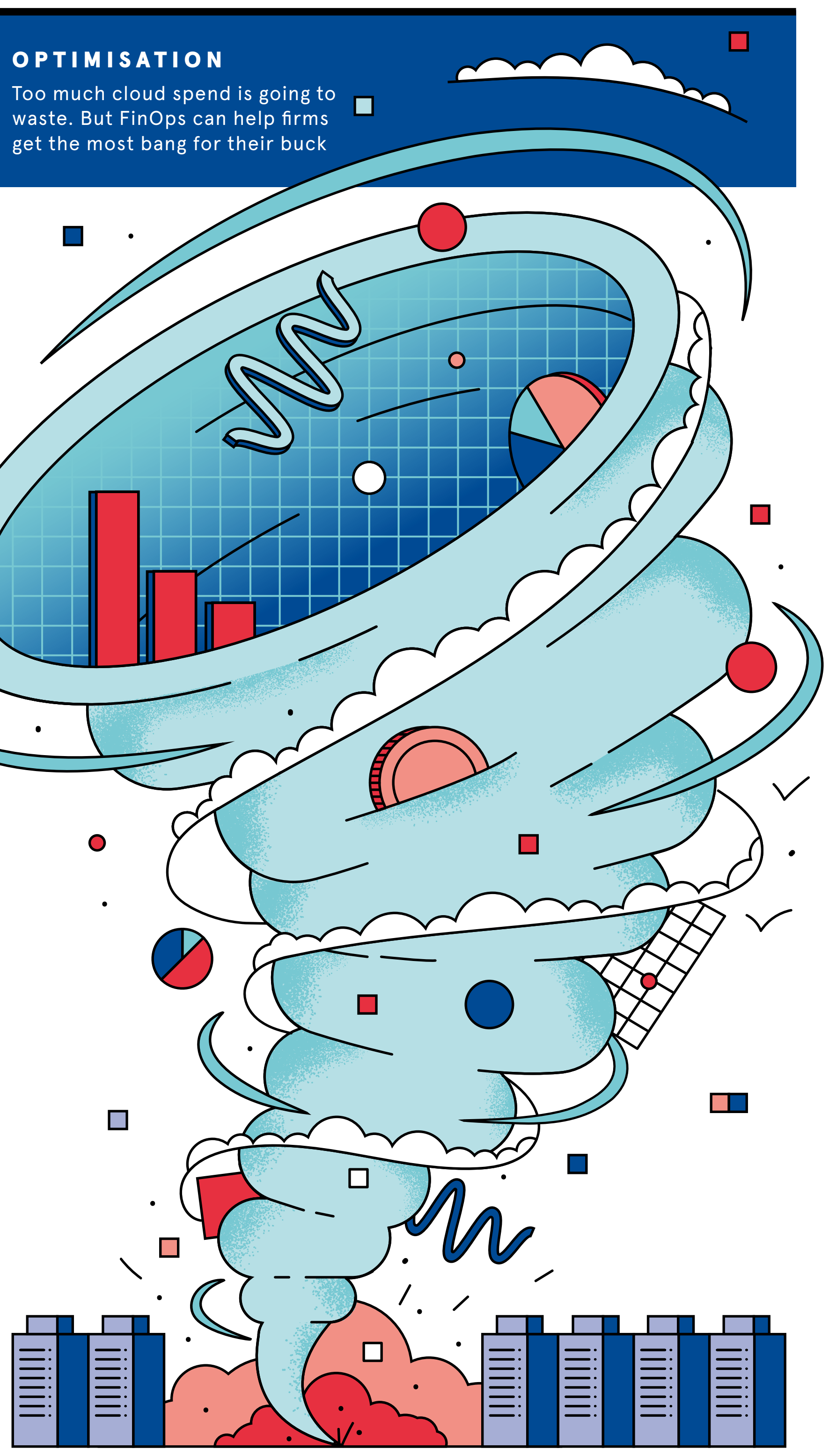
RACONTEUR.NET | #0856 | 05/03/2023

CLOUD FOR BUSINESS

DIGITAL INFRASTRUCTURE

Clouding the issue: firms rethink how to manage data

High energy costs and net-zero targets are testing cloud's image as the ultimate cost-saving technology – and an essential recession tool



Marc Ambasna-Jones

Uber announced last month that it is ditching its on-premises data centres and moving its business to the cloud with Oracle and Google. IT professionals around the country would not have been in the least surprised by the news.

Here was another example of an organisation admitting it's not in the business of running data centres. As its CEO Dara Khosrowshahi put it, Uber is in the business of "revolutionising the way people and products move across continents and through cities". Not forgetting that the deal with Oracle aims to "maximise innovation while reducing overall infrastructure costs" for Uber.

There it is in a nutshell. Cloud computing can help firms to slash costs and free them up to focus on what they do best. If only it were that simple.

Uber's shift from running its own data centres to moving to cloud services is significant. As Steen Dalgas, senior cloud economist at cloud infrastructure firm Nutanix suggests, data centres have become "increasingly expensive and complex to run". Volatile energy costs and coping with the scale of generated data have made running data centres untenable, which is part of the reason the cloud seems so attractive.

But firms must be careful. The image of cloud computing as a cheaper alternative is fair enough – to a point. Dalgas talks about the sticking plaster analogy and highlights how one of Nutanix's customers started a cloud transformation three years ago, only to determine it was "too difficult and expensive to go to the public cloud". It's indicative of the image. Hitting the wall with public cloud for Nutanix's customer meant going back to basics, modernising the entire infrastructure and taking a hybrid approach to the types of cloud services it needed to fulfil its business goals. Saving costs was just one of its aims.

While a Forrester report, *Navigating the 2023 Downturn: Technology Executive*, points to "a strong cloud strategy" as one of the key elements to face up to a recession, it comes with caveats. As Dario Maisto, senior analyst at Forrester, warns: "Cloud is the means to an outcome, not the outcome itself."

> **An IT-centric 'lift-and-shift' approach to moving to the cloud is not enough to make a difference. This is where businesses can miss out on opportunities**

Maisto adds that cloud migration goals need to move beyond cost-cutting.

Cloud platforms and services do allow firms to move expenses from capital to operation expenditure, so there is some accounting gain. But the case for cost reduction is limited. And as Maisto points out, the "pay-as-you-get dream" can quickly become a "pay-as-you-forget nightmare" – a bit like signing up for a gym membership in January and then realising in August that you've been regularly paying for something which you haven't been regularly using.

In PwC's *2023 Cloud Business Survey*, 78% of those who took part said they have adopted cloud to some level in most or all parts of their business. Yet more than half have not realised the outcomes they were after, such as lower costs, greater resilience and new revenues.

"An IT-centric 'lift-and-shift' approach to moving to the cloud or simply running functions or parts of a business on the cloud is not enough to make a difference," says Warren Tucker, a partner and cloud and digital lead at PwC UK. "This is where businesses can miss out on opportunities."

The lift-and-shift model, which is also known as rehosting, is when a business moves exactly what it is running on its own servers onto cloud services. Traditionally, this has been public cloud via one of the big providers, such as AWS, Microsoft, Google, IBM, Oracle and Alibaba.

According to Dalgas, the thinking around public cloud has shifted. Two years ago, due largely to the pandemic, conversations were mainly around using public cloud services for every workload. Today, that is no longer the case. Businesses are looking at specific workloads and choosing appropriate cloud services to fit. By assessing each workload through a set of metrics, including cost, data sovereignty, security, compliance and so on, businesses can determine the most appropriate route to take.

"Steady workloads work better in private clouds. The economics stack up better," says Dalgas. "But if you are running a project or data processing for just two days a month, very spiky workloads, you will be better off in the public cloud, which is more elastic."

There is plenty of chatter online that this year will be the year of cloud repatriation, with businesses moving away from the large public providers and adopting a hybrid strategy. It's a hangover from the Covid crisis when so many businesses panic-bought public cloud services to enable remote working. The costs of public cloud have since been rising rapidly and, according to Gartner, spending on cloud will continue to dominate IT budgets this year.

With good reason. As Sid Nag, vice-president analyst at Gartner says, inflationary pressures and macroeconomic conditions are having a push-and-pull effect on cloud spending but cloud will continue "to be a bastion of safety and innovation, supporting growth during uncertain times due to its agile, elastic and scalable nature".

This multi-cloud or hybrid strategy – a mix of public and private cloud services – is, according to IDC at least, expected to be the main beneficiary of this line of thinking. In its report *FutureScape: Worldwide Future of Digital Infrastructure 2023 Predictions*, IDC claims that those organisations that can best optimise multi-cloud and hybrid digital infrastructure environments "consistently realise higher levels of operational resiliency, security, revenue growth, and overall productivity at scale". All features prized in times of economic uncertainty.

The actual mix of cloud services will depend, as Dalgas says, on workloads. Factors such as data sovereignty, the kind of data processed and the number and quality of SaaS vendors involved can determine the direction. Whether or not the organisation works in a regulated industry is also a big factor.

Maisto suggests that a hybrid cloud strategy can deliver a certain flexibility to cloud expense management but would inevitably add a layer of complexity to the infrastructure and applications landscape. This will likely come at a cost, he says, so it has to be weighed against the actual savings and functionality gains. A cost-effective cloud strategy will leverage all the opportunities offered by the cloud vendors to reduce costs and will be successful only if cloud costs are carefully monitored.

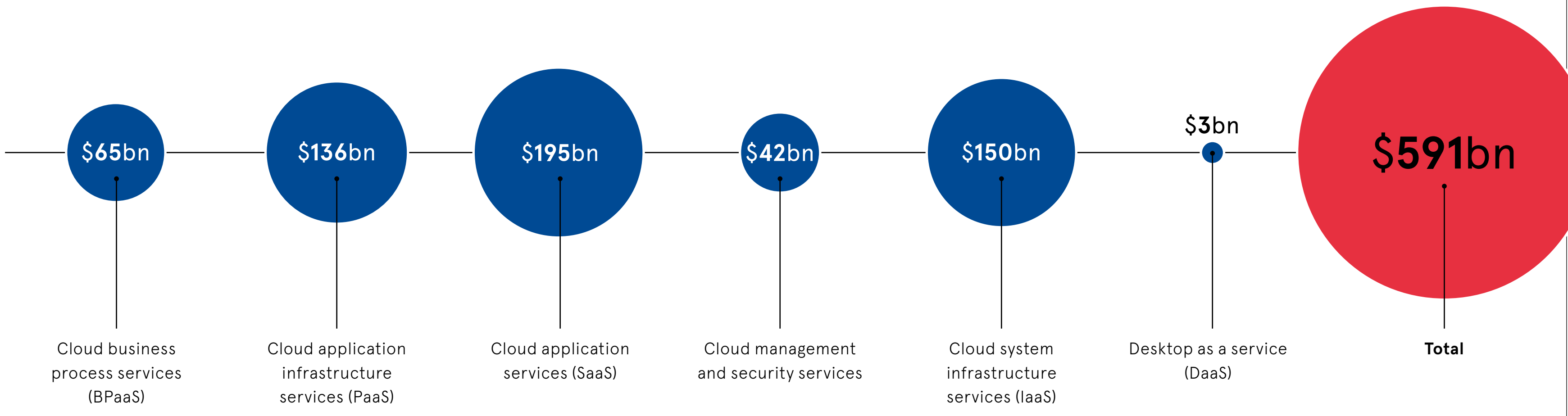
This is where FinOps comes in, which enables organisations to manage their cloud costs more effectively. It also promotes collaboration between finance, tech, and business teams in the public cloud, to drive more accurate data-driven decision-making.

A measured approach will be needed more than ever during difficult economic times. Businesses will be defined by how they balance the desire for automation, IoT devices, increased flexibility in the workplace and multi-channel experiences for customers, with the expense of cloud computing services.

Cloud computing is not the panacea for managing costs during a recession. But, provided it is managed carefully, it will certainly help. ●

THE BILL, PLEASE

Forecast of end-user spending on public cloud services in 2023 worldwide, by service



Gartner, 2022

Distributed in

THE SUNDAY TIMES

Published in association with

techUK FOR WHAT COMES NEXT

CLOUD EXPO EUROPE
8-9 March 2023 ExCeL, London
www.cloudexpoeurope.com

Contributors

Marc Ambasna-Jones
Technology, business and sustainability journalist, focusing on trends. Work published in *The Guardian, Computer Weekly* and *ERP Today*.

Jon Axworthy
Journalist specialising in health, tech, science and the future, with work published in *T3, Wareable* and *The Ambient*.

Mark Ballard
Journalist with 25 years' experience, covering technology, policy, law, business and public affairs.

Francesca Cassidy
Raconteur's deputy editor, specialising in lifestyle and business topics, she contributes to a range of business and consumer-facing publications.

Laurie Clarke
Journalist specialising in technology and science, with work published in *The Observer, The New Statesman, MIT Technology Review* and *Wired*.

Doug Drinkwater
Technology journalist, whose work has appeared in *CIO, CSO, InfoWorld, Macworld, Mashable, PCWorld, SC Magazine, The Week* and others.

Kavitha Nair
Journalist specialising in technology and business of technology, published in *The Times, CIO, The Financial Express* and others.

Chris Stokel-Walker
Technology and culture journalist and author, with bylines in *The New York Times, The Guardian* and *Wired*.

Raconteur

Lead publisher
Chloe Johnston

Reports editor
Ian Deering

Deputy reports editor
James Sutton

Editor
Sarah Vizard

Chief sub-editor
Neil Cole

Sub-editors
Gerrard Cowan
Christina Ryder

Commercial content editors
Laura Bithell
Brittany Golob
Joy Persaud

Associate commercial editor
Phoebe Borwell

Head of production
Justyna O'Connell

Design and production assistant
Louis Nassé

Design
Kellie Jerrard
Harry Lewis-Irlam
Colm McDermott
Samuele Motta
Sean Wyatt-Livesley

Illustration
Kellie Jerrard
Celina Lucey

Design director
Tim Whitlock

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 8616 7400 or e-mail info@raconteur.net. Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at raconteur.net. The information contained in this publication has been obtained from sources the Proprietors believe to be correct. However, no legal liability can be accepted for any errors. No part of this publication may be reproduced without the prior consent of the Publisher. © Raconteur Media

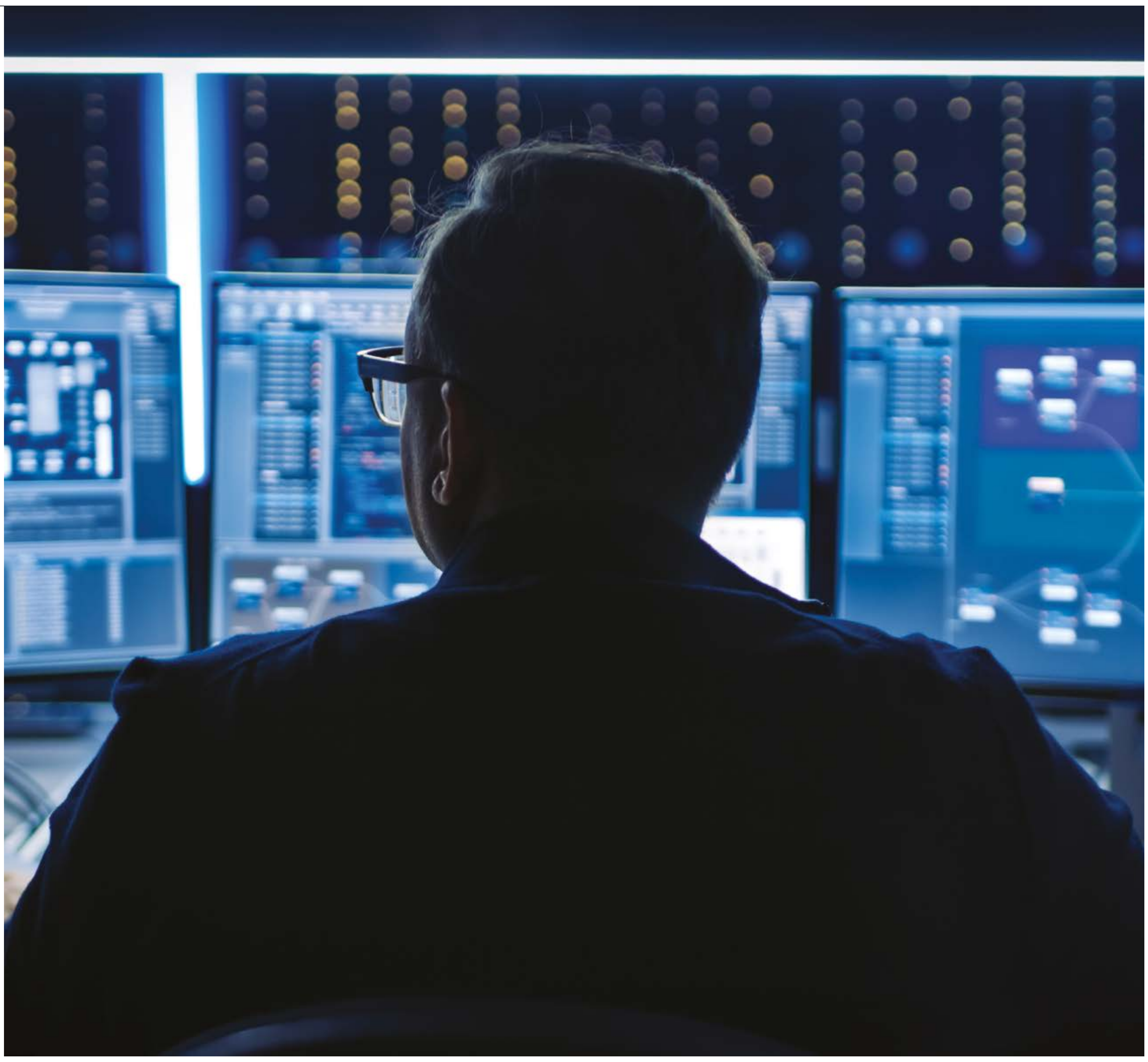
raconteur-media
@raconteur
@raconteur.stories

raconteur.net /cloud-for-business-mar-2023

Commercial feature

Why businesses are moving to managed multi-vendor cybersecurity

Mid-market companies face evolving IT security demands as they advance digital experience, accelerate cloud connectivity and enable disparate remote operations. Given their limited time and constrained budgets, the most effective solution is to bring in managed best-of-breed setups, backed by risk transfer services



As mid-market businesses advance their cloud computing, digital transformation, and hybrid work models, significant cybersecurity challenges are emerging.

For IT departments, the most pressing demand will be to manage and operate an unprecedented array of disparate connected devices, enabling users to access applications and data from branches, stores and field locations and home-working environments. They must also ensure there is a consistent quality of experience, without compromising security.

The problem for these technology teams is they often lack the resources of IT departments in larger corporations. They also face a confusing, extensive array of options when trying to make purchase and deployment decisions. Some respond to this issue by investing in services from a single vendor. This strategy may seem appealing from a management standpoint, but it typically involves using one-size-fits-all systems with limited effectiveness. Others attempt to combine multiple advanced technologies, and become submerged in the expense and intricacy of operating them.

Moving towards insurable setups

"Traditionally, many businesses have been advised by experts to put in a single vendor solution, with the aim being to reduce the integration burden and simplify control," explains Gareth Davies, executive vice-president, managed services at Fulcrum IT Partners. "But this can be very misguided, as the vendor providing them with a firewall is not necessarily proficient at endpoint protection, for example. Moving to a single vendor also involves a significant operational transition that is costly and resource heavy."

Some businesses are instead adopting the best-of-breed approach, choosing the most effective security and business continuity services in each area to achieve the strongest possible protection. However, these systems must be both fully integrated and independently managed on an ongoing basis to keep up with new security threats.

"For many companies, this is far too complicated and costly a challenge, and they will always lag behind the threats that are out there," Davies says. With cybercrime and data breaches becoming increasingly commonplace, companies also need to consider their options for risk transfer. It is essential they put in place cyber insurance to cover financial losses associated with a cyber attack, such as legal expenses, data restoration costs and reputational damage.

However, buying cyber insurance can be a challenge in itself. As a relatively new type of cover, there are many uncertainties and complexities associated with it. Cyber risks are constantly evolving, which makes it difficult for insurers to accurately assess the potential risks and develop adequate policies. As a result, it can be difficult to find an insurer willing to take on the risks associated with a particular business, and many insurers have either backed out of the market entirely or substantially reduced their cover.

> “
> **For companies, demonstrating robust cybersecurity practices can be so difficult that many insurers will simply refuse to provide policies**

"Insurers often rely on simple questionnaires that fail to establish satisfactory insights, leading them to decide they cannot quantify the risks with enough clarity," Davies explains. "For companies, demonstrating robust cybersecurity practices is so difficult that many insurers will simply refuse to provide policies. When insurers do consider approving a client for cyber coverage, it's often not at the price point or offering the level of cover that the customer requires."

The rise of managed services

These dynamics have prompted the rise of more effective forms of managed security, which are capable of addressing the concerns of both mid-market businesses and the insurers seeking to financially protect them. These managed security providers have several core focus areas: implementing best-of-breed security from across different vendors, integrating those services, administering them, providing insights and protecting customers both operationally and financially.

Businesses are increasingly working with managed service providers like Fulcrum IT Partners to ensure they have this level of defence and financial protection.

Fulcrum IT Partners takes a comprehensive approach to protecting all aspects of its customers' cybersecurity, using the most sophisticated technologies and processes in each area, implementing them and managing them. The company also has a strong connection to the cyber-risk transfer market, which means it can demonstrate to insurers the quality and strength of its customers' security posture, enabling businesses to buy the cybersecurity coverage they need at an affordable price.

"It's incredibly challenging for businesses in the mid-market to ensure they have the right levels of protection in place, and to be sure they can recover systems quickly in the event of a breach. We work with our customers to assess their setup, advise on security choices, implement the relevant systems, and then manage the technology on an ongoing basis," Davies says. "We invest heavily to ensure our staff are fully up-to-date with the latest innovations in cybersecurity and emerging threats, so we can better protect businesses."

Secure SD-WAN in practice

One of the first steps Fulcrum IT Partners takes is to implement a managed, secure SD-WAN layer for clients. By adding this virtualised layer to their wide area networks, the businesses become more agile and can unlock cost savings in their connectivity, all while increasing security and observability.

"We offer businesses a secure SD-WAN solution called Titanium, which converges high-performance SD-WAN and virtual, next-generation firewall-security capabilities into a single managed service. This removes the complexity of managing multiple network and security point products, while delivering a secure, optimised network experience across users, devices and applications. And for many companies, this can also unlock the opportunity for some cyber risk transfer and warranty, providing additional protection and peace of mind," Davies explains.

Companies using Titanium by Fulcrum IT Partners often operate highly distributed environments, spanning multiple industries and geographies. They include IVC Evidensia, a major veterinary-care provider, whose rapid expansion had led to a complex setup. Migration to a managed, secure SD-WAN solution enabled the introduction of effective multi-layered security, reduced costs and improved application effectiveness and control. Similarly, with the help of Fulcrum IT Partners's managed secure SD-WAN service, Sense, a charity supporting people living with disabilities, was able to upgrade its network and reduce operational bottlenecks, all while strengthening and integrating advanced security.

For mid-market businesses, although there is no silver bullet to protect against the ever-growing array of cybersecurity threats, there are some highly innovative response services available. With new approaches to layering security with SD-WAN technology, backed by strong access to relevant cyber insurance, companies can protect their business operations and data from an evolving threat landscape. And they can do it in a way that is both simple and affordable.

To find out more about managed multi-vendor cybersecurity, with embedded risk transfer services, visit fulcrumtitanium.com

TITANIUM
BY FULCRUM IT PARTNERS

Q&A

The evolution of SD-WAN

The advancement of SD-WAN services has enabled effective edge security, says **Gareth Davies**, executive vice-president, managed services at Fulcrum IT Partners

Q **What is driving the adoption of SD-WAN?**

A Managed, secure SD-WAN is becoming increasingly popular among businesses because it can provide improved network security, scalability and flexibility. Companies gain an extra layer of protection against cyber threats, while also being able to easily scale networks as their needs change.

Until very recently, many mid-sized businesses might not have considered themselves as a target for cyber criminals, yet they often are. At the same time, the complexity of risk mitigation and product management is greater than ever. A managed secure SD-WAN service reduces this complexity by providing a unified, centrally managed platform that allows safe and reliable access to distributed applications and data across the enterprise.

Q **What have been the key stages in the technology's evolution to this point?**

A SD-WAN emerged as a way to deliver reliable and cost effective connectivity, but has now evolved to be an essential part of securing the edge, including for remote workers. Companies use secure SD-WAN for all forms of connectivity at all their sites, connecting users to applications, and ensuring optimal performance, uptime and resilience across the network.

SD-WAN also provides the critical foundation of secure-access service edge (SASE). This network architecture supports cloud-enabled organisations by combining SD-WAN with additional network-security features – such as zero-trust network access and automated enforcements like cloud-access security brokers and secure-web gateways – into a single cloud-based offering. It provides consistent security and access to all cloud applications, so organisations simplify management, improve visibility and maximise network protection across users, devices and applications.

Q **How do you work with companies to overcome their security challenges?**

A We understand that every business has its unique set of challenges and objectives. We take a consultative approach to engagement to ensure we fully understand what the challenges and desired business outcomes are, before designing and implementing a solution that supports those needs now, but is also flexible enough to support future growth opportunities.

When it comes to cybersecurity, business leaders need to ensure they have all the right levels in place. The services we provide allow companies to reduce the complexity of network and security management, so they can free up critical resources, time and energy for mission-critical pursuits.

Q **How can you help IT leaders answer the important questions they get from the C-suite on cybersecurity?**

A We don't believe businesses are getting the best outcomes and value from their security investments. At Fulcrum IT Partners, we aim to change that by providing a service that brings together the required expertise and best-of-breed technologies that help IT managers to implement effective protection.

This means they can also accurately report to the chief executive and the chief financial officer on cost and effectiveness. By implementing robust observability measures, organisations gain timely insights to evaluate their spending and make informed decisions on system changes, thereby optimising their operations and maximising returns. Our services are also unique in that they are backed by risk-transfer services that offer operational and financial cyber resilience.

> “
> **We don't believe businesses are getting the best outcomes and value from their cyber security investments. We aim to change that**

Q **What lies ahead for companies' cybersecurity strategies?**

A While threats are constantly evolving, so too is the ability to protect against them. Companies are taking smart steps to advance their security. They recognise they no longer need to be the experts in each domain or have the capacities to constantly update and advance systems. Modern IT teams have a far greater responsibility in contributing to wider business goals.

By bringing in security specialists who integrate best-of-breed solutions across their operations, backed by risk-transfer services, companies are protected against threats, mitigating the damage from breaches and positioning themselves for effective business continuity. This allows them to focus their resources on other business priorities and gives them the peace of mind that their network and data are secure.

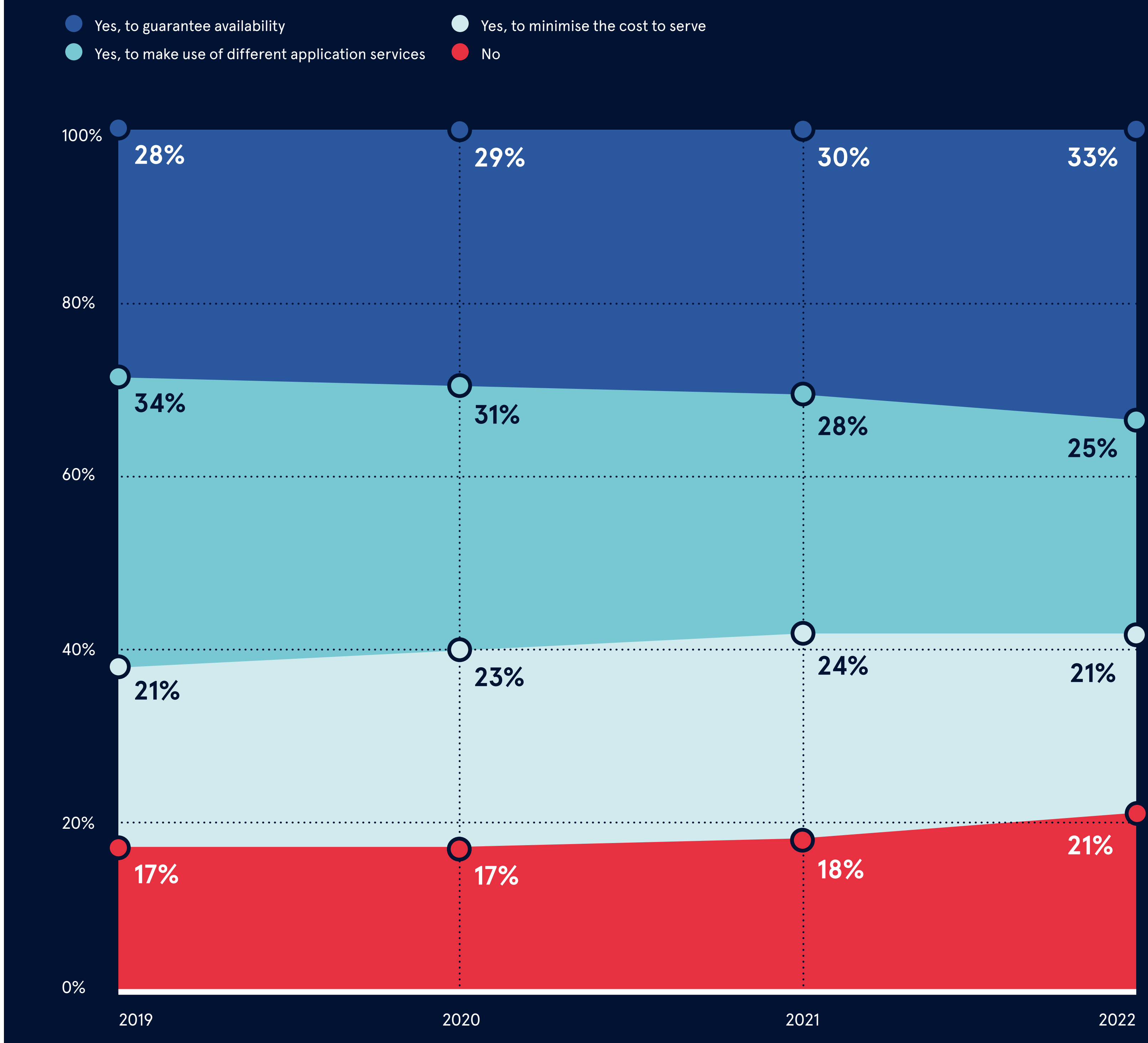
HYBRID CLOUD ENVIRONMENTS

Although a few businesses are still in the early stages of migration, most have become comfortable with using cloud services and are benefiting significantly from doing so. Now that the growing pains have passed, companies are refining their strategies. Many have opted for hybrid arrangements combining public and private cloud facilities with on-site storage. What are the pros and cons of this approach?

EXPECTATIONS FOR CLOUD FLEXIBILITY

Turbonomic, 2022

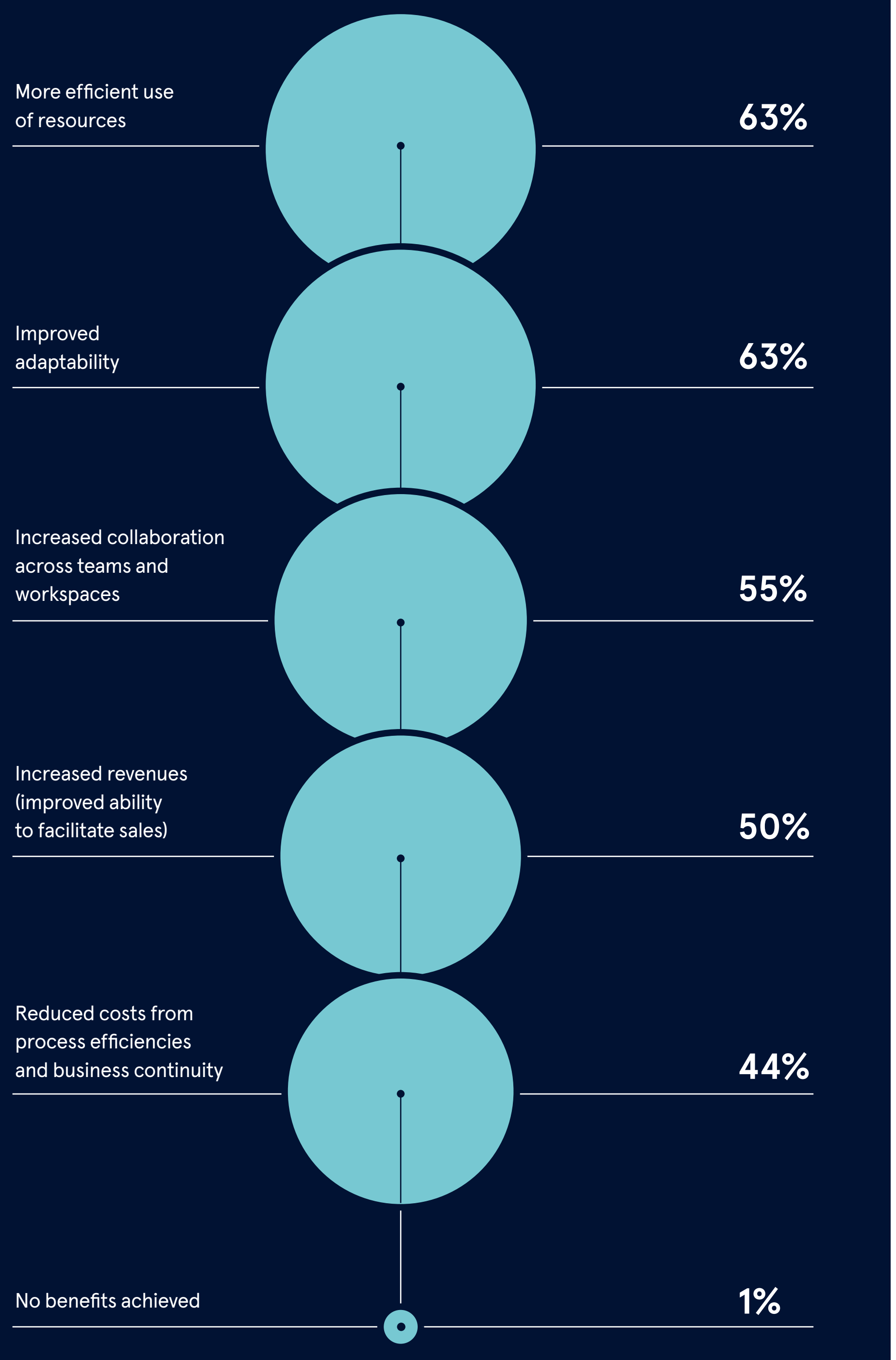
Percentage of IT professionals giving the following responses to the question: do you believe that applications will one day move freely between clouds?



HOW ARE BUSINESSES BENEFITING?

Microsoft, 2022

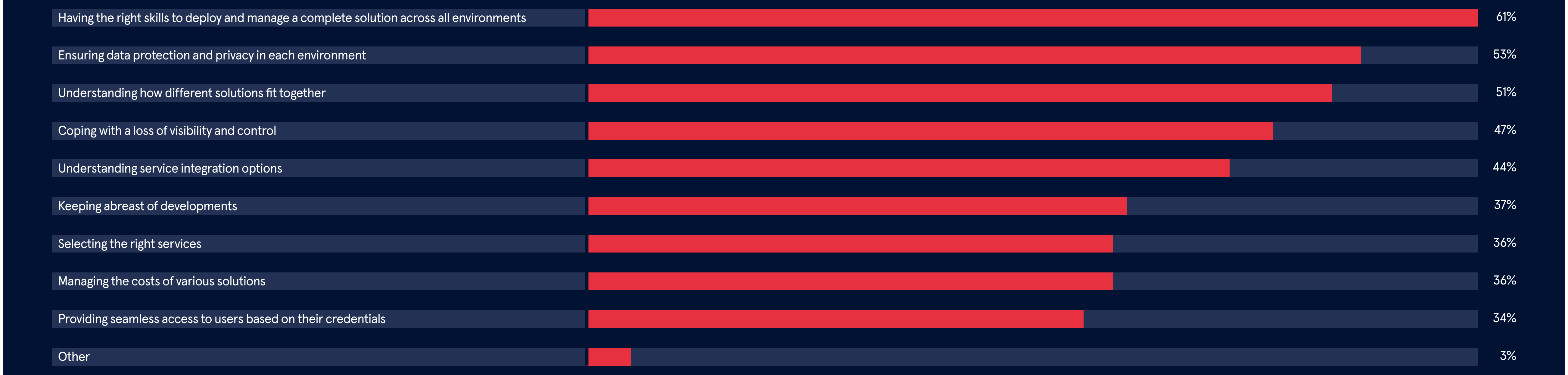
Percentage of firms worldwide citing the following outcomes from adopting a hybrid or multi-cloud approach



DOES THE HYBRID MODEL PRESENT A CYBERSECURITY HEADACHE?

ISC2 Foundation, 2022

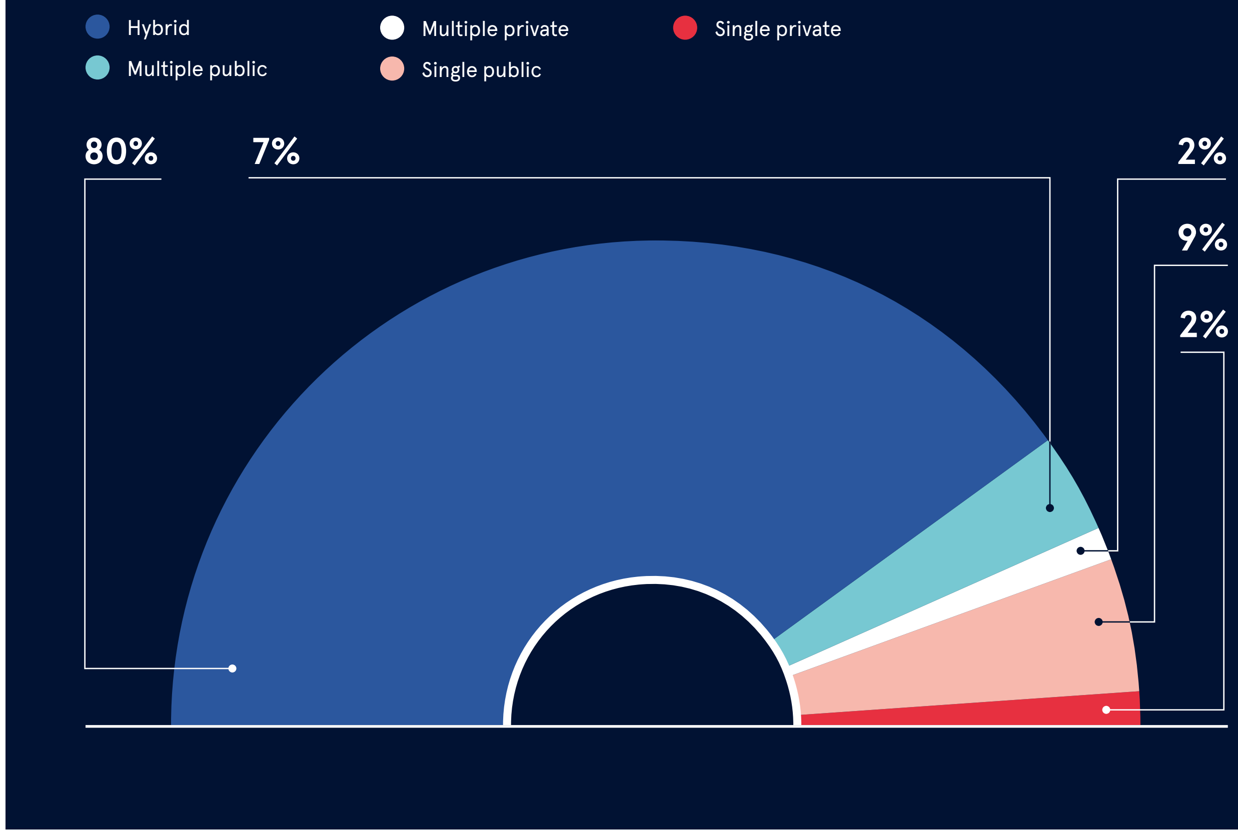
Percentage of cybersecurity professionals citing the following issues when asked: what are your biggest challenges in securing multi-cloud environments?



THE HYBRID OPTION HAS BECOME THE STANDARD

Flexera, 2022

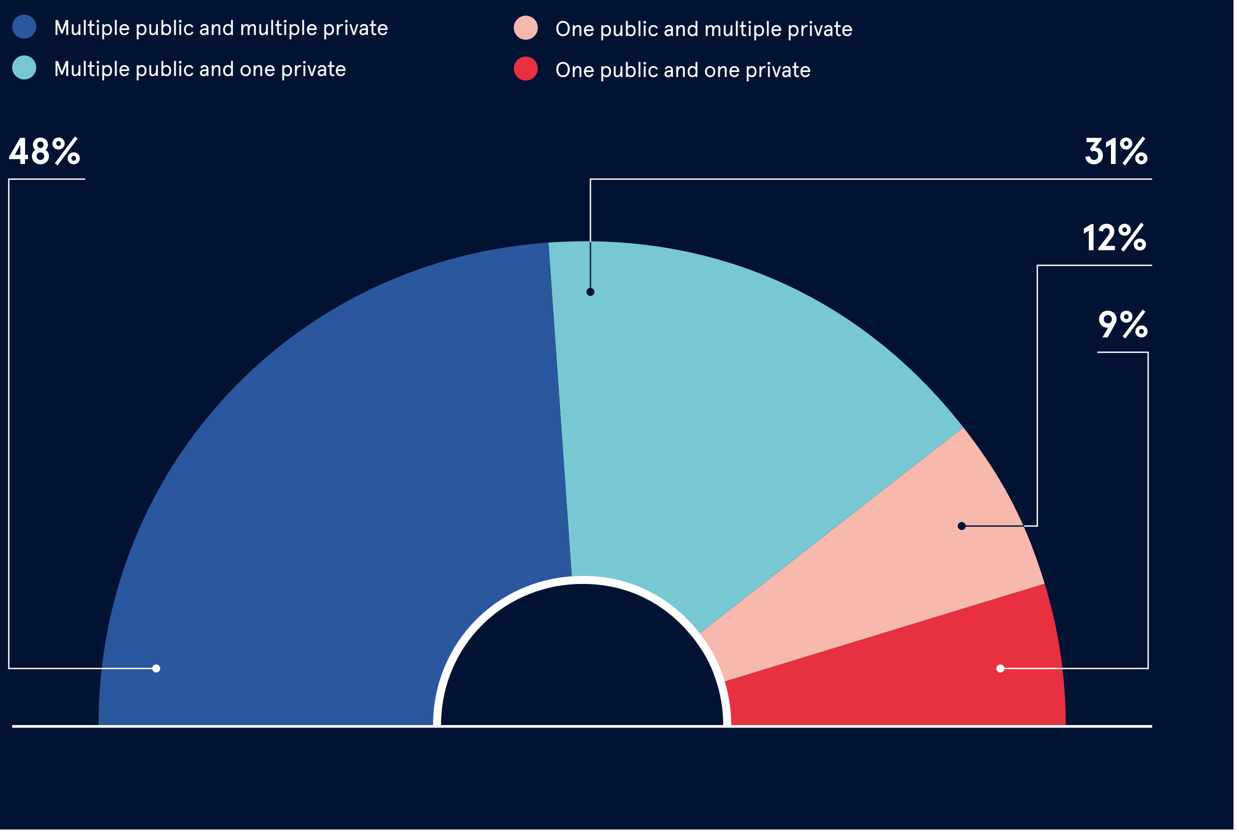
Percentage of organisations worldwide citing the following as their chosen cloud models



HOW BUSINESSES ARE STRUCTURING THEIR HYBRID ARCHITECTURES

Flexera, 2022

Percentage of hybrid cloud users worldwide citing the following as their chosen models



STR/NurPhoto via Getty Images

POLICY

What digital sovereignty means to the UK

Some states have taken such strong measures to impose their sovereign power over the internet that it has created a reckoning among global powers. Brexit threw the UK right into the centre of the argument

Mark Ballard

The UK's digital legal regime has been uncertain since it left the European Union, with a reform of the landmark EU privacy law stalled in parliament, and numerous regulatory reviews and proposals underway.

Tech firms have called for clarity, and expressed fear that the government will make the UK into such a maverick regime that they will be blocked from doing digital business overseas.

The UK took a markedly transatlantic stance in reforms it began last year, and in digital trade negotiations it has been participating in around the world.

Europe's GDPR, widely celebrated as the gold standard in privacy, has already influenced legal reforms across the globe, from Brazil to India, Rwanda to South Korea. Some US states are even taking cues from European standards.

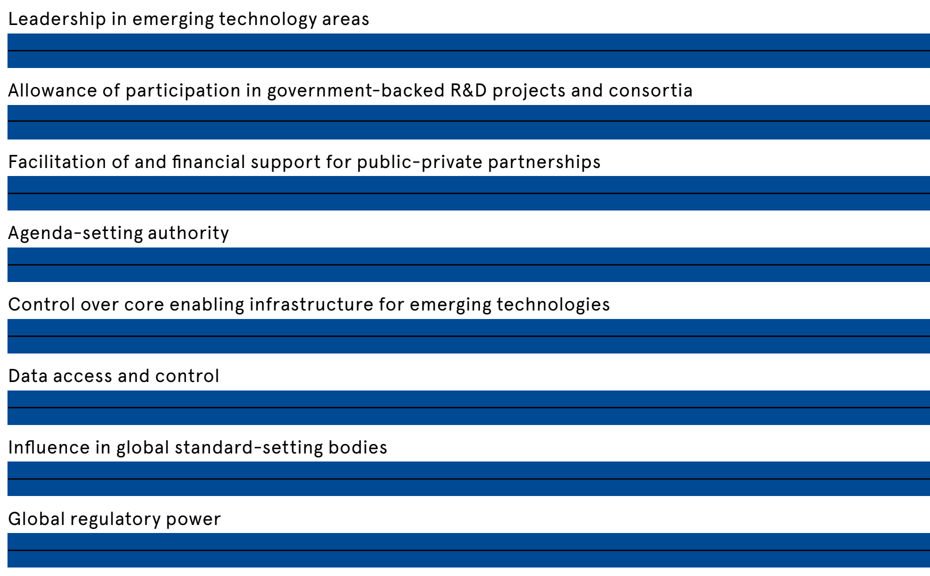
Commentators say this was the aim of Europe's digital agenda: to assert its digital sovereignty by drafting laws to protect individual human rights in cyberspace and to project them around the world.

For the UK meanwhile, Brexit had been its own act of digital sovereignty, says Sarah Pearce, a partner in global privacy and security law with Hunton Andrews Kurth. By separating data law from the EU, the UK has taken active ownership of it.

UK tech firms have been both worried and encouraged by the draft bill that followed that separation: the Data Protection and Digital Information Bill. Phil Bindley, director of cloud computing at UK-based Intercity, says his business has been left guessing about how the proposals will affect it.

HOW DOES THE EU PROJECT ITS DIGITAL VALUES AROUND THE WORLD?

Share of European tech professionals ranking the following among the EU's top-three instruments to advance the bloc's objectives for tech in global affairs



The draft bill promises a "bold", extra-EU data regime that will be "pro-growth" and designed to make it easier for companies to innovate with the use of data.

Nevertheless, says Bindley: "The regulatory uncertainty is a sword of Damocles hanging over our heads. It's very difficult to make strategic decisions."

Bindley says GDPR brought the realisation to many businesses that the data they hold isn't theirs. "You are the custodian of it. GDPR was a great step forward," he says.

Regulatory uncertainty had since suppressed UK innovation and growth, Chi Onwurah, the Labour Party's shadow minister for science, research and innovation, told a conference of software engineers in February.

The Conservative government's tech policy lacked ambition and was "wholly inadequate", she said, because it treated regulation as a barrier to innovation and growth. She went on to explain that regulation actually created growth, because it gave people trust in technology, which brought tech firms more users. And more users brought more investors.

Yet Matt Peake, policy director for Onfido, a global UK artificial intelligence software firm, points out the dangers of overly stringent regulation.

"GDPR can act as a break on innovation and a chill on investment. There are a lot of hoops and hurdles to go through to generate new products," he comments.

For all its good points, "it can be over-restrictive, highly burdensome, quite costly to comply with and goes beyond what it needs to protect user data," he says.

Onfido had been trying to use its customer data in innovative ways, but repeatedly found that EU rules make it "really, really difficult". It had tried to build new services for its customers in financial services and found they were afraid to use them for fear of being prosecuted.

But Peake also worries that the UK will diverge so far from GDPR that it will lose its adequacy in EU law. A formal EU adequacy decision in 2021 granted EU and UK firms permission to share data because post-Brexit Britain had not diverged from the data statute it inherited from the EU, but this decision could be reassessed.

"We need to process data all over the world with minimal restrictions. The risk is we take a data sovereign approach and it becomes harder," says Peake. He fears a global fragmentation of data flows.

Eve Maler, chief technology officer of identity software firm ForgeRock, believes the world is entering an Era of heavy regulation of AI and data and is also concerned about the impact. "It can be an overwhelming burden," she says. "I'm concerned with crushing innovation." She thinks the government should leave the market to innovate choice for users, and keep regulation to defining broad principles of behaviour, which should be stated in the negative.

> **The regulatory uncertainty is a sword of Damocles hanging over our heads. It's very difficult to make strategic decisions**

Commercial feature

Why cloud repatriation is a 2023 priority

Companies' long-established dependence on public clouds has recently declined, due to spiraling costs, security problems and outages. Businesses across sectors and geographies are reconsidering private dedicated infrastructure to host their key applications

For well over a decade, businesses of all sizes have steadily placed their digital systems onto platforms run by large cloud providers. Everything from CRM and data storage, to new applications and analytics, have ended up on the servers of major cloud providers, which are shared between multiple businesses.

While executives often have strong expectations about saving money and ensuring elastic scalability, the realities of using public cloud services can be more complex. In many cases, businesses endure spiking costs, unexpected add-on expenses, security problems and little influence over the technology being used. A recent outage at one of the world's largest cloud providers even saw thousands of businesses' core email and collaboration systems go offline for several hours.

"The buzz around public cloud provision has been really big, and to some degree that's understandable given its scalability. But businesses rarely understand what they are actually getting into," explains Jake Madders, co-founder and director of managed hosting provider, Hyve.

Typically, migrations to the public cloud are kicked off by well-intentioned developers, who see its capacity to support important and growing applications without having to buy new servers. But prices are rising as the number of providers in the market dwindles. Companies also experience 'bill shock' when they have surges in network traffic, which can happen for reasons as diverse as a successful marketing campaign and a DDoS security attack.

There is another hidden cost. "Typically, businesses moving to the public cloud quickly find they need consultancies to help them manage the technology on a daily basis, given the complexity of choices in front of them at every stage," Madders notes. "These consultancy costs often equal or exceed the actual cloud provision costs."

Such challenges have prompted many businesses to rethink their approach. "There has been a strong trend towards cloud repatriation, which means pulling the data and apps out of the public cloud, and back into controlled, secure private cloud setups," explains Madders. Private cloud gives businesses their own managed, dedicated servers, stronger security, better disaster recovery and backup options, consistent support and much more control over costs and technology choices.

> **The private cloud empowers businesses in mission-critical areas, massively increasing capabilities and efficiencies**

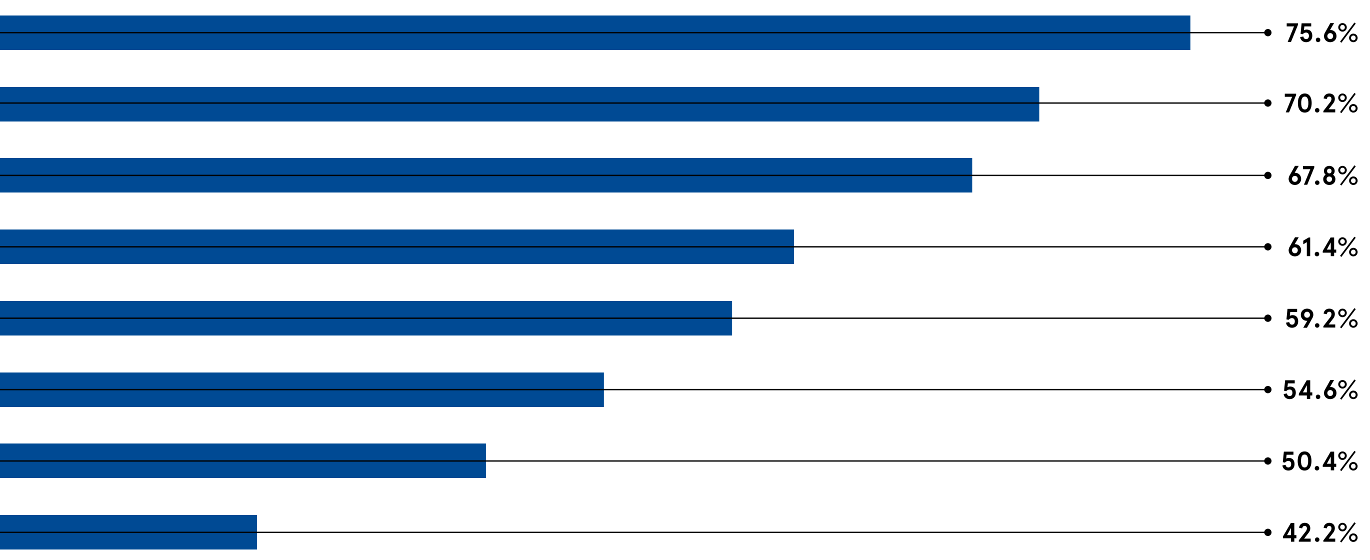
With Hyve's help, businesses are choosing and running powerful, cost-effective and secure private clouds that meet local needs, including around low latency, data sovereignty and on-the-ground support. "Choosing servers, processing power and myriad other options is incredibly complex, particularly from a cost and performance perspective," Madders says. "Companies come to us to help with the critical decisions so they make the most effective choices."

Hyve also provides ongoing managed-support services, which help customers run their private clouds from day-to-day. Madders adds: "When a business needs to discuss its setup, change anything, or spin up capacity, the executives know they can speak to the same experts each time, who already know them, and they won't have to explain themselves over and over."

Companies including Côte Brasserie, PureGym, NHS Queen Victoria Hospital and Capita have all made significant changes to their IT setups with the help of Hyve. The restaurant chain Carluccio's also partnered with Hyve to improve reliability and security across its systems as it upgraded its website, table bookings and online shop. Meanwhile, the self-storage business Safestore brought in Hyve to underpin the growth and reliability of its website, through which around 80% of its business is consistently derived.

Increasingly, businesses are counting on Hyve to meet multiple critical needs. The company is now active in over 35 markets worldwide, and is expanding rapidly in the US and Germany. "As businesses look to retake control of their cloud infrastructure, moving away from a reliance on a single provider, they are turning to the private cloud," Madders concludes. "Doing so empowers them in mission-critical areas – including high-performance computing and artificial intelligence – massively increasing their business capabilities and efficiencies."

To find out more about moving to a powerful, cost-effective private cloud, visit hyve.com



German Council on Foreign Relations, 2021

In an October 2022 edition of the *Maastricht Diplomat* podcast, Margrethe Vestager, the European commissioner responsible for data, AI and social media, stressed that choice is an aim of the "digital agenda" by which the EU has been extending its digital sovereignty.

The energy and commodity shortages that have followed Russia's invasion of Ukraine have exposed clear vulnerabilities in the EU's dependence on Russian fossil fuel and Ukrainian minerals.

The EU's sovereignty push, which strove beyond data privacy to build indigenous cloud and chip industries that could rival those of US and Chinese firms, likewise strove to reduce the EU's dependence on sole foreign suppliers.

But Europe's digital sovereignty project has drawn comparisons to authoritarian regimes such as China and Russia. It has also attracted criticism from the White House, which lobbied against elements of the EU's proposals.

Europe insists that it seeks not separation but a competitive market that brings choice of technologies. Western countries, citing fear of foreign interference, have meanwhile stopped Chinese tech firms from dominating communications infrastructure within their borders, and blocked Russian misinformation in digital media.

Choice aside, Suki Dhuphar, head of EMEA at software firm Tamr, believes innovations in EU government data processing are held five to 10 years behind China and the US by heavy regulation.

"Rightly or wrongly", China's advanced handling of data, such as issuing automatic fines to jaywalkers, set an example. UK reforms would ease rules on police data processing, but such innovations are being challenged in EU courts.

Widespread mistrust of the internet was apparent in conversations that Joe Baguley, EU chief technology officer of cloud software firm VMware, has had with government officials around the world, and with executives from all sectors of industry.

Government officials have increasingly asked Baguley for his advice on building sovereign cloud-computing systems within the borders. Their motivation is to ensure that the most sensitive data isn't stored in some other country where foreign governments might interfere with it.

The UK made combating such fears one of the main thrusts of its post-Brexit digital policy. Declaring mistrust a risk to global trade that could be resolved only by the recognition of common data-privacy rules in international forums, it pursued agreement on "global trusted data flows" in the OECD and G7 clubs of democratic nations.

In December, it struck a trade agreement with Japan, which had been striving for a common global data adequacy. This issue was also on the agenda of talks which the UK and US opened in January.

Trust was in the spotlight again – after the US wrote into an adequacy agreement with the EU a capitulation to various long-standing demands for checks on US interference in cyberspace.

> GDPR was a moment of awakening for a lot of businesses, a realisation that the data you hold is not yours

Their agreement sought to heal mistrust that stemmed from the infamous Snowden revelations that the US, hunting for terrorists, had tapped the world's internet traffic in ways that federal law forbade it from doing to its own citizens. The US relinquished some of this sovereign power it had assumed over the global internet.

The OECD, where the UK took its effort to establish a "pro-growth and trusted data regime", turned the US intelligence reforms into a pledge by which other countries said they would pursue the same course.

The Covid outbreak exposed how severe public distrust was in the internet when it emerged that people in minority, vulnerable and disadvantaged communities withheld data from health authorities for fear it would be used against them by other agencies with nefarious intent.

In reality, the laws underpinning the EU's digital agenda were never about sovereignty. They were only an attempt to restore people's trust in cyberspace, so that digital trade and firms could thrive. This point was made by Werner Stengg, one of the architects of the EU laws in Vestager's office, in a webinar by The Atlantic Council, a US think-tank, in November.

Software firms celebrated UK proposals to pare back the EU rules, which would allow personal data troves to be used for research and development, and soften permission requirements around data use.

The UK data regulator made the first step, for the sake of innovation and growth, by allowing firms to decide when, where and how it was safe to trade data with foreign regimes based on a mere risk assessment, instead of detailed and onerous comparisons required by the EU. ●

INSIGHT

'The cloud presents fantastic opportunities for sustainability in a climate-conscious world – but not without your help'

Stuart Crowley, editor, Techerati.com, explains why every stakeholder across the cloud value chain must be involved in the push for sustainability

Undeniably, the climate crisis is one of the most pressing issues faced by the global community. For world leaders, the topic received top billing at the World Economic Forum this January, while for business leaders there is an expectation that more and more money be put into sustainability initiatives.

Tech companies invested £44.6bn in clean power last year, which is more than any other sector according to a report by the American Clean Power Association. And for pioneering minds, the climate crisis presents opportunities to spearhead green innovations in the race against the 'Doomsday Clock'.

The adoption of cloud and cloud-enabled technologies like AI and machine learning has accelerated since the pandemic. During that time, promises of cost savings, flexibility, scalability and remote adaptability made cloud the newest essential business and workplace technology. We later started heard about what cloud can do for sustainability – 77% fewer servers as a direct result of resource sharing, 84% less power consumption and 88% reduced carbon emissions compared to legacy data centres. In almost every new data centre announcement, you'll see companies highlight their use of renewable resources and pledges for net-zero emissions.

Most business leaders recognise the cloud's potential for advancing sustainability, but the benefits can be obscured by some metrics. For example, when migrating to the cloud, there is a lot of electricity-intensive processing involved. And while firms may see reductions in scope-one emissions, those difficult-to-observe scope-three emissions could potentially increase your company's carbon footprint, since you cannot control where your cloud provider sources their energy.

But this should serve as a reminder: we must not lose sight of the progress that still needs to be made and the opportunities available to help our industry lead the charge for a sustainable future.

As end-users, there are ways to reduce energy consumption by optimising cloud usage through data deduplication, compression and auto scaling. Running virtual machines from a single server, making use of container technology and considering serverless innovations also have the potential to reduce carbon emissions if they are optimised and closed down when not in use.

Public cloud giants like Microsoft Azure, AWS and Google Cloud are also adding tools for customers to gain more transparency about their own usage and their providers' data-centre emissions. However, it remains the responsibility of end-users to lobby for continued investment in sustainable solutions by their cloud providers, and partner with policymakers to progress sustainable development commitments. Every business leader should devise internal policies on responsible cloud usage and sustainable disposal of obsolete data, as well as ensuring the environmental policies of cloud providers are a good match.

All stakeholders in the cloud computing space should also start preparing to get involved in the circular economy. Firms are looking for ways to design out waste and pollution, reuse resources and establish end-to-end transparency from supplier to consumer. No matter the industry or buying power, businesses can be more conscious of their buying decisions. The more ambitious can even partner with companies to investigate how technology like AI can help to drive new insights for better product design and sustainable development.

We are at a critical point in the battle against climate change. We all have a responsibility to help leave the world in a better state than our predecessors did. There are boundless opportunities for the tech sector to lead the way. With the ubiquity of cloud technology, embracing sustainable usage and advocacy is a critical decision that business leaders should not overlook. ●

CloserStill Media's Tech Show London on 8-9 March at ExCeL London. Get your FREE ticket for access to all five shows: Cloud Expo Europe, DevOps Live, Cloud & Cyber Security Expo, Big Data & AI World, and Data Centre World. Register at techshowlondon.co.uk

Stuart Crowley
Editor, Techerati.com

Risk and reward: how do insurers identify strategic value in the cloud?

The insurance industry is well-versed in the intricacies of risk management. Increasingly, the sector is embracing cloud technologies to navigate volatility, drive growth and build greener businesses

By now, businesses are no stranger to recovery and reinvention. Preparing for tomorrow's economic and geopolitical disruptions is part and parcel of good governance and requires organisations to prioritise resilience.

Everything from weathering the recession to addressing climate change begins with insightful, decisive leadership. Without it, businesses risk being at the mercy of events rather than rising to the challenges they present.

Few sectors understand this principle better than insurance. Indeed, protecting companies, governments and communities from increasingly unpredictable global shocks is the industry's bread and butter. But even for insurers, adversity has made meeting client expectations and shareholder demands more pressing - and more challenging.

Robust cloud operations have become essential for establishing efficiency, flexibility and resilience and helping insurers navigate geopolitical tensions and global shocks. When executed well, they have the potential to streamline the process of developing and pricing new products giving leaders the confidence to enter new markets, despite rife uncertainty. But, while the world might be especially volatile right now, there are exciting growth opportunities too.

Peter Phillips is the president and CEO of Aon's PathWise Solutions Group within Aon's Strategy and Technology Group, which offers a GPU SaaS enterprise solution for life insurance companies for reporting, hedging, new product development and pricing of structured reinsurance solutions. He believes that now is the time for insurers and reinsurers to embrace the agility and resilience the cloud yields to capitalise on these opportunities through better and more timely business intelligence.

"Management's need to understand what's happening around them to make better decisions has never been greater … and the cloud plays a key role in managing complexity and improving decisions and outcomes for businesses in a cost-effective manner," says Phillips.

Advanced data analytics, powered by the cloud, provides insurers with a deeper understanding of their portfolio mix, allowing them to adjust their business strategy quickly and deploy or reallocate capital more effectively. Accurate data drawn from every area of the business that is centrally available for instant analysis can also help the C-suite identify and resolve inefficiencies that may otherwise restrict growth while extracting actionable insights at speed and scale.

"In the life insurance space, users are able to interrogate their data warehouse and think about the next generation of products using modern technology like green GPUs, which use a seventh of the power versus conventional CPU-based cloud solutions and also offer a material speed up in computation time," Phillips continues.

For insurers, modelling tasks have understandably grown more complicated in recent years. "There's greater climate volatility, for example, and people want better management information (MI) to respond," says Alun Marriott, technology chair of Aon's Strategy and Technology Group. "As computational power has increased, the cloud helps insurers access this power efficiently without the inherent economic and environmental costs associated with on-premise data centres."

> It's far more efficient to only commission the resources you actually need rather than leave kit unused in your own data centre

Catastrophe modelling has taken a giant leap forward in recent years; artificial intelligence can provide insights that would have been impossible in the not-too-distant past. "A satellite can now fly over a town hit by a hurricane, and an AI engine can work out the resulting damage to property," says Marriott. By sharing cloud hardware, insurers can accelerate their response to those affected and offer meaningful, timely support.

"The cloud allows companies to embrace better and faster technology that would otherwise be out of reach to them," Marriott says. "That gives them access to better MI, better decision making and better support for their customers."

Through advanced modelling, analytics, automation, and hedging simulations, Aon's PathWise platform uses powerful, scalable parallel GPU processing to improve organisational workflows and cut complex life insurance calculation times down from days to a few hours or minutes. From a growth perspective, automating routine tasks through cloud-enabled machine learning tools frees employees to dedicate more time to activities with tangible strategic value.

Thankfully, transferring operations from on-premise to the cloud or shifting to a new SaaS solution has also become more efficient. "While in days gone by you'd have to recode everything from scratch, nowadays templates and workflow tools can help you automate the conversion and reduce the cost of onboarding a new solution," says Marriott.

Once the switch has been made, insurers need only pay for the storage and computing power they need to perform certain tasks. "It's far more efficient to only commission the resources you actually need rather than leave kit unused in your own data centre," he continues.

By reducing the vendor lock-in that often goes hand-in-hand with legacy systems, insurers can also integrate tools from different suppliers with minimal fuss. "It's a more integrated network of components," says Marriott, "and that allows you to scale up and scale down as the business changes, so firms can enter new markets and also leave markets in a more measured and dynamic way."

However, he also notes that, in some ways, spending money comes all too easily within a cloud-based environment, so the C-suite must have a clear understanding of precisely where the cloud adds value. "You can add on servers and capability very easily, so you've got to be much more careful about controlling what you buy and why you buy it and then reducing capacity if warranted," says Marriott.

Phillips outlines the questions that decision-makers must ask themselves before financing cloud infrastructure: "What are the cloud costs? How does it map back to the strategy? And who are the service and solution providers with deep experience that they can really partner with companies to obtain these cloud efficiencies?"

Beyond a company's growth goals, reducing the demand on data centres also generates substantial energy savings, keeping organisations on track to meet their ESG ambitions. For example, Aviva is transitioning its life model to the Tyche platform. The anticipated speed and efficiency gains from the switch will allow the insurer to permanently reduce the number of servers it uses.

Meanwhile, Zurich Insurance has minimised its physical hardware by adopting Aon's ReMetrica Cloud Solution. The global insurer's catastrophe reinsurance model requires substantial computing power to run but is only operational at set times each month. After considering various infrastructure options – including upgrading its internal hardware – it now deploys the service on-demand. Zurich is only charged when it uses additional cloud capacity to run its model, and simulation time has been drastically reduced.

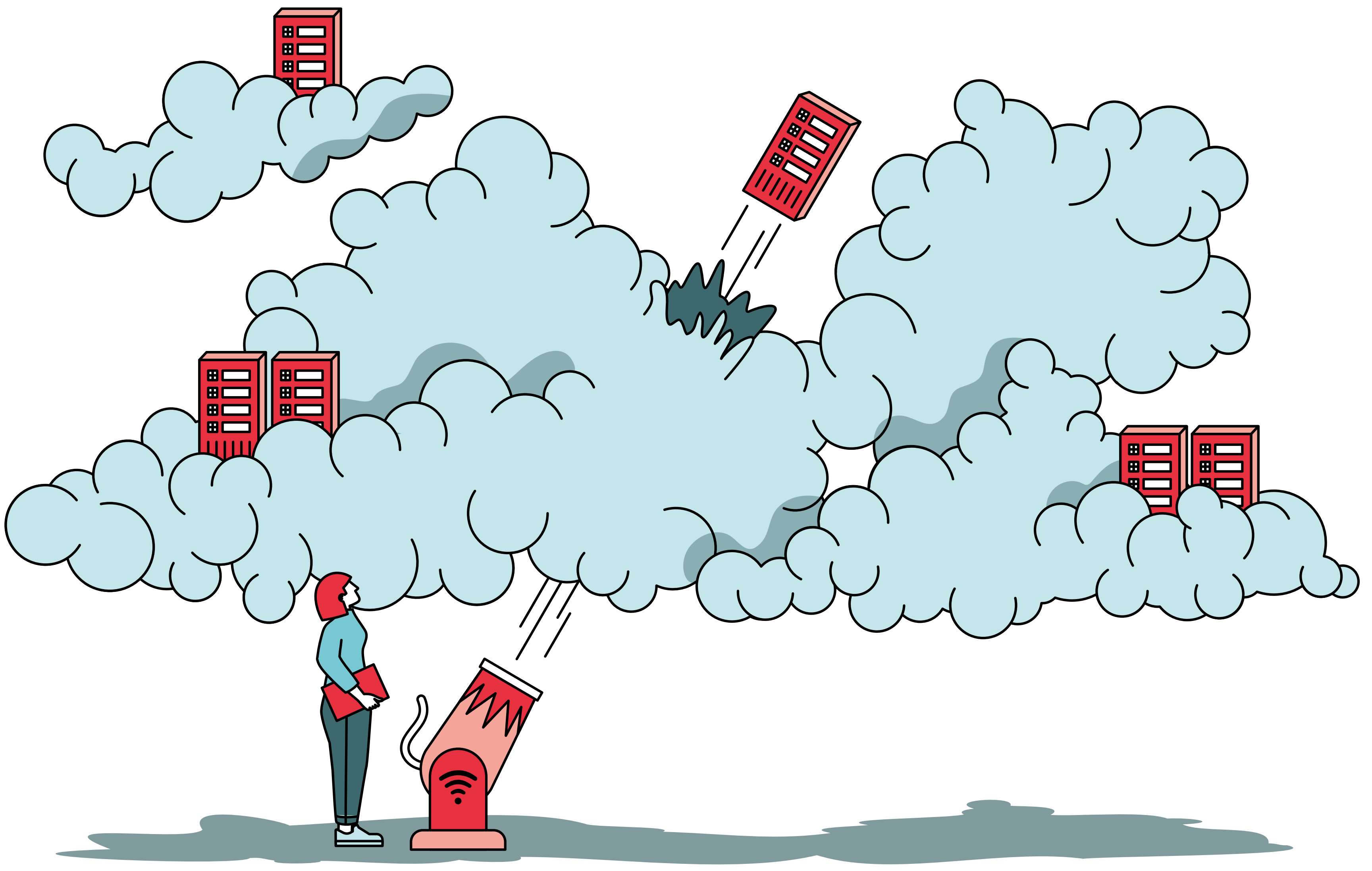
In other words, the cloud offers insurers a platform for meeting their green goals while supporting resilience, cost and efficiency gains. And the benefits reach far beyond the insurance industry, impacting businesses, governments and communities that need protection in a fast-changing world.

CONTINUITY MANAGEMENT

Fit to burst

Cloud bursting – whereby firms shift some of their processing workload to a public cloud when demand is rocketing – is becoming a popular way to ensure service continuity at optimal cost

Jon Axworthy



For many digital businesses, the ability to handle huge increases in demand – from the rush to an etailer's site on Black Friday to the Saturday night stampede for meal delivery services – is key to their ongoing competitiveness.

To cope with the extra burden, these firms often look to divert some of the data processing workload from their own systems to a public cloud service. But the fact that the spikes in demand are temporary means that they won't need that additional capacity permanently – and they definitely won't want to pay for it. This is where cloud bursting, an application deployment method first proposed by Jeff Barr, chief evangelist at Amazon Web Services, comes into play.

An adaptation of the hybrid approach, using both public and private clouds, it enables IT teams to set workload thresholds for their own systems and applications. When such a threshold is reached, the cloud bursting configuration will trigger an application to start working in a public cloud, where it can more easily cope with the increase in traffic coming its way.

"Cloud bursting offers evident advantages to businesses in terms of cost, flexibility and service continuity," says Ravi Mayuram, CTO at cloud database platform Couchbase. "First, you pay only for what capacity you use, avoiding fixed overheads. Second, resourcing can be much more flexible: you scale back once the need goes away. And third, cloud bursting means that applications and services can continue operating during demand peaks (or at other times) without negatively affecting the user experience."

> The challenge is to plan for adequate networking bandwidth between private data centres and the public cloud, so that bursting actually happens effectively

Although dealing with workload spikes is its main application, cloud bursting can be utilised for processor-hungry modelling tasks such as 3D rendering, or in software engineering, where running virtual machines can become prohibitively costly. Bursting into a public cloud also gives users access to tech that's often optimised for big-data analytics and AI tasks.

Sounds attractive, doesn't it? Especially as there are established container environments that natively handle cloud bursting. But there are some caveats and preparation is needed before adopting this approach.

First, a company must look closely at each application to determine whether bursting it would be feasible in its current state. This will often boil down to how an application has been designed, notes Steve Judd, senior solutions architect at the Jetstack consultancy.

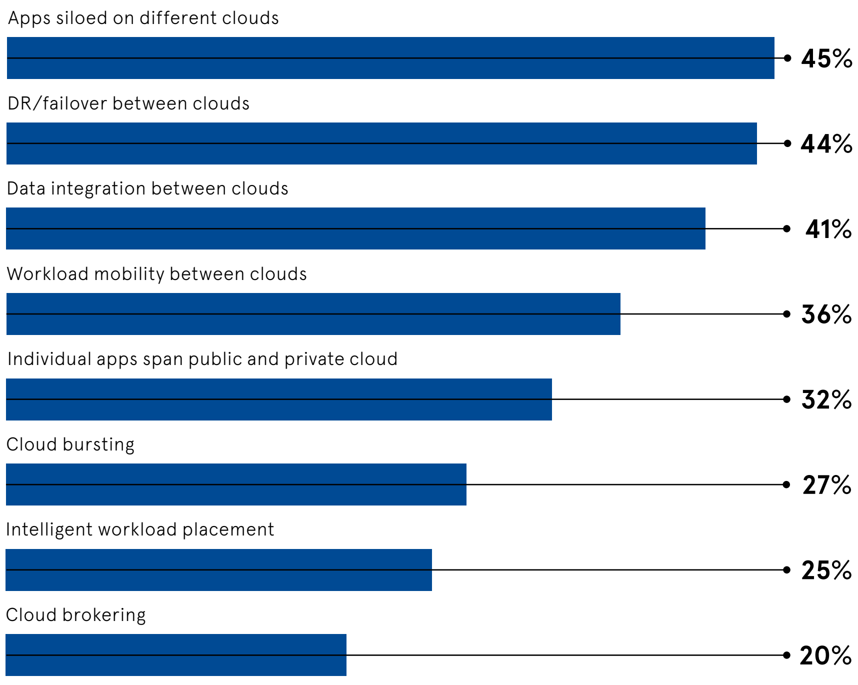
"The ideal architecture is loosely coupled and independent," he says. "This means that the components communicating between the private data centre and the public cloud don't need to transfer large amounts of data between them. They can also tolerate unpredictable latency."

Once an application's suitability has been established, the CIO will need to determine the most suitable bursting mechanism. There are three options available with the big cloud service providers.

The first is manual, where an IT administrator must decide when to instigate the burst and when to bring that workload back. The second is automated, where the tech manages cloud resources and shifts workloads as per the instructions given to it. The third is distributed load balancing.

CLOUD BURSTING IS BECOMING A POPULAR MULTI-CLOUD STRATEGY

Use of multi-cloud architectures by organisations



Flexera, 2022

Judd explains: "You have a small capacity of standby servers provisioned and ready in the cloud. This mitigates the risk of having your own servers overwhelmed when there's a steep increase in traffic." The balancing system allocates the workload between the two environments automatically.

The manual option is the most accessible of the approaches and it's a good way for organisations to test cloud bursting projects, but it's also most prone to inefficiency and error, given that it relies on human judgement.

"Automation is key," says Greg Adams, vice-president of Dynatrace's operation in the UK and Ireland. "The most effective way to support this is by using service-level objectives (SLOs) to set thresholds for an acceptable user experience. For instance, SLOs for application response times can enforce an automated process that invokes cloud bursting if the user experience falls below that threshold."

Mayuram notes that network capacity problems can sometimes stymie a cloud burst because such problems tend not to reveal themselves until it's too late. If there isn't enough bandwidth, he says, "then all the goodness of cloud bursting is only a theory; it will never materialise. The challenge is to plan for adequate bandwidth between private data centres and the public cloud, so that bursting actually happens effectively and meets your SLOs."

No matter which mechanism is chosen, security and regulatory compliance must remain a priority when bursting is enabled.

"The data that will be sent has to be monitored and protected," Mayuram stresses. "If there is material which is protected by compliance requirements or industry-specific governance standards, companies need to take adequate precautions to ensure their security procedures are tight enough."

To safeguard the data being transferred in bursts, businesses should set up encrypted routes between their systems and the public cloud, Judd advises. "Also, the dynamic nature of cloud bursting creates an influx of machine identities," he says. "Companies must deploy a control plane to automate the management of these identities. This gives their teams the observability, consistency and reliability to manage their machine identities."

Ultimately, a firm needs to monitor its cloud bursting constantly to check that its performance keeps within the tolerances and to verify that the method remains cost-effective. If doubts were to arise on either count, the CIOs would need to review their workflow models to determine whether their bursting strategy is still viable. Otherwise, it can be all too easy to get caught out in the rain. ●

Commercial feature

Are consumer trends increasing business risk?

Following the Covid pandemic, remote and hybrid working have become the norm, hugely increasing the number of different access points and devices that need secure and continuous connection to businesses' networks, applications and data

When network breaches happen, as the number of access points rise, it is ever clearer that proper backup and recovery will be critical to companies in sustaining their operations.

"Within most businesses, employees now use their own devices to access critical apps, and it's essential to remaining productive," says Stephen O'Brien, CMO at cloud and connectivity company M247. Given this new reality, he explains, businesses must go beyond thinking only about how to prevent network breaches, and assess how to confidently mitigate the damage done if they occur.

"Business networks are constantly being hit, by everything from automated bots to more sophisticated and targeted attacks," O'Brien says. "Given there is no way to be 100% secure, executives need to think about how to introduce a system-wide approach that provides both a protective layer and ensures constant access to data and applications."

Many companies still have data and apps running in multiple cloud locations, with differing levels of protection and little ability to restore systems quickly, he warns. "Business backup and recovery capabilities often do not match up to the threats they face today, and they have misplaced confidence in what they're doing," O'Brien notes. "It is essential to implement a robust strategy to avoid huge operational risk, fines and reputational damage."

Such a complex setup tends to develop over time in business. "It's a bit like our own health – when all seems well we're less likely to take proper steps to look after ourselves," he explains, adding that executives should allocate time in their schedule to analyse the potential impacts of a breach for their business.

In order to develop an effective response, a thorough strategy for backup and recovery is required, and this can be achieved by working with industry experts to keep pace with evolving threats. "We help businesses by first auditing their processes and systems, to understand the state of play and what needs to be changed, then they can properly protect the perimeter," O'Brien explains. "We then overlay powerful backup and recovery as the critical last line of defence."

> It is essential to implement a robust strategy to avoid huge operational risk, fines and reputational damage

Many companies already work with M247 to improve their security, including through mirrored data and apps located at multiple sites. Among them is Odeon, which has used a variety of cloud systems to store data and applications. M247 assessed the cinema chain's setup, introducing backup and disaster recovery programs that enable the rapid restoration of apps whenever needed, protecting uptime in a new hybrid cloud setup. Meanwhile, football club Sunderland AFC worked with M247 during the pandemic to ensure high connectivity to a much more resilient website. M247 introduced a hybrid cloud and backup as a service to enable supporters to easily stream games from its website at all times.

Looking ahead, M247 is responding to the massive growth in the number of Internet of Things devices, used at home and in sectors including retail, distribution, healthcare, manufacturing, telecoms and energy. "There is a huge positive impact in terms of what businesses can do now, but of course there also needs to be a clear security and performance response. Our own 5G-enabled core network will fully serve and support such communications," O'Brien notes.

Meanwhile, with artificial intelligence and machine learning speeding up decision-making, automating processes and supporting immersive virtual reality, there is a parallel rise in automated security threats. M247 is responding by ensuring that its defence mechanisms also use advanced AI to provide highly effective breach identification and mitigate any operational consequences.

Today, as business risks grow with the explosion in remote working and the increasing number of devices accessing company systems, so does the need for advanced backup and recovery strategies to protect operations. By working with industry experts that keep pace with all of the emerging security developments, businesses can ensure they mitigate potential damage and secure always-on uptime.

To find out about advanced backup and recovery, visit m247.com/cloud

M247

OPEN DATA

Europe's quest for digital trust

The ambitious European plan to network cloud services providers would usher in a new system of sharing data – and uphold EU data privacy laws. But much work remains to be done

Santiago Urquijo via Getty Images

Marc Ambasna-Jones

If anyone were in doubt of the impact that the misuse of data can have on businesses and nation states, they'd need look no further than the recent investigations surrounding Team Jorge in Israel, the disinformation unit that allegedly worked to disrupt elections in countries worldwide.

Five years on, the Cambridge Analytica scandal is a reminder of how data is increasingly woven into the fabric of modern society and the dangers when it is weaponised.

While arguably it was Edward Snowden's whistle-blowing in 2013 of National Security Agency activities that triggered global discussions on data sovereignty, the Cambridge Analytica events accelerated it.

Just a year later, aware of the growing importance of cloud computing as the backbone of modern technology, governments in Germany and France came up with a cunning plan.

> This is the edge revolution, the data gravity concept is driving it, and Gaia-X is the only concrete initiative addressing a need not satisfied yet by any of the large cloud operators

Today, that plan has evolved into what is called Gaia-X, an association of governments, technology firms, academics, public bodies and not-for-profits that is working to define a common way to solve Europe's digital sovereignty conundrum. The need, according to Francesco Bonfiglio, CEO of Gaia-X, is driven by the fact that big tech platforms are controlling everything.

"It's time for a change," Bonfiglio says, adding that this change needs to be in the direction of "a distributed, decentralised, federated, transparent, interoperable cloud that is orthogonal to the model of the top hyperscalers".

All the cloud hyperscalers rank among the association's 373 members. Bonfiglio says that despite stories suggesting "this was to destroy the initiative or to condition our decisions," these businesses (which are all US-based except for China's Alibaba Cloud) need the European market and understand that currently, the region is "missing a common definition of trust for digital services".

Figures from Synergy Research Group in September last year put the big three cloud providers firmly in the driving seat in Europe, with a 72% market share. It's difficult not to feel a power struggle brewing, which is why Gaia-X needs critical mass. The member list is impressive but far from comprehensive.

While Bonfiglio talks about "a monopoly of a handful of private commercial operators," the reality is that the hyperscalers are dominating for a reason. But he is clear that this cannot be an 'us or them' scenario. Gaia-X is, he says, a sort of bridge, to help any cloud provider solve data trust issues within European sovereign boundaries.

"Gaia-X or not, Europe cannot do without the hyperscalers," says Dario Maisto, senior analyst at Forrester. "These companies invest some $40bn in new services every year. Furthermore, the hyperscalers can build partnerships with local providers to ensure that their offering stays compliant with sovereignty requirements, which does help in overcoming some of the European organisations' concerns."

Maisto adds that some SaaS vendors deploy their solutions on the hyperscalers' infrastructure and take a federated approach to data. This data, he says, is anonymised before leaving the sovereign environment to be processed by the external AI or machine learning solutions sitting in non-sovereign environments.

While this ticks a few boxes to do with data sovereignty, Bonfiglio's point that Europe still needs a trusted, federated system, whereby data is shared regardless of the cloud provider, still stands tall. In many respects, he is advocating a future-proof framework for data that is cloud agnostic and acts as a gateway to European organisations and markets.

This is why the hyperscalers are involved. Chris Drake, senior research director at IDC, points out that data sovereignty is increasingly a key factor in the selection of cloud service providers.

"This partly reflects the growing importance of regulation, including GDPR, which emphasises the importance of personal data protection and provides specific rules around data storage and transfer," explains Drake.

For Bonfiglio, the key to solving the sovereignty issue lies within the Gaia-X digital clearing house (GXDCH), described as "the one-stop place to be verified against the Gaia-X rules and obtain compliance in an automated way". The GXDCH is built on a framework of "fundamental bricks to build the data economy", says Bonfiglio. This consists of federation, data exchange and compliance. Where much of this concerns the practicalities of data management and exchange, it is underpinned by the need for trust. Everything is measured against a set of compliance rules, such as GDPR.

This month, we will get to see what this all means at the Market-X event in Vienna, Austria. Bonfiglio admits that 2023 is a big year for Gaia-X and Vienna represents the first showcase of what it is all about. There are already trials, or what Gaia-X calls Lighthouse projects, underway. Everything from automotive to manufacturing, tourism, transportation, agriculture and smart cities is being explored, using Gaia-X's principles and components.

Bonfiglio says they have already learnt some lessons here, a key one being that the federative approach is now proven to be "a necessary economical element to create resilient value chains, that can resist unplanned dramatic events, and compete in a market where no single operator can survive alone." The idea is that no single business can operate without sharing data with the others in the chain.

Bonfiglio has no hesitation in saying that countries would be "scared of sharing data due to a distrust of monopolist platforms or giving data to platforms without insurance of trust". This, he says, would run the risk of losing value and competition, where the major technology players would act as de facto regulators.

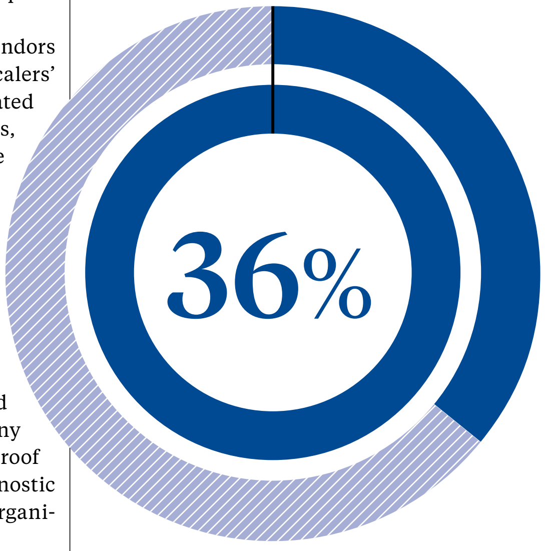
While the current generation of cloud services is hypercentralised and hyperscalable, Bonfiglio believes Gaia-X is needed for these providers to stay relevant. The new generation of cloud and digital services must be distributed, federated and interoperable by definition, he says.

"This is the edge revolution, the data gravity concept is driving it, and Gaia-X is the only concrete initiative addressing a need not satisfied yet by any of the large cloud operators. We are doing something the market needs," he says.

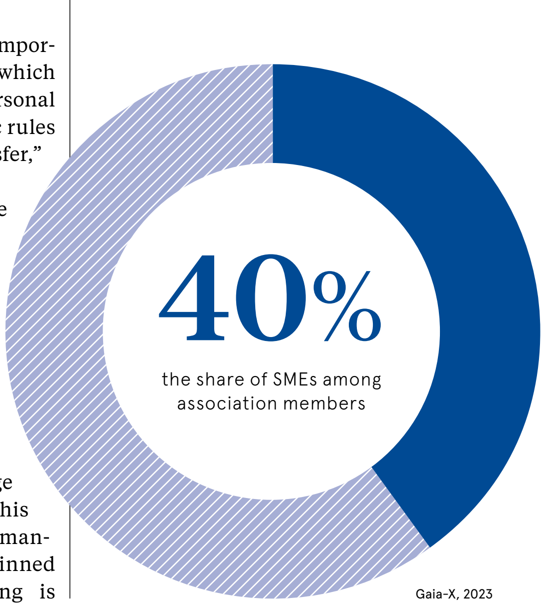
He may have a point. Last year, French vendor OVHcloud sued Microsoft for unfair commercial practices and objected that the personal data of French healthcare patients should not be stored on Azure but in the data centre of a native French cloud provider, to grant EU standard privacy rights. This one is still in the hands of the EU's competition department. Meanwhile, the future of our data, businesses and societies may be in the hands of the data goddess Gaia-X. ●

22 the number of member organisations that founded the Gaia-X European Association for Data and Cloud AISBL, in 2021

373 the total membership at the time of writing



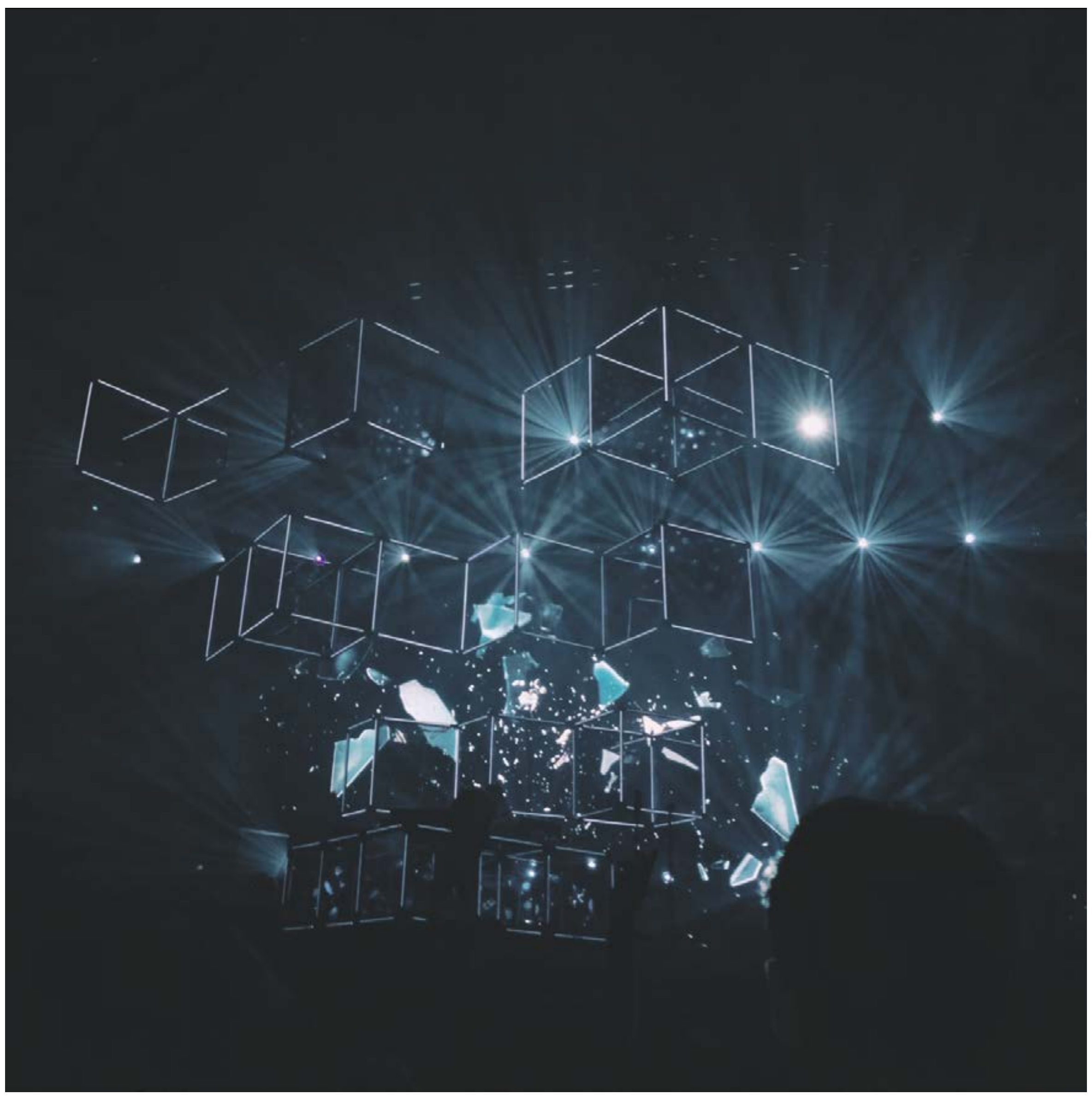
the increase in total membership since Gaia-X was founded



the share of SMEs among association members

Gaia-X, 2023

Commercial feature



Data analytics and automation essential in a recession

Amid an array of macroeconomic challenges, businesses are refocusing on analytics and automation to drive efficiency gains, raise profits and improve decision-making

Each day, business leaders are confronted with predictions of a potential prolonged recession, or at best weak growth. These are prompting several strategy changes.

First, many are abandoning their long-running emphasis on growth over profitability. Prior to and during the coronavirus pandemic, these businesses had assured investors that they would eventually deliver or grow profits, if they could first focus on driving customer numbers.

"While growth is always desirable, there have been businesses that for years valued it over everything else. Essentially, the tougher conditions and end of the 'free money' era have prompted a major switch in approach," explains Martin Willcox, EMEA vice-president of technology at Teradata, the cloud analytics and data platform company.

Prioritising profitability and efficiency

Businesses are typically now prioritising profitability, a shift that demands focus on operational efficiency and making sure activities justify their budgets. "Businesses will need careful and thorough use of data and analytics for proper measurement and interpretation, if they are to achieve this profitability," explains Willcox.

In addition, previously unbridled pursuits of innovation are now being kept in check, while faster, clearer returns on investments are demanded. This has meant companies are re-examining where they invest and eliminating overlaps. "Some organisations have had multiple operations running in parallel with relatively little cost control, and now they have an emphasis on being more intentional," Willcox adds. "There isn't a tolerance for having three departments pursuing the same objectives separately."

Reliable analytics underpin accurate measurement and good decision-making, so businesses are quickly moving away from descriptive analytics towards predictive and prescriptive models. "Companies can use data to see what's likely to happen, and then to know how to optimise outcomes," Willcox explains. Equipped with technologies such as the recently launched VantageCloud platform from Teradata, businesses are improving supply chains, identifying upselling opportunities, eliminating fraud and security risks and transforming myriad key processes.

Combining billions of insights

A clear emphasis will be on excellent use of advanced cloud-based analytics. Businesses will combine multiple data sources, while filtering and interpreting insights using natural language processing systems that understand context. Online shoppers, for example, might put items into a digital basket but take them out again. In that scenario, a retailer needs to make intelligent alternative recommendations that are both appealing and reflect stock availability. "There are many dimensions involved in solving that problem, including ordering, supply chain and warehousing, plus interpreting a customer's intent," Willcox says.

Such combined analytic techniques can also be applied to internal decision-making. "Every day, across businesses, teams have to make a huge number of micro decisions," Willcox notes. For example, a grocery chain with 50,000 products in 3,000 outlets faces 150 million different combinations for demand forecasting. This would mean a mass of models to train and score continuously. "Automation is crucial here for routine decisions," says Willcox. "Meanwhile, in the more complex cases AI can present the best options to managers. Our ClearScape Analytics operationalises AI and ML at scale, so that it can be used to solve the more complex business problems."

Accuracy here depends on ever smaller analytics models and niche data sets. "Businesses need a per-segment approach to get high levels of accuracy," Willcox explains. "While once it would've been sophisticated for a company to have 50 analytics models in development, looking a decade ahead it's absolutely conceivable that large businesses will each have hundreds of millions of models running."

> Fundamentally, there is no good AI without good data: the models are only as good as the data, and the recommendations are only as good as the models

Such complex modelling is used already to stop certain types of banking fraud such as remote account takeover, or to limit sales from stolen cards. It can also be applied to many other domains to streamline processes, supply chains, profitability measurement and much more. For instance, 5G network providers can apply massive analytics to better manage their quality of service and costs, manufacturers can replace physical testing with multiple automated measurements during production, and utility firms can forecast demand to optimise the distribution and storage of renewable energy.

Where to begin: Analytics 1-2-3

Given the complexity and scale of the challenges at hand, against a backdrop of a possible recession, businesses are looking for methodical, cutting-edge solutions. Teradata guides them through an 'analytics 1-2-3' approach, focused on setting the foundations for data interpretation, preparing models for scalable analytics and deploying those solutions in a manageable way. .

"Fundamentally, there is no good AI without good data: the models are only as good as the data, and the recommendations are only as good as the models," Willcox explains. "Companies begin by getting the data foundations right, and Teradata has extensive libraries of data preparation functions – critical for readying information for AI and ML."

Then there is the question of scale. "Instead of data scientists spending most of their time finding information rather than building models, companies can begin a production line of impactful models," he says. The Teradata platform is used by companies to quickly and widely deploy feature engineering, with extensive reusability. Models can be trained very rapidly, partly because Teradata's platform has advanced learning functions, which can also integrate with companies' other tools.

Finally, companies must address deployment, which means focusing on having the right people in place, and using model ops that enable them to manage potentially millions of different analytics models daily. Teradata's model ops toolset enables users to deploy and manage ever more effective models throughout their business.

Success in practice

Numerous large enterprises are transforming their operations using Teradata's analytics and automation. They range from holiday companies identifying new destinations likely to become popular among travellers to surface-transport businesses assessing and cutting fuel usage. Meanwhile, telecoms firms are using the analytics and automation platform to understand customers and unlock cross selling opportunities, as financial and retail businesses eliminate data silos and empower prescriptive steps for sales agents.

As the technology advances, businesses will increasingly be able to harness ever more unstructured multimedia data, such as CCTV footage and image recognition outputs, to better inform decisions. These could be used in myriad ways, such as to assess if the layout of premises is optimised, to identify customers' habits, or to spot products running out on the shelves. "Companies will be able to take complex data and extract insights, with model training that ensures predictions become more and more accurate. So far, we are all just scratching the surface of what can be achieved," says Willcox.

With businesses facing tough macroeconomic conditions, the smartest executives are advancing the use of analytics and automation to solve complex problems, raise efficiencies and strongly augment profitability.

To find out about smart analytics and automation, visit teradata.com

teradata.

Commercial feature

Customer centricity, data and AI: a future-proofing trinity for retailers

In a challenging and ever-changing environment, retailers must embrace the cloud to take the data-driven approach necessary to understanding the needs of customers

Retail is the beating heart of the UK economy, directly responsible for 5% of GDP and nearly a tenth of all employment, according to the ONS. Indirectly, its impact is even greater. As a principal touchpoint for consumer spending, however, it feels the peaks and troughs of economic activity the sharpest. This has been accentuated by a shift to ecommerce, which had grown gradually over two decades and then drastically accelerated when Covid-19 restrictions pushed online shopping to over 30% of retail sales.

Although the Bank of England now predicts a recession in 2023 to be shallower and shorter than previously expected, this particular economic downturn is unique in that retailers are feeling the impact on both their sales and their cost base. Typically, unemployment increases in a recession and a surplus of available talent enables companies to better control their salary bills. But this time, with unemployment at record lows and inflation high, retailers are under pressure to pay their staff and suppliers more while their customers are spending less during the cost-of-living crisis.

The pandemic and Brexit also magnified flaws in the just-in-time supply chains that have become prevalent in recent years. While this model enables companies to be lean and agile during normal times, when supply or demand is majorly affected they can quickly find themselves unable to keep up with customer orders, affecting loyalty. In a study by Edit and Kin + Carta, just 6% of consumers claimed loyalty to any ecommerce brand, making it the worst-performing sector. Retailers are often guilty of conflating customer habits with customer loyalty. Rather than just repeat behaviour, the true factors of a customer's loyalty are likely to be convenience, cost and inclusivity.

"We've seen consumer expectations shift drastically over the last few years, from demands for seamless ecommerce platforms and sustainable produce and packaging to how they discover, purchase and pay for goods," says Andre Azevedo, CEO of Ancoris, which helps companies innovate and transform through the use of Google Cloud. "The reality of retail is that it's so affected by external factors. But consumers are in fact still spending – albeit in a more targeted way – and there are plenty of ways retailers can remain competitive. The answer is in the data."

The power of a single customer view

As a key enabler of an AI and data-driven retail strategy, the cloud is crucial. The route to brand loyalty in the retail sphere remains startlingly simple – deliver to customers the products they want, at the time they want them, through an easy process of buying and (if necessary) returning. But achieving that in an increasingly omnichannel environment is far from simple, and altogether impossible without the ability to centralise, organise and analyse data.

Customer centricity requires a holistic understanding of the customer, which can only come from a single view of all relevant data, enabling retailers to make better and more informed decisions throughout the entire life cycle of getting a product to a consumer. That single-customer view not only enables an understanding of what they want today, but also predicts and helps influence what they are likely to buy in the future. Such a nuanced and evolving understanding of customers relies heavily on the right data.

"That's where cloud technology comes into play," says Azevedo. "You need a secure, robust place to store, organise and apply machine learning and AI models to your data, and visualise it in a way that enables decision-making. The cloud is a key enabler for implementing these transformative processes.

> **Consumers are in fact still spending and there are plenty of ways retailers can remain competitive. The answer is in the data**

Cloud technology and digital platforms are intrinsically linked as they can be built and improved quickly, as well as scale virtually without limits. Cloud technology is now incredibly mature and includes lots of best practices and out of the box solutions that customers can leverage to accelerate adoption, build their IP on top, and ultimately deliver frictionless digital experiences for their consumers.

Retail for the future

The technology is only one piece of the puzzle, however. It's only when customers can apply cloud technology to build industry-specific solutions that they see true transformative impact – and this is where cloud solution providers like Ancoris differentiate. Ancoris leverages Google Cloud suite of technologies combined with industry expertise and capabilities to build bespoke solutions that solve specific retail use cases, such as increasing personalisation, building the modern store, capturing omnichannel revenue and driving sustainable operations.

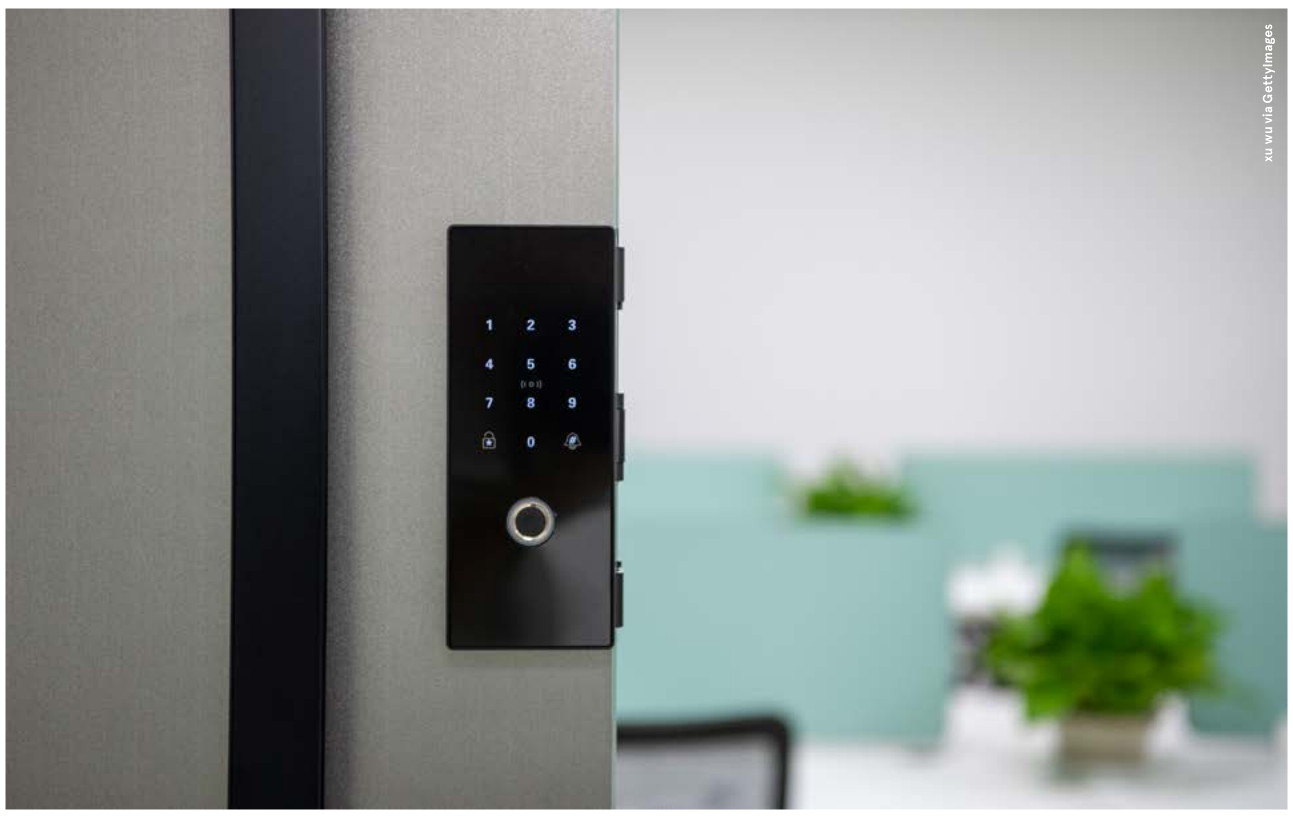
Ancoris's industry expertise results from its extensive experience of helping to modernise retail organisations. One recent customer for instance, a cycling retailer, approached Ancoris when its just-in-time supply model ran into issues during periods when particular products were experiencing demand surges. Ancoris leveraged various Google Cloud technologies to create a single customer view that now enables the company to anticipate what consumers are going to want and optimise its cash flow and warehouse space accordingly.

"Similarly, we also created data visualisation tools to help them make decisions, plus a dynamic pricing tool," says Azevedo. "Not only do they know what their customers are going to buy next and so can optimise their supply chain in the most appropriate way, but they also understand their competitors' pricing and can dynamically adjust their own pricing to ensure they remain at the optimum level. That's what we do as a company: we bring all these technologies together to really add value to the customer and ensure they're increasing brand loyalty and selling more.

He emphasises: "Retailers can and absolutely will thrive in the future, including physical stores, but only by providing an experience that customers really want. They have to use data and AI to build out a single view of the customer to predict what is going to be most valuable to their customers. Only by doing that can they really meet the needs of consumers wherever they are in the omnichannel journey. Industry-focused solutions will bring best-in-class technology to companies to differentiate them by focusing on experience and bringing their brand promise to life in the most compelling way."

For more information, visit ancoris.com

Ancoris



xu wu via Gettyimages

VIRTUAL PRIVATE NETWORKS

Veritably penetrable networks: are VPNs becoming a liability?

The explosion in the number of remote workers using virtual private networks since 2020 has vastly increased the attack surface for cybercriminals. This is prompting a security rethink among CIOs

Laurie Clarke

At the end of last year, network security giant Fortinet warned clients that zero-day vulnerabilities in its virtual private networks had been exploited by hackers in a way that could grant them control of vulnerable VPN servers. It said that this sophisticated attack seemed to be the work of a state-level group seeking to target other national governments.

There was fevered bartering on the dark web for the hackers' successful code. Other criminals used the exploit script in their attempts to infect a global investment firm and a Canadian college with ransomware.

Many firms used VPN technology at the start of the pandemic to share their data. The Covid crisis brought with it a steep rise in cybercrime in 2020, partly because the widespread move to remote working that started during the first lockdowns created so many more potential weak spots for criminals to probe.

The kind of attack that affected Fortinet – the targeting of VPN vulnerabilities – has become far more common than it was before the pandemic. The VPN's status as a secure solution has therefore declined significantly in the past couple of years. In the US, for instance, the FBI, the Cybersecurity and Infrastructure Security Agency and the National Security Agency have all warned businesses about the weaknesses of VPNs.

For the millions of companies that have adopted a hybrid working model over the same period, the need to give staff secure remote online access has outlived the lockdown era. With these security concerns in mind, firms are focused on exploring alternative approaches.

Some industry insiders believe that VPNs are still workable in concert with other measures, while others favour a shift to an entirely new set of security protocols. J D Sherry, a partner in the consultancy practice at cybersecurity firm Istari, is in the first camp.

"While VPNs can be effective tools for ensuring data security, companies can become overly reliant on them," he argues, adding that their use can create a false sense of security, even though their defences can easily be bypassed if users don't practise basic cybersecurity hygiene.

"A VPN can encrypt data and protect against certain types of attack, but it isn't a silver-bullet solution," Sherry says.

Phil Robinson, principal consultant at cybersecurity consultancy Prism Infosec, is more cautious about the security offered by VPN servers and attached devices. These are susceptible to software vulnerabilities, including serious flaws that would allow attackers to gain access and even full control, he contends.

Robinson points out that other big commercial VPN vendors, including Cisco and Juniper, have been found to have coding frailties or weak protocols for authentication or encryption. In the recent Fortinet case, an authentication bypass vulnerability enabled unauthenticated users to access devices on the network.

Such incidents have prompted many experts in the field to declare the imminent demise of VPNs. But Robinson – despite his criticisms of the technology – isn't one of them. "Contrary to popular opinion, the VPN is not dead – yet," he says.

Indeed, companies may not need to discard VPNs at all. There are several ways in which a firm can make them more secure. Number one is choosing a reputable provider that works to strong encryption standards, such as AES-256. Moreover, two straightforward practices that will hugely improve security are using two-factor authentication and updating software regularly to obtain the latest patches.

Paul Bischoff, editor and consumer privacy advocate at Comparitech.com, says of two-factor authentication: "Requiring a one-time PIN or passcode when logging into the VPN will prevent many attacks that would otherwise result from credential theft. Two-factor authentication may be an inconvenience for employees, but it is worth it."

As for ensuring that the software is updated regularly, Bischoff points out that nearly every vulnerability, once discovered by the vendor, will be eliminated in the very next update. This means that "only businesses that refuse or ignore security updates" would remain at a high risk of getting hacked.

Any company that's slow to upgrade its VPN software for whatever reason is making itself a tempting target for ransomware gangs and other threat actors. This is why the US National Security Agency issued a cybersecurity advisory notice in October 2019 that strongly urged firms to pay attention to updates issued by their VPN providers and install the patches as soon as they became available.

Another straightforward safeguard that employers should implement is a so-called least privilege regime, meaning that a particular user has access only to networks and services that are crucial to their work. Such features are likely to be built into cloud-based VPNs.

Some experts believe that the main weakness associated with VPNs is human rather than technological, with criminals using social engineering methods such as phishing to steal users' credentials. This, they argue, means that providing cybersecurity awareness training for all staff is one of the most effective ways for an employer to protect itself.

In his role as a director and solicitor-advocate at law firm Freeths, Will Richmond-Coggan specialises in group litigation arising from cybersecurity breaches. He contends that "something like a VPN – if properly understood and configured – can be an important part of a business's armour. But it should be part of a wider jigsaw of protections that are assembled with a good understanding of the business, how it operates and the risks it faces."

But fast-developing trends in network tech and the emergence of new tools mean that the situation is changing, according to Robinson. "Realistically, the 'deperimeterisation' of the network and the demand for remote access mean that the days of the VPN are numbered," he says.

The replacement for VPN is generally agreed to be the 'zero-trust' approach, which is more of a concept covering the interaction of products across identity verification, access management and network segmentation. The approach takes as a starting point the notion that no device or user seeking access to a network is to be trusted. With a VPN, on the other hand, once a user is authenticated, they can typically access the entire network. Traditional products won't raise an alarm if that person logs in from a different location or in any way act suspiciously.

> **A VPN can encrypt data and protect against certain types of attack, but it isn't a silver-bullet solution**

Instead, zero trust relies on a series of ID and access management tools, such as multi-factor authentication and device profiling, to grant access on a case-by-case basis.

The concept has caught on: 80% of IT and security professionals responding to a 2022 survey by Cloud Security Alliance said that adopting zero-trust systems was a high priority for them.

But the move from VPNs to zero trust is likely to take years. Businesses tend to rely on legacy systems that are designed to work with VPNs, which means that many of them will probably need to be replaced too.

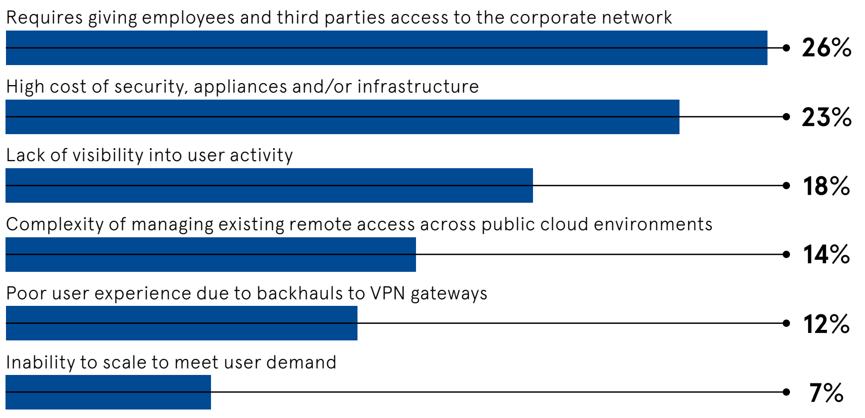
"The network needs to be micro-segmented to limit access, which can be both complex and costly to achieve," says Robinson who adds that zero trust is "very much a strategy with no one-size-fits-all solution. Projects are bespoke and will require a range of solutions."

What, then, is the first big hurdle for IT chiefs to clear on the way towards a zero-trust regime? Robinson suggests that persuading the rest of the C-suite – who may believe that the VPN is working just fine as it is – of the need for change could be quite the challenge.

"Until they can convince those at board level that zero trust isn't a passing fad but is essential in securing a distributed enterprise", he says, "many zero-trust projects will struggle to get off the ground." ●

UNDERSTANDING THE RISKS

Most important VPN challenges worldwide according to cybersecurity professionals



VPNoverview, 2022

CLOUD WASTE

As cloud costs surge, business turns to FinOps

Businesses are rapidly increasing their investment in the cloud, so it's vital they spend their money effectively. That's where FinOps comes in

Kavitha Nair

gilaxia via Getty Images

To stay competitive in a digital world, businesses invest huge sums in cloud services. How can they ensure they spend their money wisely?

It's a growing question for business leaders, for obvious reasons. According to market intelligence firm IDC, spending on public cloud services in Europe alone will hit $148bn (£122bn) in 2023, reaching a staggering $258bn by 2026. As this spending rises, so do concerns over its effectiveness.

To address such concerns, many business leaders are turning to FinOps. This management practice encourages collaboration between finance, technology and business operations to manage an organisation's cloud-computing infrastructure and costs.

It could be the key to optimising cloud expenditure, according to IDC. If the firm's numbers are anything to go by, 2023 may be a pivotal year for FinOps, as increasing macro-economic pressures and the push towards cost-effectiveness drive investments in the cloud.

As it stands, well over 60% of businesses globally have already adopted a FinOps approach. About 15% of these adopters are mature in their FinOps adoption.

Flexera's *2022 State of the Cloud Report* found that organisations on average wasted more than 30% of their cloud spend. This waste could stem from underutilised resources like low CPU usage, unused or forgotten resources like inactive projects or failure to shut resources properly, failure to delete unnecessary machines or over-provisioning resources, among other factors.

For a start, it provides tools for users to monitor these factors. "But FinOps is a great deal more than that," says Edwin-Alexander Kuss, director of global sales at Hystax, a provider of FinOps and multi-cloud cost management software.

Organisations that get FinOps right look beyond cost-cutting, focusing instead on realising the full value of cloud services. "This mindset is what is crucial to an effective FinOps strategy and critical to its success," says Archana Venkatraman, research director, CloudOps, at IDC Europe.

Take Grammarly, an AI-powered writing assistant that suggests improvements for written communication. The company experienced rapid growth from 2021 to 2022, but also saw its cloud spend increasing at a similar pace. It turned to FinOps. "The adoption of FinOps was not solely about cost reduction; it was also about realising the value the cloud offers and making everyone more accountable," says Scott Meyer, staff engineer at Grammarly.

To get companies started, industry body The FinOps Foundation has devised a roadmap that lays out three phases of adoption: inform, optimise and operate.

The first phase, inform, gives engineers greater visibility over an organisation's cloud operations, providing them with a fuller picture of where waste is occurring. In the optimise phase, teams use that information to make informed decisions about cost optimisation – they can see what's essential and what's not and can provide finance with forecasts and budgets.

Finally, firms are left with more efficient, cost-effective cloud operations, where waste can be quickly identified and eliminated. "Following this roadmap, we have made significant progress in our FinOps journey since we started it in 2022. We are now starting to have conversations around the opportunity costs, which is a big step for us," says Meyer.

Adopting the FinOps approach does not require an overhaul of the existing IT setup. Companies can either set up their own FinOps team or collaborate with a vendor.

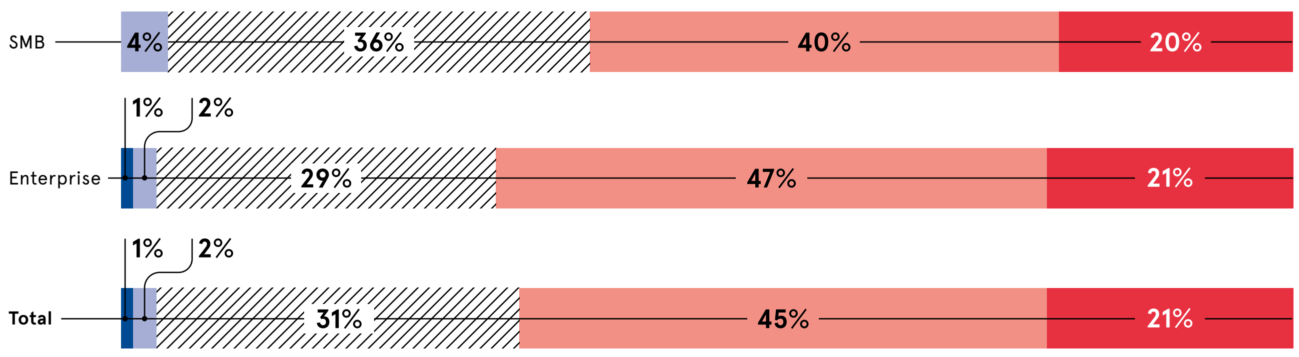
The first phase, which enables greater visibility, is almost entirely internal. It is only at the optimise and operate stages where tools for observability, visualisation and AI and ML are needed to provide insights into how cloud is being used.

THE MAJORITY OF FIRMS SPEND MORE THAN ANTICIPATED ON CLOUD SERVICES

Predicted cloud usage and spend, versus actual usage and spend

Flexera, 2022

● Significantly lower than planned ● Somewhat lower than planned ▨ About the same as planned ● Somewhat higher than planned ● Significantly higher than planned



No matter which approach is adopted, businesses need to bear in mind that all large cloud service providers have multiple tools for cost optimisation, which may add complexity to the process. It's preferable to have a strategy that uses a single, customised tool, providing observability across the entire cloud environment. "This is a long-term process that will take time to achieve," cautions Venkatraman.

Grammarly is between the optimise and operate phase and has already started to see the benefits from FinOps.

The company has noticed an improvement in its unit economics with a decrease in cost-per-user and economies of scale. It has also gained better control over its budget and forecast, along with better planning to determine the best option for its actual needs. All of this has allowed Grammarly to negotiate more effectively with cloud vendors.

For example, to realise the full value, it is imperative that optimisation occurs at a large scale and is not focused on one business resource. This gives businesses the potential to yield savings of 30% to 40%.

The focus is currently limited to optimising the infrastructure or commodity aspect of the cloud: storage and compute instances, for example. But Venkatraman notes that: "Commodity resources are just the starting point. It does play a big part but companies should not stop there.

"To enjoy the full benefit of FinOps, companies would need to take a holistic view of this approach, which should include software as a service."

> "
> The adoption of FinOps was not solely about cost reduction but also realising the value the cloud offers and making everyone more accountable

Mindset is the other big challenge for FinOps adoption. Historically, engineers haven't been involved in decision-making over costs, so they face a cultural shift to understand the costs associated with their work, including the impact of changes on the cloud per user.

But as engineers become more involved in cost optimisation, they can make informed trade-off decisions themselves. "To get the engineers to prioritise these new optimisation efforts could take three to six months," advises Meyer.

Businesses need proper collaboration and planning to be successful in the cloud. It is a fragile asset and if it isn't used properly, the value of it will not be realised. Implementing FinOps allows companies to adopt cloud solutions in a secure and transparent way, bringing about a cost-effective cloud experience.

Kuss and Venkatraman believe the key to FinOps success is not the size of a company, industry or budgets spent on cloud services. Basic implementation of FinOps principles such as visibility, control, collaboration and cost optimisation will help make the most of spending and improve governance.

Industry experts suggest starting small. To begin, businesses should form a dedicated FinOps team consisting of members from IT, finance and other executives. This will include establishing a FinOps process that defines the responsibilities of each team member.

An effective strategy outlines clear goals to understand potential cost savings, both in the short and long term. At a later stage, businesses might consider FinOps certifications and upskilling whole cloud teams.

Experts recommend that businesses start by utilising the available tools in the market, which can help identify cost-optimisation opportunities and provide transparency. Engaging the engineering teams also helps reduce friction and ultimately improves cost optimisation.

Rather than waiting for the shock of a steep cloud bill, FinOps is a proactive approach to optimising cloud spending. It's a way to address spiking cloud costs, for sure. But it also helps organisations to realise the full potential of their cloud strategy, saving time and money and maximising resource utilisation. ●

INSIGHT

'Edge computing can accelerate businesses transformation in 2023'

Times are tight and business leaders are looking for new ways to maximise efficiency and profitability. **Sue Daley**, director for technology and innovation, techUK, says now is the time to rethink your cloud strategy and invest in the edge

There has never been a more crucial time for businesses to adopt technologies that will help them be more efficient, productive and profitable. While cloud continues to sit at the heart of this process, edge computing is another key enabler of digital transformation that businesses are turning to and we could see the much wider adoption of edge computing in 2023.

Market research firm IDC predicts that worldwide spending on edge will hit $208bn (£174bn) in 2023 and see compound annual growth of 10% to 20% across multiple industries including banking, manufacturing, retail, transport and healthcare. So why are businesses investing so much at the edge?

Organisations that move compute processes closer to users and sources of data are benefiting from minimal latency, increased resilience and fewer bandwidth constraints. This supports real-time analytics and automation in manufacturing, improved diagnostics and patient monitoring in hospitals, and personalised customer experiences using augmented and virtual reality in retail. From autonomous vehicles, to utilities, to the metaverse, the list of potential use cases for edge computing is endless.

In seizing these opportunities, businesses are bringing edge and cloud together to deploy applications across a geographically diverse fabric of infrastructure – a distributed 'hybrid cloud' – that can include internet of things (IoT) and end-user devices, on-premises edge servers, multi-access edge services offered by telecoms, local 'edge data centres' and an enterprise core in public or private cloud.

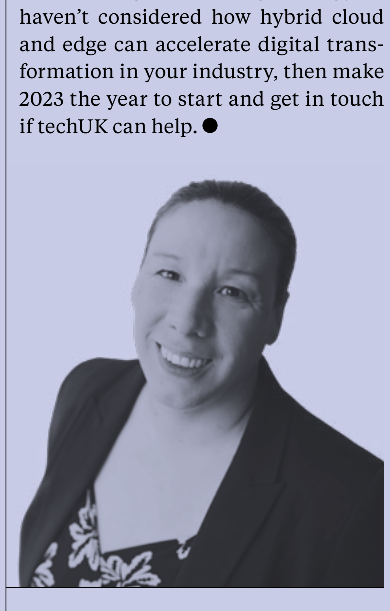
This hybrid approach has been driven by advances in 5G, AI and IoT, which are unlocking valuable data at the edge, and also by the rise of software-defined networking and virtualisation technologies, like containers, which bridge the gap between edge and cloud. Accelerating edge adoption has also triggered a wave of partnerships between cloud providers, telecoms operators and other infrastructure businesses diversifying into edge and offering integrated end-to-end services from cloud core to end-point device. The message from industry is clear – hybrid cloud and edge are definitely here to stay.

However, securing the full economic potential of edge is not without challenges. Some organisations will need to rethink cybersecurity strategies to account for a more complex and varied physical infrastructure, applying principles of secure-by-design and zero trust, and integrating secure access service edge (SASE) into these hybrid clouds. Interoperability and data portability will also be key, as the ability to deploy applications and move data across a hybrid infrastructure, including many edge nodes and multiple cloud providers, will make it easier for organisations to leverage edge for wider business value.

The UK will need to remain at the forefront of full-fibre, 5G and 6G connectivity if we want organisations, from every sector of the economy and every region of the UK, to see the full benefits of hybrid cloud and edge computing. Urgent action to address the UK's digital skills gap is also key to widespread edge adoption, as businesses are already finding that skills are one of the main barriers to digital transformation.

Finally, as the use of edge computing accelerates, and more compute and data storage devices are deployed outside data centres and across diverse physical locations, we must consider how to build this distributed network with sustainability in mind.

These are all issues techUK will be exploring in 2023 as we work with our members to unlock the benefits of edge and drive a new wave of disruptive innovation in industries across the economy, adding value for businesses and customers. If you don't have an edge computing strategy or haven't considered how hybrid cloud and edge can accelerate digital transformation in your industry, then make 2023 the year to start and get in touch if techUK can help. ●



Sue Daley
Director for Technology and Innovation, techUK

Martin Berntzen / EyeEm via GettyImages

STRATEGY

Four ways to win over the cloud laggards

Adopting cloud services is far more than a cost-efficiency matter. The full business case for doing so has several elements that should reassure even the most sceptical of business leaders

Chris Stokel-Walker

The rise of cloud services has been seemingly unstoppable in recent years. Research last year by US jobsite Zippia estimated that 94% of businesses were using the cloud in some capacity.

If you're a decision-maker in one of the 6% that haven't adopted this technology and you're yet to be convinced that the pros outweigh the cons, here are four persuasive reasons to change your mind. Each is based on what your firm could be losing out on by steering clear of the cloud.

Digital Vision via GettyImages

Losing out on competitiveness

Even if your company isn't trying to use the latest technological advances to gain an edge in its market, most of its rivals are certain to be.

Alister Sneddon is head of product at CMC Invest, the developer of an app-based investment platform. He says that "using cloud technology – and using it right – helps businesses to stay at the cutting edge of developments and keep pace with their customers' needs. Using the cloud to manage security patches, for instance, enables teams to focus on improving processes. Having that time back is crucial in helping you to innovate and enhance the customer experience your products provide."

Cloud technology has enabled CMC Invest to deploy new features rapidly on the app that it has developed.

"Using the cloud to 'spin up' tests and manage technical spikes means that we can create and test ideas at a low cost without affecting our hardware," Sneddon says. "We can respond to customer feedback within hours, not weeks. As the technology enables serverless edge computing, we're as close to our customers and their devices as possible, which reduces latency and dependencies."

DEV IMAGES via GettyImages

Losing out on adaptability

Another cloud benefit is that its flexibility enables firms to scale their use of its services up and down according to their requirements. This functionality is often viewed through the lens of cost-efficiency, but it's not only about the bottom line. It's also about how your business can match the pace of change in a fast-moving market.

"Most businesses have peaks in demand, typically five times greater than usual loads," says Danny Quilton, co-founder and CTO of the Capacitas consultancy. "If they didn't use the scalability of the cloud, businesses would have to build their infrastructure five times larger than they need for normal usage."

He cites JD Sports as an example of a company that spins up ecommerce capacity in the cloud when it can see spikes in demand approaching.

While the ability to turn cloud assets on and off like a tap clearly does offer cost savings, there are also business continuity benefits. A company experiencing a growth spurt and taking on an influx of customers, say, can quickly ramp up its capacity in a way that wouldn't be possible with a traditional hardware solution. The firm can buy and access cloud services within hours.

Such flexibility works equally well when a business is on the downswing. For seasonal enterprises, for instance, the ability to stand down cloud services easily when it doesn't need them can be just as valuable.

Manuel Breva Colmeiro via GettyImages

Losing out on resilience

One of the hardest things for a company to do is get back on its feet after a serious cybersecurity breach. The impact of a successful ransomware attack can be powerful enough to knock a firm out of business permanently.

Although the number of ransomware attacks worldwide declined slightly between 2021 and last year, according to IBM, the business-interruption risk they pose remains high. Entrusting your data to the cloud won't prevent such attacks (in many cases, that would require training to stop employees making basic errors such as clicking on suspicious hyperlinks), but it can help your business to get up and running again if the worst does happen.

Businesses using the cloud are twice as likely as non-users to say that they've implemented a complete disaster-recovery plan within four hours of an attack. Off-site online back-ups often make it possible for them to recover data that might ordinarily have been compromised by such a hack.

"It's difficult for ransomware to encrypt files in the cloud, as they tend not to be part of your corporate network," notes Alan Woodward, visiting professor of cybersecurity at the University of Surrey. "It creates a partial firebreak."

But he cautions against relying on this tactic in the ongoing war against the cybercriminals. "This is not a guarantee – and its usefulness is more about recovering once you've rebuilt your in-house platforms," Woodward stresses.

Sarin Soman via GettyImages

Losing out on the changing face of data

One of the big changes we're seeing in how businesses operate in recent years concerns the presentation of data in their workflows. The International Data Corporation has predicted that 80% of the world's data will be unstructured by 2025. That will have a huge impact on the way systems work and what businesses can do to ensure that they can stay on top of the masses of material they're expected to handle.

This is another area in which cloud technology can help.

Sébastien Marotte, president of cloud supplier Box in EMEA, explains: "Unstructured data is at the heart of every company's workflow, from image searches in the marketing team to contract negotiations in the legal department. It can be incredibly hard to secure, access and collaborate on.

"The cloud enables a centralisation of content in all forms, including unstructured data, and supports collaborative workflows, optimising cooperation and data-driven decision-making."

He adds that this is becoming ever more relevant as the rise of AI continues and various industries find applications for the technology.

"Only from that centralised data set will businesses eventually take advantage of the great strides that are being made in artificial intelligence and the potential it promises for productivity," Marotte predicts. "This affects every role in an enterprise." ●

Commercial feature

Enterprises seek escape from escalating vendor support costs

The costs of migrating to the cloud and managing a hybrid environment are escalating due to increasing support fees and costly technical resources, but enterprises don't have to accept the prices imposed by vendors

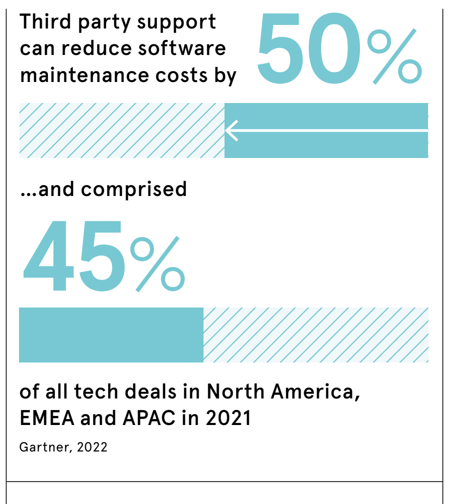
Enterprises have widely embraced the move to the cloud over the past decade to reduce IT costs, accelerate service delivery life cycles and make them more agile amid changing market conditions. While this has been largely successful, the ongoing goal for greater cost optimisation has hit a stumbling block in more recent years as organisations have grown increasingly concerned about increases in the support costs charged by software vendors.

Software support and maintenance is essential as without it companies are exposed to bugs, failures and vulnerabilities in their products and wider operations. However, the ability of software vendors to increase their support fees by the rate of inflation or more each year has left some organisations feeling they have little choice but to absorb these additional costs.

At the end of 2021, Gartner predicted that software ownership, operations and support costs would increase by up to 35% by the end of 2025. Given the double-digit spike in inflation over the past year, in particular, that could now be an underestimate. During a time of economic uncertainty, when companies are reining in their spending, this is a business critical concern.

"We have seen growing worry among enterprises about the rising cost of vendor software support, which has become the second highest IT spend category," says John Forde, managing director at bluesource, which guides and supports organisations on their move to the Microsoft Cloud platform and has offices in central London, New York and Dallas.

"With 2023 looking like a year for belt-tightening across many industries, procurement and sourcing teams, IT departments, CIOs and COOs are urgently reviewing how to mitigate these escalating costs.


Third party support can reduce software maintenance costs by 50%

...and comprised 45%

of all tech deals in North America, EMEA and APAC in 2021

Gartner, 2022

"At the same time, the very nature of SaaS and cloud platforms means they are constantly updated, which increases the pressure to acquire the best IT department skills and expertise to deliver for the business. Success requires end-to-end observability of the platform, as well as intricate knowledge of both the client operating environment and general direction of travel from a technical, security and governance perspective. It's important to ensure configurations are cost effective, high performing and able to scale for peak usage."

Continuous maintenance

Despite what many think, SaaS solutions such as Microsoft 365 are not plug and play. Keeping abreast of vital components like updates, bug fixes and security patches, as well as maximising the capabilities of the software through feature adoption and aligning business process requirements, warrants daily, weekly, monthly and quarterly task management.

The consequences of neglecting important tasks such as governance checks were widely displayed during the Covid crisis when organisations expedited the implementation of collaboration tools like Teams and Zoom, something many are still cleaning up to this day.

Finding and keeping talent is a challenge closely linked to the evergreen nature of cloud platforms. How do organisations know the technical capability of its resources if they are not living and breathing the technology every day? They also want the flexibility in their software maintenance to opt out of features or updates if they do not see the value to their business.

"Flexibility during deployment is also important. Planning deployments to meet real business needs helps maximise licence investments and drive productivity," says Viam Mercer, chief technology officer at bluesource UK. "And don't forget about how you migrate your data to the cloud. Many organisations have a 'lift and shift' mentality that is costly and time consuming.

"Understanding your data through insights such as how old the data is and who's accessing it can help reduce cloud migration costs. Do you need to move old, redundant, obsolete data? Probably not. Automating processes and implementing technical changes based on continuous performance reviews can reduce operating costs on a typical cloud platform by 30%.

"When organisations would traditionally upgrade software within their IT estates, support was delivered by one function while installation and upgrades were handled by a different team, or through external experts brought in. These two areas are now converging."

The evolution of MSP

This new reality, combined with the rising support costs imposed by software vendors, has catapulted demand for lower-priced third-party software support, which can drastically reduce support costs, provide better access to specialist skills and extend the lifespan of software that does not need to be upgraded. According to Gartner, third-party software support can halve the ongoing costs of maintaining software and comprised 45% of all tech deals in North America, EMEA and APAC in 2021, up from 27% a year earlier.

The managed service provider (MSP) environment is also changing, with companies now expecting not only strong understanding and support for their environment, but also knowledge of upcoming updates and feature additions from the vendor and how they will impact them. The most innovative and forward-thinking MSPs are evolving to an 'MSP+' model.

Beyond reducing vendor support costs, this new model adds value to cloud applications, which are continuously updated and require constant management. If a company is on a journey to Office 365 E5, for instance, the Microsoft product might be the best replacement for security, but it also might not. Organisations want access to the right technical expertise to guide the decisions which protect their business, while optimising their costs and performance.

A new age

For organisations on Azure and Microsoft 365, bluesource is leading the charge to MSP+. Having delivered 22 years of managed and delivery services to more than 250 enterprise clients, bluesource is now shaping a new age MSP landscape defined by the convergence of support and continuous delivery capability. Its deep technical capability and understanding of Microsoft environments is reducing support costs for some companies by up to 60%.

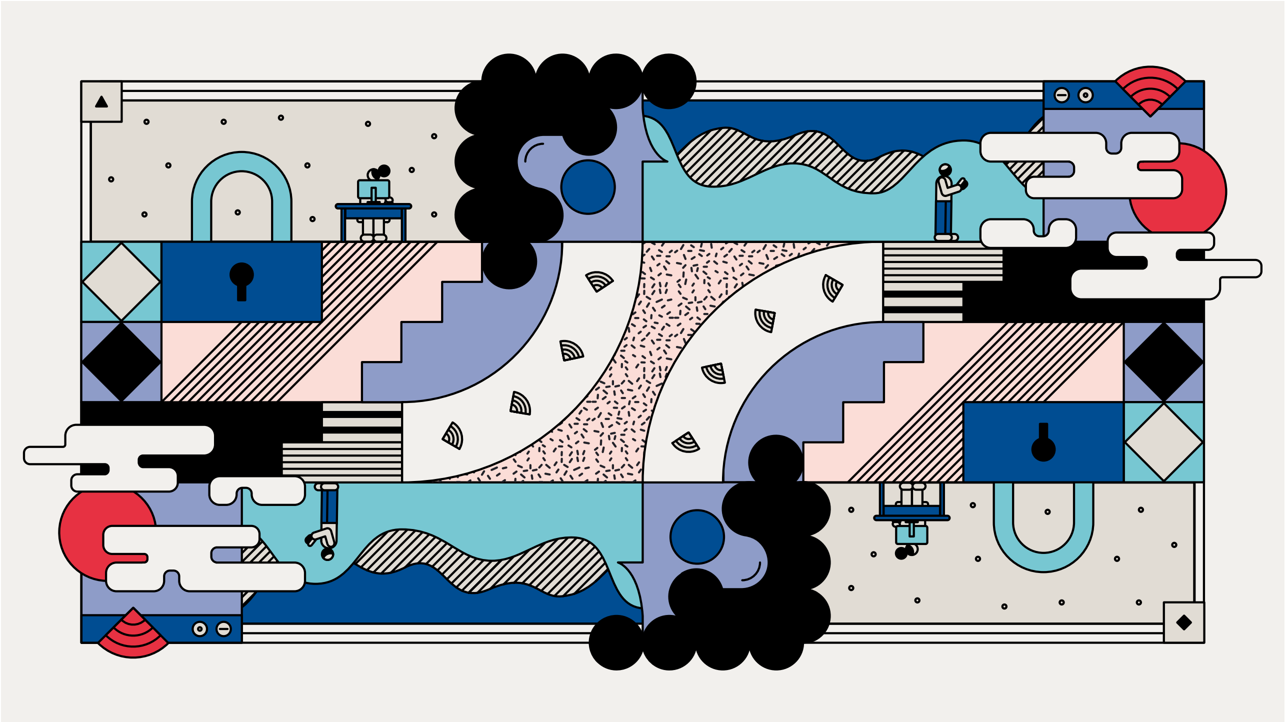
"Working as an extension to a client's IT department, bluesource offers a lower cost alternative to the escalating support and maintenance fees being charged," says Forde. "Our expertise and experience from supporting and managing hundreds of cloud environments means we understand exactly what a fix should look like. We continually optimise cloud services and use the latest capabilities to ensure they are well governed and secure.

"Traditionally we had an outsource mentality – now it's out tasking. Previously MSPs would discuss software upgrade cycles and focus on patch and update management. Through continuous improvement and delivery, MSP+ is about cost optimisation, subscription management, cloud workload and security posture management.

"Our model also de-risks support as we still have the escalation path to Microsoft when needed. We are shattering the traditional ways of doing it and enabling companies to maximise their software investments."

For more information, visit bluesource.co.uk

bluesource
Support that Delivers



LEADERSHIP

Tech chiefs share their resolutions for 2023

IT leaders in a range of sectors reveal their priorities for a year that's set to be challenging for the many that are trawling the same small talent pool

Francesca Cassidy

Pravina Ladva

Group Chief Digital and Technology officer, Swiss Re

I believe that technology leaders will be less focused on the new trends coming down the line in 2023 and more focused on how we better harness the tech we already have.

I'm thinking about how we use data in a way that adds greater value to our business. And are we implementing long-established cloud technologies in the right way? That's going to be a key area of focus.

This year is all about developing people at Swiss Re. We're thinking about how we can help more of our employees to learn about things such as data democratisation and the use of low-code platforms and application programming interfaces.

We're also considering how to attract new talent. We're going to be looking for cybersecurity specialists, data scientists and engineers. The company's purpose is to make the world more resilient. I think that really attracts people to it.

The tech sector suffers from a lack of diversity, so a big task for me will be to work out how to attract a wider range of people across all our territories. We truly believe that diversity of thought will make a positive difference to our progress.

I love it when the teams I work with collaborate well, have fun and win together – it energises me. My big goal for this year is to have vibrant and productive teams across the world that make stuff happen.

> “The tech sector suffers from a lack of diversity, so a big task for me will be to work out how to attract a wider range of people

Kate Smaje

Global Leader, McKinsey Digital

I'm not excited about any one trend in isolation, because this is never about technology for technology's sake. The tech becomes relevant only when it enables you to do something different. I'm more into the chance to combine trends and see what that will unleash in 2023.

That said, I'm probably most intrigued about applied AI and how that's going to accelerate. We saw a big shift towards it in 2017-18, but things then started to plateau. This has to be the year when people figure out how to scale it up.

It's an interesting time for talent management. It's not only about recruiting the best people – although we have our foot firmly on the gas for that. It's also about how to make them wildly successful once we have them. I'll be spending a lot of time on redesigning career pathways here.

We must ensure too that our people are not only successful but also happy in what they're doing. I'm exploring the idea of an index of developer and engineer happiness, which really could unlock how we think about success.

We also need to manage multi-disciplinary teams effectively because we're at our best when marrying deep domain knowledge with deep technical prowess.

> “It's not only about recruiting the best people – it's also about how to make them wildly successful once we have them

Lastly, we have to keep dreaming big. It is clear that digital is a winner-takes-all activity.

If we can't help our clients have audacious aspirations for how their technology will create value, we'll have got something wrong.

Charles Eagan

CTO, BlackBerry

This year, I'm focusing on the intersection between the internet of things (IoT) and cybersecurity. I'll be considering how to secure IoT devices and make the cyber unit more aware of IoT.

I'm looking at how to improve our preparedness through education, storytelling and the simplification of technology. We know that security is better when it's by design, not bolted on.

Everyone is aware of cyber risk and everyone thinks it's someone else's job. If we work together and share insights, then we become a much more formidable foe for attackers – offering them no low-hanging fruit.

The tech talent shortage is certainly a challenge. The reality that many people can work from anywhere has prompted a lot of IT professionals to move jobs. In the early stages of the pandemic, I predicted that much of this movement would slow down – and that hasn't happened. But I'm optimistic. Whenever an expert leaves an area, the people they leave behind often think: how are we going to cope? Then new smart people emerge.

My general management philosophy is to find out what work someone is good at and put a mountain of that in front of them. At BlackBerry we have a lot of tough problems that are fun to work on. I think that this is an effective way to retain people.

Krithika Bhat

CIO, Pure Storage

We are running many initiatives focused on improving the employee experience in 2023. One of these is increasing our self-service capabilities. When you provide these, you empower people. They know that they can do what they need to do themselves, rather than relying on a back-office person.

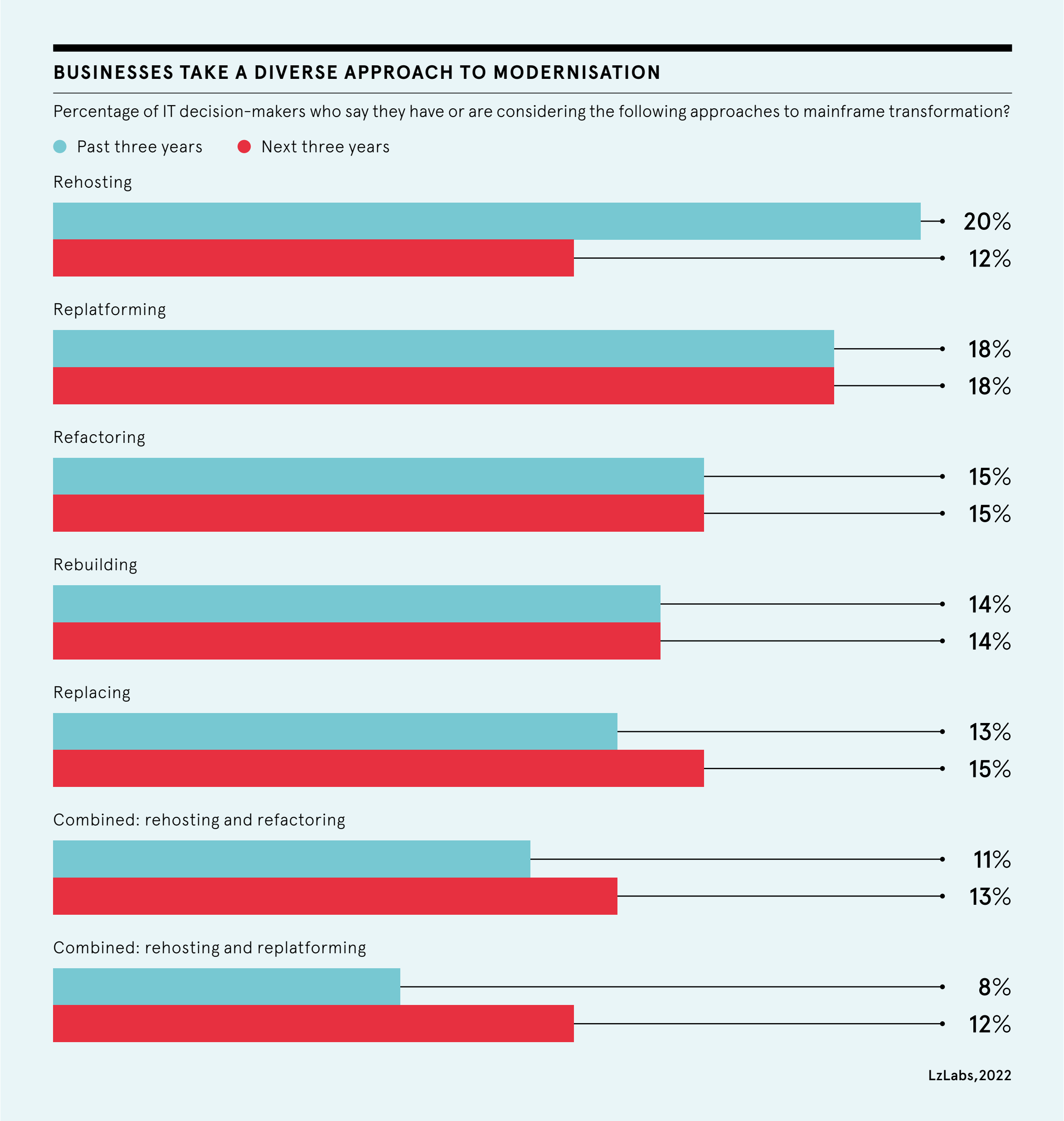
Another priority is to provide truly equitable hybrid working. When I joined the business in March 2022, I was pleasantly surprised to see that lots of people were back in the office two, three or four days a week. Since then, I've had a digital workplace team focused on the ease of hybrid working. What can we do, in terms of tools, technology and culture, to ensure the wellbeing of our people? Addressing this question will remain crucial for me this year.

I expect the organisation to grow over the coming year and, indeed, I'm hiring. I'm not selecting people primarily for their experience. Experience matters a lot, but technology is changing constantly – what's hot today is gone tomorrow. What we really want is adaptability. When we interview candidates, we look at their experience and skills, of course, but aptitude is a crucial component. How willing is this person to learn and do something new? We're looking for the potential that people will bring.

We are also big proponents of internal mobility – how we enable employees to find other jobs within the company. We hear so much about how leaders are looking for new talent, but we must also work hard to retain the talent we have attracted. ●

> “One priority is to provide truly equitable hybrid working

Commercial feature



BUSINESSES TAKE A DIVERSE APPROACH TO MODERNISATION

Percentage of IT decision-makers who say they have or are considering the following approaches to mainframe transformation?

LzLabs,2022

Legacy modernisation: there is no silver bullet

Companies across industries are reliant on complex systems birthed years, or even decades, ago. As they attempt to modernise, they need to take care when basing key systems in more innovative and adaptable environments

What is new in tech today, will be old tomorrow. As businesses attempt to become more agile, the adaptability of their key technology, applications and hardware is often in question. Over recent decades, this has certainly been the case with mainframes, on which companies base many of their key applications. Similar change has also affected even the most modern enterprise resource planning platforms and cloud-based apps.

But modernising existing setups should not necessarily involve complete replacement. In fact, many aspects of an organisation's technology architecture are there for good reason and remain critical to core processes. Elsewhere, however, parts of an IT infrastructure might not be as adaptable to current demands and shifting business objectives. Rather than looking for a silver bullet to solve these issues at once, a more nuanced approach is necessary.

"Many companies are moving away from running data centres and mainframes due to the costs and complexity involved," explains Thilo Rockmann, chief executive of the mainframe transformation and modernisation company LzLabs. "Executives at a car manufacturer or a retailer, for example, might ask themselves: 'Why would I want to spend resources running a data centre when I have more pressing business priorities to focus on?' While this question is understandable, there needs to be a more nuanced view of what needs modernising and how."

At the same time, businesses are facing a growing skills problem. In many cases, personnel who implemented these older systems or wrote the source code have not only quit the company, but left the workforce entirely. Their retirement means organisations have some loss of control over core systems.

Worsening the situation is the fact that data centres typically rely on multiple technologies, from operating systems such as UNIX and Linux, to different processor architectures such as ARM and x86, as well as multiple coding languages including COBOL and Python.

'Big-bang' change

When tackling these problems, companies are increasingly attempting to 'lift and shift' all their IT and data to the cloud, hoping that centralised technology will solve their operational concerns.

"The pressure around this ultimately comes from business leaders, who want tech change and business model adaptation to happen more quickly and for systems to meet multiple emergent demands," Rockmann warns. "It's a bit like having hundreds of people working on a spreadsheet, and expecting it to be switched to offer the capabilities of a database – sometimes a system just can't keep pace with requirements."

Among some executives, the idea that the grass is greener with a different setup typically leads to a strategy of shifting to a singular system or service. In practice, when businesses implement a central off-the-shelf platform, many later regret being tied in with one vendor and unable to customise the technology. So-called 'big bang' shifts also end up taking so long to prepare that the requirements have often changed by the go-live date. Alternatively, businesses may hand over all systems to a cloud host, perhaps mistakenly allowing key knowledge to leave the company.

By contrast, other businesses attempt to rewrite large tranches of their software. However, this quickly becomes incredibly complex and takes longer than leaders usually expect. Developers may realise that either the source code is nowhere in sight, or the documentation they have is not representative of the system in live production.

Methodical and iterative improvement

A more effective approach to legacy modernisation is to work step-by-step towards an innovative and adaptable setup. This means tech leaders recognising nuances in their company's changing needs, and in how their systems serve these requirements.

"Modernisation is really like solving a complex mathematical equation, you can't jump to the answer," Rockmann explains. "The only way is to work step-by-step in analysing system strengths and then making the right changes in sequence, without too many concurrent moving parts."

> “Modernisation is really like solving a complex mathematical equation, you can't jump to the answer

Businesses should start by recognising the value in the systems they have with a view to preserving what works. They then make changes only where necessary, focusing on introducing a fluid pace of modernisation that delivers steady results from early in the process. This approach also means ensuring interoperability and the use of open source software where possible, to avoid being tied into a particular vendor.

"Sometimes businesses need to make a leap in aspects of their modernisation, but as a rule it's far better to be cautious and considered when it comes to introducing technological change," Rockmann says.

The benefits of a more measured approach are twofold. First, the risk of technology failure is minimised because businesses move away from big bang thinking towards a continuum of change supported by an agile culture and an ability to course correct. And, second, IT staff and an organisation's entire workforce have the chance to adjust and develop with the new ways of operating.

Success in practice

Companies worldwide are working with LzLabs to adopt this effective approach and deliver legacy modernisation that meets current and future business needs. LzLabs brings in a tailored strategy for each application and aligns it with business priorities, with its experienced talent pool enabling change and helping companies augment their own technology knowledge. Wherever a mainframe remains critical, LzLabs brings in its software-defined mainframe system, a thin compatibility layer that allows legacy applications to live within a more modern cloud-based environment.

LzLabs focuses on interoperability, control and iterative change being maintained, improving businesses' adaptability and speeding tech development. "In practice there is no silver bullet for everyone, so it's essential to effect and manage change carefully. Because we've advanced the technology of so many different companies, we can help clients modernise their legacy applications in the most effective, tried-and-tested ways that suit their particular objectives," says Rockmann.

Businesses typically begin their conversations with LzLabs when seeking to modernise their systems by moving to the cloud or by virtualising their data centre. LzLabs carefully analyses what is working and is most relevant in their setup and identifies areas that are not sufficiently future-ready. The company can then advise on a step-by-step modernisation programme, including a shift of core legacy systems to the cloud and innovation platforms of choice.

As broader economic conditions evolve and business leaders push for more rapid operational and business model transformations to meet these new realities, IT departments are under immense pressure to maximise the value of their systems and any changes made. The smartest companies are carefully undertaking legacy modernisation, while retaining essential parts of their IT infrastructure and placing them in improved environments. Those that act assertively, but with consideration and methodical change, position themselves well for long-term success.

To talk about a pragmatic path for your legacy modernisation contact us at lzlabs.com

LzLabs®

CLOUD SERVICE PROVIDERS

Are cloud's cost savings overstated?

Once its major selling point, today's reality reveals that public cloud won't save you money – automatically

Doug Drinkwater

katleho Seisa via Getty Images

Last October, project management firm Basecamp lit a fire under public cloud.

In a blog post which was widely shared across the tech community, CTO David Heinemeier Hansson wrote that the series B firm was turning its back on the cloud, thanks in part to a bill reaching $3.2m (£2.6m) a year.

"The savings promised in reduced complexity never materialised. So we're making our plans to leave," he said. The cloud typically excelled, he added, for those with low-level or unpredictable traffic but not for a medium-sized business with "stable growth".

Despite Basecamp's troubles, the ability to save costs in the cloud was once a key selling point. With most contracts pay-as-you-go or subscription-based, the flexibility and scalability of cloud was meant to reduce the operating and administrative overheads of maintaining on-premises data centres, and the burden on operations teams.

But amid the rush to digital services through the pandemic, newer models of cloud consumption, rising inflation and an incoming recession, the cloud cost-success stories of yesterday are increasingly few and far between.

In its 2022 *State of the Cloud Report*, Flexera notes that organisations waste 32% of the money they spend on cloud infrastructure, while IDG's *Cloud Computing Study* says that cost control is a key barrier to migration, along with the cost of moving data into and between clouds.

Common cost issues include higher than expected usage, suboptimal design, runaway license costs and the additional expense of requiring data egress and disaster recovery services. The explosion of data has pushed up storage prices, with Basecamp spending almost $1m to archive 8 petabytes of data on AWS S3. Many SaaS services were also simply under-utilised throughout the Covid crisis.

For many business and technology leaders, saving money in the cloud was always something of a misnomer. "Cloud costs and the lure of savings has been overstated, but most specifically due to how cloud applications and hosting is used," says Roxane Heaton, CIO at Macmillan Cancer Support.

Mudassar Ulhaq, CIO at Waverton Investment Management, agrees. "When I presented to the board, the key objectives were business resiliency, increased capacity to grow, adapt to new technologies and introduce a flexible cost model," he says, adding that flexible working was another.

Through carbon footprint savings, the cloud is now also inadvertently contributing to Waverton's sustainability initiatives. "The sustainable benefits weren't part of my objectives," Ulhaq notes. "But the board now sees how carbon-footprint beneficial we are, and that's a message that our clients want."

For the cloud hyperscalers, the volatile market means they must balance customer satisfaction with profitability.

In the past year, cloud service providers (CSPs) have been badly hit by rising energy bills, inflation, chip shortages in Taiwan, which accounts for two-thirds of the semiconductor market and by the war in Ukraine, which provides 70% of the world's neon gas, a key chemical element used in semiconductor manufacturing.

There's the suggestion too that the cloud might now have reached economies of scale, where the early market gains slow or even disappear.

AWS, Azure and GCP have all missed revenue targets in recent quarters, citing market slowdown. Microsoft will raise the price of all cloud services in Europe from 1 April, while GCP costs have increased for storage, operations and data transfers. Analysts at Canalys forecast that public cloud prices will rise 30% in Europe this year, and some say this could lead to increased tension between suppliers and customers.

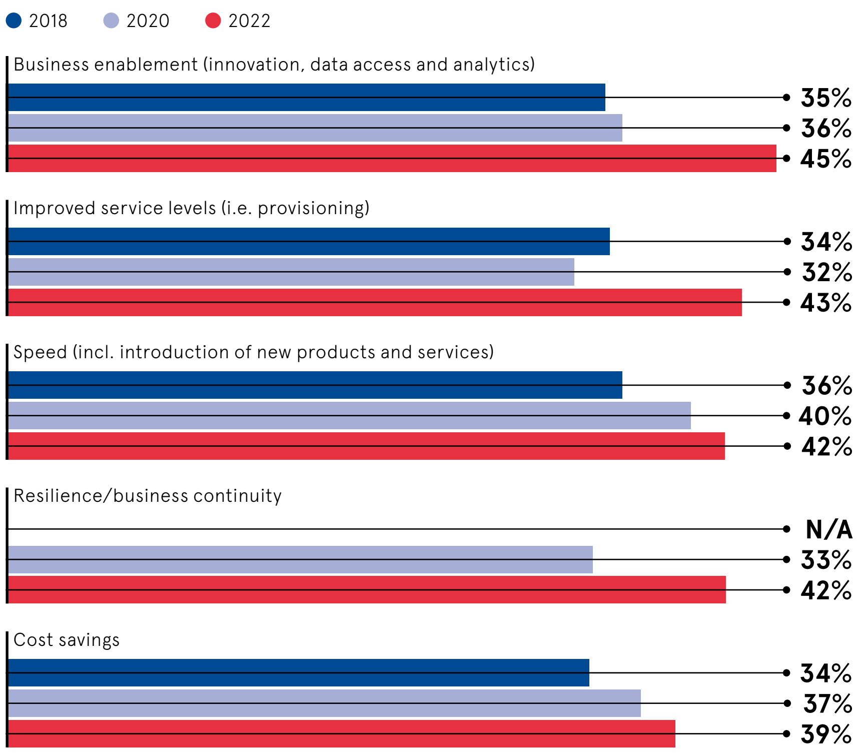
"It's not that cloud providers are bad," says Joe Weinman, a long-time industry analyst and author of *Cloudonomics: The Business Value of Cloud Computing*. He describes the relationship with suppliers as a "fair value exchange". He adds: "It's the nature of capitalism, competitive markets and autonomous entities that have their own mission objectives, shareholders and financial objectives."

CSPs are focused on cost optimisation in order to help their customers. That includes better monitoring of accounts, reviewing the metrics which relate to cost, moving to cloud-native environments and making better decisions through the availability of real-time data.

There is renewed vigour currently around right-sizing workloads. This is the process of maintaining a sufficient level of service for the lowest cost. It could entail shutting down unused instances and moving to more affordable packages, such as lower-tier storage or significantly cheaper spot and reservation instances. Cloud-cost-management tools offer recommendations of where organisations can cut costs.

FEWER THAN TWO IN FIVE FIRMS HAVE ACHIEVED THE COST SAVINGS EXPECTED FROM CLOUD

Share of companies that have fully achieved the following expected cloud outcomes



Accenture, 2023

> It is the responsibility of the cloud vendors to make the billing simplified, transparent and less complex

FinOps, the operational framework designed to bring technology, finance and business together on financial accountability, is in vogue too, with some consultancies claiming it can help save up to 20%-30% on cloud bills.

Giving the example of developers considering cost during code design, Archana Venkatraman, research director, CloudOps, at IDC, says that FinOps makes cost control "everyone's responsibility".

"FinOps is something you think of proactively, even before cloud migration, so the concept is embedded in the design stage," she explains.

Yet critics argue that CSPs should also do more to help with budgeting, not least given the complexity of cloud bills and as pay-per-use procurement models rarely align with traditional budgeting mechanisms.

"It is the responsibility of the cloud vendors to make the billing simplified, transparent and less complex," says Venkatraman. "And empower the users with tools where they can see how their use changes."

Ulhaq agrees with this view. "By introducing a mechanism of review with your customer, you can set budgets and identify unutilised resources that you may not be using," he observes.

Control of cloud costs starts with identifying its value within the business, due diligence, designing cloud environments to suit usage and working collaboratively with suppliers and resellers from brief through to billing. IT departments should be on top of capacity planning and policy management. They should carry out regular cost reviews, where CSPs can provide greater transparency, control and support.

There must also be clarity of the technology leader's role.

"Should they be focused on worrying about what the right orchestration tool is?" asks Weinman. "Or should they be focused on the customer value proposition and competitive differentiation of your products and services?"

Risk mitigation is crucial, and many technology executives have developed cloud cost management and cloud exit strategies. Heaton believes that leaders should be ready to pivot to alternative operating models. "We need to stay close to alternatives, to different ways of delivering the same impact," she advises. "And we need to build ever smarter to both diverge, and consolidate as needed." ●