CLOUD FOR BUSINESS

04 MIGRATION
There are key considerations in moving to the cloud even for those with the smallest budgets

07 HOSTING
Netflix and Spotify prefer a single-provider solution, yet this approach remains unfashionable

10 SECURITY
What should your firm be doing to protect itself from cybercriminals probing for weak links?

EDGE COMPUTING

Cumulo-nimble: giving the cloud a competitive edge

As businesses digitise more assets at the fringes of their operations, they're adopting edge computing to compensate for the cloud's limitations. How well do the two paradigms blend?

Kenny MacIver

Like companies around the world, US fast-food chain Taco Bell responded to the pandemic's commercial impact by accelerating its shift to the cloud. As customers' traditional patterns of restaurant and drive-through consumption changed rapidly – and often permanently – to include kiosk, mobile and web ordering, often through third-party delivery services, Taco Bell moved the remainder of its group IT to cloud services.

But this 100% cloud-based approach stops at the restaurant door. Given that many of its 7,000 outlets don't have fast and/or reliable internet connections, the company has recognised the limitations of the public cloud model and augmented its approach with edge computing. This set-up enables the company to process data near the physical point at which it is created, with only a periodic requirement to feed the most valuable material back to the cloud and receive updates from it.

Taco Bell is just one of thousands of firms seeking to exploit the fast-evolving – and much-hyped – distributed IT capability that edge computing can offer.

"Edge computing is getting so much attention now because organisations have accepted there are things that cloud does poorly," observes Bob Gill, vice-president of research at Gartner and the founder of the consultancy's edge research community.

Issues of latency (time-lag) and limited bandwidth when moving data are key potential weaknesses of the centralised cloud model. These drive a clear distinction between the use cases for cloud and edge computing. But the edge is also a focus for many organisations because they want to add intelligence to much of the equipment that sits within their operations – and to apply artificial intelligence-powered automation at those end points.

Early adopters include manufacturers implementing edge computing in their plants as part of their Industry 4.0 plans; logistics groups seeking to give some form of autonomy to dispersed assets; healthcare providers that have medical equipment scattered across hospitals; and energy companies operating widely dispersed generation facilities.

> **Cloud and edge are pure yin and yang... When put together effectively, they're highly symbiotic**

"For such applications to be viable and efficient, their data must be processed as close to the point of origin or consumption as possible," says George Elissaios, director of product management at Amazon Web Services. "With edge computing, these applications can have lower latency, faster response times and give end customers a better experience. Edge computing can also aid interconnectivity by reducing the amount of data that needs to be backhauled to data centres."

In some ways, the emergence of edge computing represents a new topology for IT. So says Paul Savill, global practice leader for networking and edge computing at Kyndryl, the provider of managed infrastructure services that was recently spun out of the technology firm IBM.

Companies are looking at the edge as "a third landing spot for their data and applications. It's a new tier between the public cloud and the intelligence at an end device – a robot, say," he explains.

But most organisations don't expect their edge and cloud implementations to exist as distinct entities. Rather, they want to find ways to blend the scalability and flexibility they have achieved with the cloud with the responsiveness and autonomy of internet-of-things and satellite processors installed at the edge.

Gill believes that "cloud and edge are pure yin and yang. Each does things the other doesn't do well. When put together effectively, they are highly symbiotic."

They will need to be, as more and more intelligence is moved to the edge. More than 75 billion smart digital devices will be deployed worldwide by 2025, according to projections by research group IHS Markit. And it is neither desirable nor realistic for these to be interacting continuously with the cloud.

"When you start to add in multiple devices, you see a vast increase in the volume, velocity and variety of the data they generate," says Greg Hanson, EMEA and Latin America vice-president of data management company Informatica in. "You simply can't keep moving all of that data into a central point without incurring a significant cost and becoming reliant on network bandwidth and infrastructure."

In such situations, edge IT performs a vital data-thinning function. Satellite processors sitting close to the end points filter out the most valuable material, collate it and dispatch it to the cloud periodically for heavyweight analysis, the training of machine-learning algorithms and longer-term storage. Processors at the edge can also apply data security and privacy rules locally to ensure regulatory compliance.

Gill notes that edge computing has shifted quickly "from concept and hype to successful implementations. In many vertical industries, it is generating revenue, saving money, improving safety, enhancing the customer experience and enabling entirely new applications and data models."

Before achieving such gains, many edge pioneers are likely to have surmounted numerous significant challenges. Given that the technology is immature, there are few widely accepted standards that businesses can apply to it. This means that they're often faced with an overwhelmingly wide range of designs for tech ranging from sensors and operating systems to software stacks and data management methods.

Such complexity is reflected in a widespread shortage of specialist expertise. As Savill notes: "Many companies don't have all the skills they need to roll out edge computing. They're short of people with real competence in the orchestration of these distributed application architectures."

The goal may be to blend cloud and edge seamlessly into a unified model, but the starting points can be very different. There are two fundamentally different – though not totally contradictory – schools of thought, according to Gill. The 'cloud out' perspective, favoured by big cloud service providers such as Amazon, Microsoft and Google, views the edge as an extension of the cloud model that extends the capabilities of their products.

The other approach is known as 'edge in'. In this case, organisations develop edge-native applications that occasionally reach up to the cloud to, say, pass data on to train a machine-learning algorithm.

Adherents of either approach are seeing significant returns on their investments – when they get it right.

"We may be in the early phase of exploiting that combination of IoT, edge and cloud, but the capabilities enabling these distributed architectures – the software control and orchestration tools and the integration capabilities – have already reached the point where they're highly effective," Savill reports. "Some companies that are figuring this out are seeing operational savings of 30% to 40% compared with more traditional configurations."

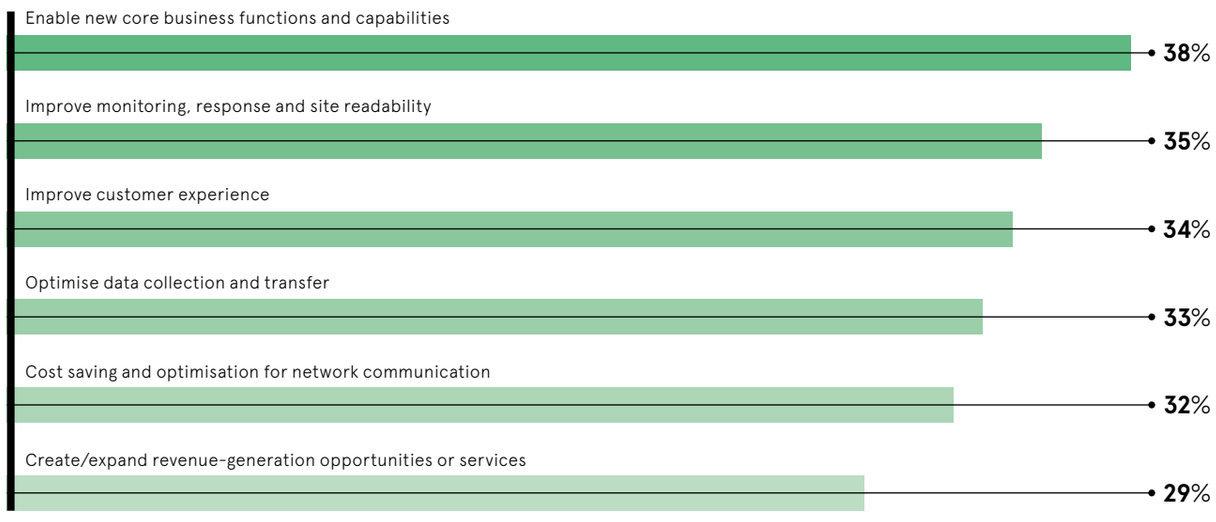
In doing so, they are also heralding a large-scale resurgence of the edifice that cloud helped to tear down: on-premises IT – albeit in a different form.

"In the next 10 to 20 years, the on-premises profile for most companies will not be servers," Elissaios predicts. "It will be connected devices – and billions of them."

WHAT ARE THE BENEFITS OF EDGE COMPUTING?

Percentage of IT professionals who expect the following to be benefits of an edge computing strategy

451 Research, 2021



A MARKET SET TO BOOM

Projected size of the global edge computing market

2019
$2.94bn

2030
$68.71bn

NMSC, 2021

Distributed in THE SUNDAY TIMES

Published in association with techUK

Contributors

Peter Archer
Bestselling author and experienced journalist, he is a former staffer on the Press Association.

David Benady
Writer, editor, content creator and analyst who specialises in media, marketing, retail and IT.

Adrian Bridgwater
Specialist author on software engineering and application development who contributes to *Forbes* and *Computer Weekly*.

Marianne Curphey
Award-winning financial writer, blogger and columnist for various publications, and former staff at *The Guardian* and *The Times*.

Kenny MacIver
Award-winning journalist and ex-editor of *Information Age* and *Computer Business Review*.

Charles Orton-Jones
PPA Business Journalist of the Year, former editor of *EuroBusiness*, specialising in fintech and high growth startups.

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

Mark Taylor
Freelance business journalist and editor, who specialises in coverage of compliance in highly-regulated sectors, where law meets business meets innovation.

raconteur reports

Campaign Manager
Chloe Johnston

Managing editor
Sarah Vizard

Deputy editor
Francesca Cassidy

Reports editor
Ian Deering

Sub-editor
Neil Cole
Gerrard Cowen

Head of production
Justyna O'Connell

Design and production assistant
Louis Nassé

Design
Kellie Jerrard
Celina Lucey
Colm McDermott
Sean Wyatt-Livesley

Illustration
Sara Gelfgren
Samuele Motta

Design director
Tim Whitlock

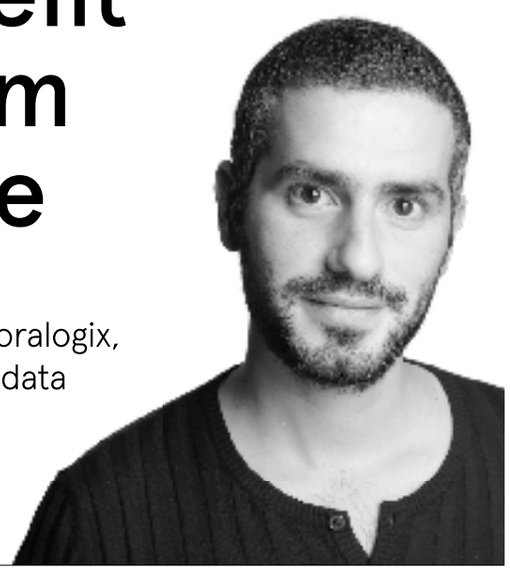
/raconteur.net
@raconteur
@raconteur_london

raconteur.net /cloud-for-business-2022

Commercial feature

Q&A

Analytics in reverse – how to benefit from the boom in data volume



More data means better insights, right? **Ariel Assaraf**, co-founder and CEO of Coralogix, explains why switching the sequence of data analysis helps ensure that data insights aren't lost in the din

Q **Why is the exponential growth in data volumes such a challenge?**

A It's absolutely true that data continues to explode every year, which is a fact in DevOps and security. Whether you are talking about log analytics, security data, or other business metrics, the output generated grows so fast it overwhelms traditional architectures.

The headline result is a spiralling cost. Most data service providers charge by data volume or the number of queries you run, so when data grows exponentially, so do costs. The performance also takes a hit. You'd think more data equals better results, but exponential data volumes can lead to slow or shallow analytics. This leads to companies carefully cherry-picking the analytics they want to run, resulting in lost valuable insights. In a way, it forces companies to look for the needle in a haystack.

Q **What is the problem with traditional solutions?**

A Traditional methods slow down as the data grows in volume. Every query takes longer to perform which impacts the entire enterprise. If you are an organisation with 300 developers and each developer runs 10 queries a day – which is not a lot – that's 3,000 a day. If each query takes just 30 seconds longer, you are losing two full workdays, across the organisation – every day.

Worse is the way cost and performance influence the approach to analytics. Companies know they don't have the time or resources to search all the data, so they only run quick queries or limit their scope, reducing their observability. Rather than offering insights, data growth is, therefore, a major problem at present.

Q **What is the optimum approach?**

A At Coralogix, we've flipped the architecture. Traditionally, the sequence is to store data and then analyse it. Our method is the reverse. We analyse data in real time, with no delays, and then let the customer choose whether to store it or not. This means every drop of data can be analysed. Users can then archive it, throw it away, or if anything is interesting they can put it on hot storage for frequent search.

The advantages are huge. It reduces cost, increases coverage, and solves performance issues. Analysis is done in real time, with no delays; insights can be spotted the moment they occur; teams no longer need to cherry-pick which queries they run; and the cost is much lower.

Interoperability is crucial too. Coralogix is not dependent on a storage or database schema. We allow multiple syntaxes and dashboards. Users can plug Coralogix into Kibana, Grafana, Jaeger, Tableau, or SQL client. Alternatively, users can use our API or CLI tool.

Q **How can companies query the data for insights?**

A Companies are welcome to use their current suite of analytics tools and dashboards. Integration couldn't be easier. And we provide the most extensive alerting mechanisms on the market. We offer anomaly detection to identify unusual code behaviour like error ratio spikes and code flow anomalies. Our machine learning alerts are world class, offering a dramatic reduction in alert fatigue which stems from false positives. Users can define an event, and then our alerts will let them know it happened more than usual.

Most importantly, our alerts run on their complete data set in real time, spotting problems far earlier than possible with human observation or traditional methods.

> **We've flipped the architecture. We analyse data in real time,with no delays, and then let the customer choose whether to store it or not**

Q **Does this method of analysis impact costs?**

A Legacy vendors charge linearly. The more data you produce, the more you pay. As data grows exponentially, so do costs. Coralogix operates a radically different billing model. We charge by use case. You pay for what's important to you. So monitoring data, which is the everyday stuff you need to focus on in real time, is priced differently to frequently searched data. Compliance data, which is of low-operational value, is the cheapest. This way, you pay per value instead of volume. Each data priority level is priced according to its business value. Crucially, you get access to all Coralogix features no matter what use case you opt for.

The key is that costs are decoupled from data volumes. Your organisation can produce as much data as it needs, without costs rising lockstep.

Q **Tell us about Coralogix**

A I co-founded the company in 2015 and today we serve more than 2,000 clients such as Monday.com, Masterclass, UCSF, and Fiverr. We also cooperate with more than 10,000 DevOps and engineering users, monitoring half a million applications, with more than 3 million events processed per second.

Importantly, we have all of the necessary qualifications – including HIPAA, PCI, ISO/IEC 27001 and 27701, GDPR, and FCA – to work with the most demanding clients across financial services, healthcare, government, and other highly regulated industries.

Q **Is it easy for companies to work with Coralogix?**

A Because of our architecture, onboarding is made easy. We use common syntaxes such as the Elastic syntax, PromQL, and SQL. And we plug into any dashboard you have in your ecosystem. And because we don't change the collection layer you can send data from anywhere, any way you like. You can visualise it any way you like, and use any syntax you like. There's no vendor lock-in and you don't have to retrain your people.

Q **What is the company's five-year vision?**

A We started with log data, and continued with metric information, such as performance and infrastructure monitoring. We launched a security product for posture, compliance, and network security monitoring. And now we're launching tracing and APM.

Our plan for the future is a continuation of this vision; one where we are a unified generic data platform that can accept any data, analyse it anyway, and display it with any syntax. In the next few years, that will extend to business information, marketing information, and compliance data. For us, it's all a data problem we know how to solve.

Visit coralogix.com to learn more

Coralogix

COST STRATEGY

Platinum linings: how to bring down cloud expenditure

As businesses produce ever more data, the costs of handling all this material have rocketed. Finding efficiency savings in this area is becoming a C-suite priority

David Benady

Cloud services are gobbling up an increasingly large share of corporate technology budgets as businesses rush to digitalise. The search is on for ways to keep costs in check and extract maximum value for money from the cloud.

Gartner calculates that expenditure on public cloud services will surge from 9% of global enterprise IT budgets in 2020 to more than 14% in 2025. Its researchers have estimated that global spending in this area rose by 23% year on year in 2021 to $332bn (£249bn). They're expecting a further 20% increase this year.

"Humanity is generating ever more data," observes Maxim Melamedov, co-founder and CEO of Zesty, a provider of software designed to optimise cloud utilisation. "It's inevitable that we will see inflation in the costs of running, storing, managing and getting insights from this tremendous amount of data."

Businesses have been updating their IT infrastructure for more than a decade as they keep pace with digitalisation trends in their industries, but the process in many sectors has been accelerated by the Covid crisis. Industries ranging from retail and entertainment to financial services and travel have been going digital-first. They have moved their computing provision from small-scale, in-house data centres to the big public cloud providers, such as Amazon Web Services (AWS), Google Cloud and Microsoft Azure.

With providers carrying the risk and capital expenditure of running data centres and renting out storage and computing capacity, this already offers businesses considerable efficiency savings. But, even with these improvements, business leaders are starting to become sensitive to the scale of the investment required.

"Cloud costs are becoming more visible to the C-suite as a growing recurring expense," notes Martin Hosken, chief technologist for cloud services at VMware. This topic is "moving up the food chain in most organisations because it is so outcome driven – and CEOs care about outcomes".

Moving from in-house data centres to outsourced cloud provision can actually prove more costly at first, because it may take several months to transfer everything over. In that bimodal interim, companies are paying to use both systems.

A cost-saving tip from Hosken is for firms to rationalise the use of their apps during the migration rather than doing a 'lift and shift', in which the apps are moved at the same time.

While businesses will want their move to the cloud to be quick and efficient, they should first carefully assess each app they use to ensure it isn't consuming an unnecessary amount of processing power and storage space, he stresses.

Companies should keep their wits about them and beware of public cloud costs that can quickly escalate as applications scale up to millions of users. Providers offer the ability to cap usage and there are ways of reducing waste, so an app will consume computing resources only when necessary.

A cost-saving method that many companies have adopted is to use market forces and play competing vendors off against each another, Hosken notes. Rather than depending on a single provider for all their cloud needs, which would give them less bargaining power, they are using two or more in order to angle for discounts.

"We are seeing a lot more of the deliberate use of multiple clouds to reduce cost and improve bargaining power," he says. He adds that negotiations with vendors are typically managed by the chiefs of IT, finance and procurement, plus any director with the ability to strike a good deal.

This underlines the fact that public cloud provision has extended beyond a concern just for the IT team to become an enterprise-wide issue. With the entire C-suite focusing on ballooning cloud costs, there is pressure on the whole business to ensure that its use of the cloud is efficient.

The greatest cloud usage usually occurs on the customer-facing side of a business, but all other functions need to be aware of the costs they can control in this area. Some companies are setting up 'cloud centres of excellence', bringing together leaders from across the business to assess expenditure and decide where cutbacks can be made.

> **It's inevitable we will see inflation in the costs of running, storing and getting insights from the huge amounts of data we are producing**

The main public cloud vendors offer software that enables companies to analyse the costs of running individual applications. A company running a food delivery service can track the cost down to a specific app and establish the appropriate usage, for instance. In the same way, every business unit, including HR, R&D and app developers, can monitor the costs of their activities in the cloud and then see where any wastage is occurring.

Melamedov is a proponent of "right-sizing", which entails using software that can predict how much storage and computing power a company is likely to need over a given period. This enables cloud provision to be dialled up or down as and when needed to ensure optimal efficiency.

Sid Nag, vice-president in Gartner's technology and service provider group, agrees that companies need to keep a tight rein on their cloud usage. The holy grail of cloud computing is self-service, enabling end users to use the cloud under their own steam through self-service application programming interfaces.

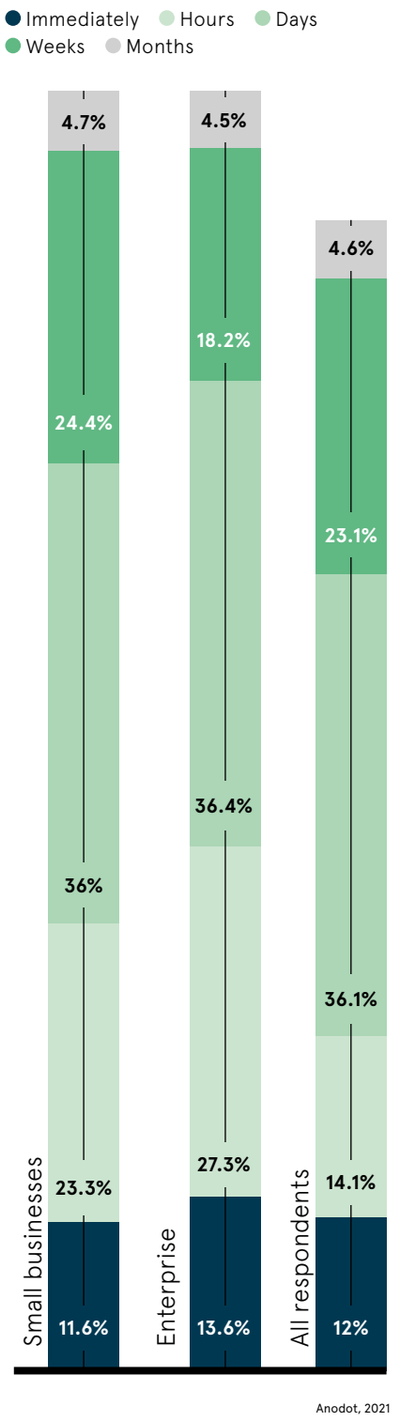
"But that approach has its hazards," he warns. "You also need to have oversight so that you don't have runaway costs and rogue and shadow clouds being stood up by your end users. You want to have a curated environment, such as a portal where you provide the end capabilities for your users to consume."

Data centres are massive guzzlers of energy, the cost of which is spiralling at present. But the big providers are all aiming to reach net-zero carbon emissions – Amazon, for instance, is the world's largest corporate buyer of renewable energy – and enterprises can use their cloud contracts to offset their own emissions.

It's clear that, as long as the costs of accessing transformational cloud technology keep rising at such a remarkable rate, the issue of how to control them will climb the C-suite's agenda at much the same pace.

NOTICING THE COST OF THE CLOUD

How long IT, finance and operations leaders say it takes to notice a rise in cloud costs



Anodot, 2021

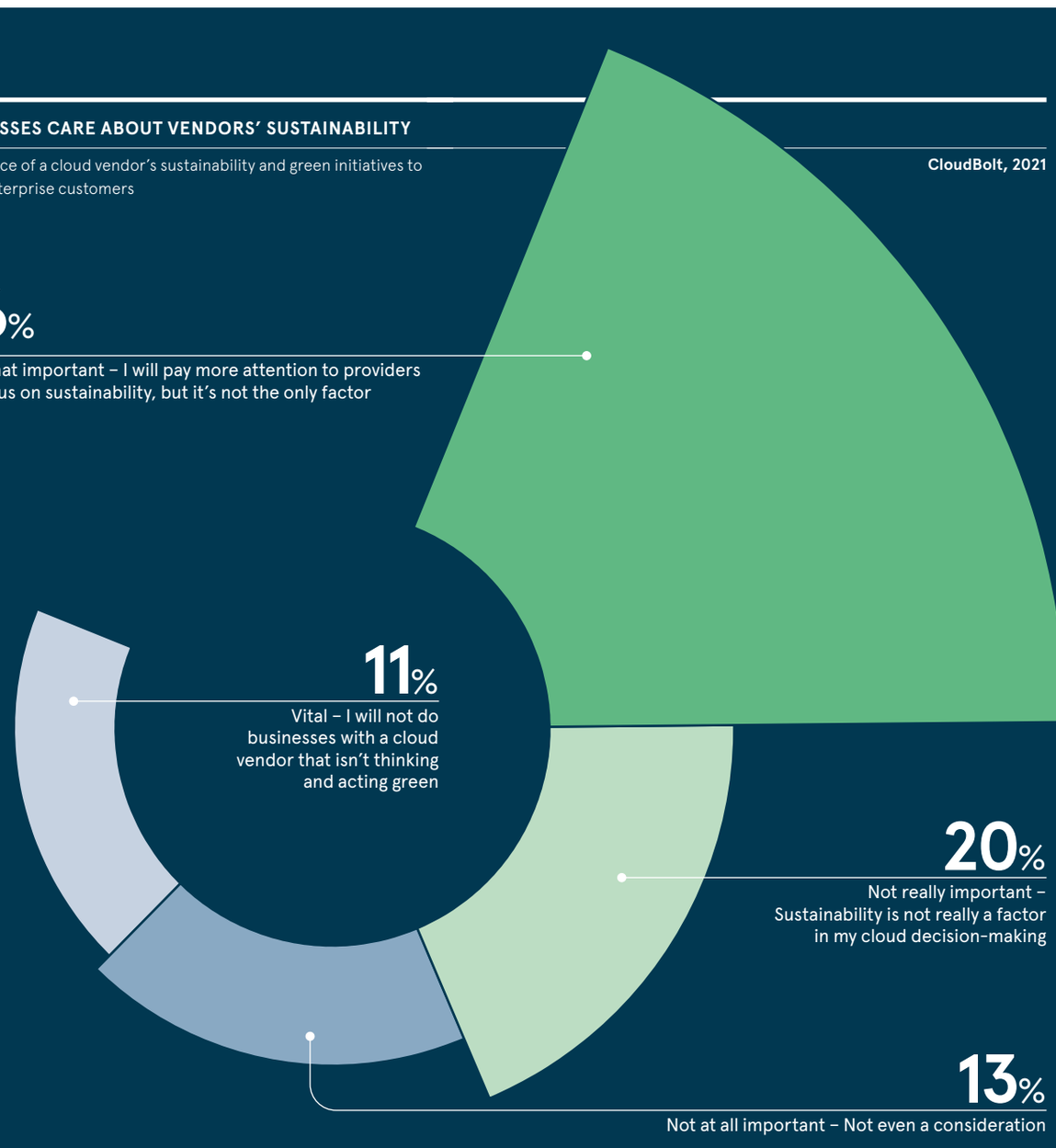
GOING GREENER WITH THE CLOUD

There are many reasons to move to data-led and cloud-based business models: the increased efficiency, the cost savings, the decision-making agility. But there is also an environmental case to be made. Businesses are increasingly concerned about their ESG credentials and there are opportunities to be greener by building sustainability into enterprise IT strategy

BUSINESSES CARE ABOUT VENDORS' SUSTAINABILITY

Importance of a cloud vendor's sustainability and green initiatives to global enterprise customers

CloudBolt, 2021



56%
Somewhat important – I will pay more attention to providers who focus on sustainability, but it's not the only factor

11%
Vital – I will not do businesses with a cloud vendor that isn't thinking and acting green

20%
Not really important – Sustainability is not really a factor in my cloud decision-making

13%
Not at all important – Not even a consideration

THE CLOUD HAS HELPED DATA SERVICES BECOME MORE EFFICIENT

Energy use by data centres globally

194tWh (2010) ▶ **205tWh** (2018)

Only a **6%** increase in data-centre energy usage

6x increase in computing capacity of data centres

10x increase in internet traffic

25x increase in storage capacity

Science, 2020

CLOUD PROVIDERS ARE MAKING EFFORTS TO BE MORE SUSTAINABLE

Carbon reduction goals of the world's largest cloud providers

Google, Microsoft, Amazon, 2021

Google	Microsoft	Amazon
2030	**2030**	**2040**
↓	↓	↓
Carbon free	Carbon negative	Net-zero carbon emissions

CLOUD STRATEGIES COULD BE BETTER

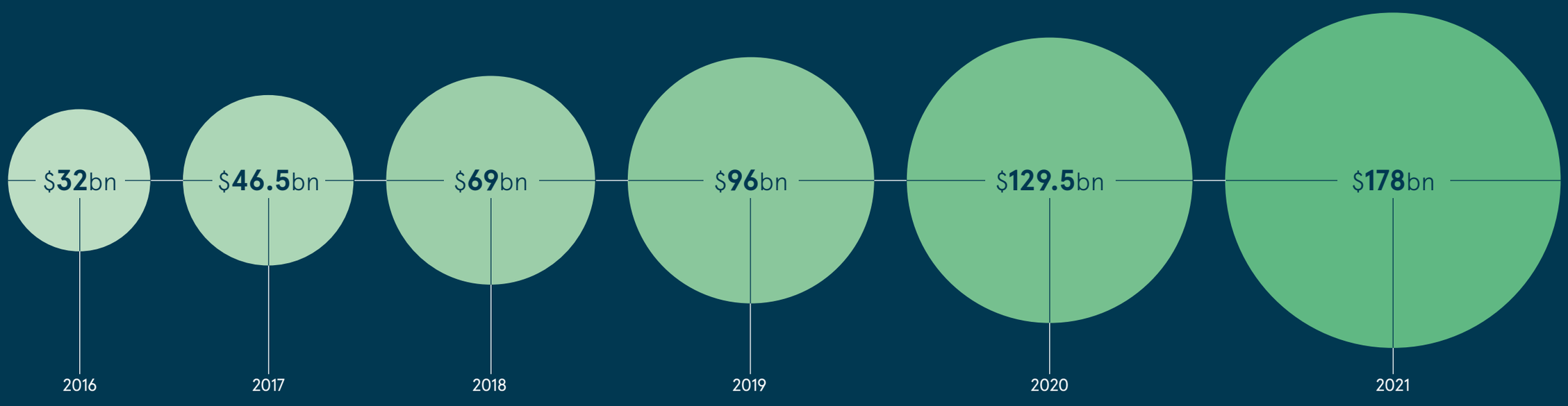
Percentage of companies that have taken measures in their cloud computing/virtualisation strategy to reduce their carbon footprint

Capgemini, 2021

BUSINESSES ARE INVESTING HEAVILY IN THE CLOUD

Enterprise spending on cloud infrastructure services

Statista, 2022



79%
of technology leaders said their IT departments were expected to help their organisation achieve its sustainability goals

CloudBolt, 2021

80%
potential reduction in energy usage by European companies that switch to the public cloud from self-managed data centres

451 Research, 2021

3.6x
positive difference in efficiency between cloud storage and average enterprise IT in the US

451 Research, 2021

1 billion
tonnes of CO2 emissions that continued adoption of the cloud could prevent from 2021 to 2024

Capgemini, 2021

> **For businesses using simpler cloud applications, the primary driver should be functionality, followed by security, compliance, scalability and cost**

CLOUD MIGRATION

Do sweat the small stuff

SMEs have as much to ponder as large companies do when considering cloud migrations. Even those on the tiniest budgets would be unwise to become preoccupied by providers' headline prices

Marianne Curphey

For several years, Peter Ambrose, MD of The Partnership, contemplated moving the 20 million files held by his business to the cloud.

Every evening, the 80 employees at the property law firm's offices in London and Guildford would back up the day's conveyancing documents, searches, emails and other correspondence to a huge bank of on-site servers.

"Each case generates about 160 documents," he explains. "Every time we created a document, we stored it. We needed to back up our data and keep it safe because it is incredibly sensitive personal information that includes bank details and identity checks. My top concern – which literally kept me awake at night for years – was whether that data was vulnerable to a ransomware attack."

Finally, after months of research and planning, in November last year The Partnership migrated all archived and live case data to a cloud service.

"It was scary – I'll make no bones about it," Ambrose admits. "Although we had done all the tests, until you've actually moved this huge amount of data, you worry about whether it's going to work."

The Partnership is one of a growing number of SMEs that have successfully moved their operations to the cloud. Another is Dakota Hotels. The luxury accommodation group needed a cost-effective cloud-based software solution that could be scaled up as the business grew.

It also wanted to harness the potential of the cloud to help with the HR challenges that the pandemic had forced upon the hospitality sector. As an additional benefit, the company gained greater insights into its costs and commercial opportunities.

"The time savings we've accrued by moving to the cloud have freed people up to focus on innovation," says the company's operations director, Andrew Ovenstone. "This has enabled our finance professionals to move away from number-crunching and become value creators."

All hotels under the Dakota brand compile their own profit-and-loss statements, which meant that a cloud-based solution would be an ideal solution to support multiple data entries. This has granted each hotel the autonomy to input data without compromising consolidation, reporting or intelligence at group level.

For SMEs, there are several key factors to consider when contemplating a move to the cloud. The first of these is the issue of cost versus opportunity.

"Cost matters for SMEs, but you also need to think about what moving to the cloud can enable for your business," says Dr Antonio Weiss, senior partner at The PSC, a consultancy that helps providers of public services with their digital transformations.

"If you hold data and applications on your premises, you probably run quite a restricted service," says Weiss, whose book, *The Practical Guide to Digital Transformation*, was published in February.

"The cloud enables huge possibilities in terms of data processing and analysis. It also offers better security and improved performance for your customers and staff. So, while you should aim to keep costs low in any cloud transition, you need to focus on how it can make your business better and to ensure that you have a plan to capitalise on this."

The second key factor to consider is flexibility. One of the challenges for The Partnership was to find a cloud provider that would store and register multiple versions of documents rather than providing a static record. This enables employees to return to the material and update it where necessary.

"We looked at Microsoft and Amazon Web Services, but found that they wouldn't work for us," Ambrose says. "We needed a system that could cope better with changeable data, so we partnered with Egnyte."

The third consideration is the level of functionality required in the short and long term. SMEs need to be realistic about what level of service and availability they will need, says Mairead O'Connor, executive for cloud engineering at AND Digital.

"Public cloud platforms enable SMEs to occupy the same playing field as big, cash-rich corporations," she says. "Every company has been granted access to technology like machine-learning tools. Until recently, functionality of this sort would have been out of reach to all but the biggest and most well-funded multinationals."

But firms should not adopt such technology without first considering their strategic direction. Cloud transformations are complex and, unless are executed properly, can lead to serious operational inefficiencies and data leakage. Before parting with any money, CIOs and CEOs should take a step back and review their business model.

Ash Finnegan digital transformation officer at Conga, an enterprise cloud computing and data company, observes that a lot of SMEs have been rushing their digital transformations.

"Regardless of their size, organisations need to complete a thorough assessment and understand where they are with regard to their digital maturity today," she says.

"This involves analysing their current operational model, identifying strengths and weaknesses, and establishing how they can better connect with their customers and serve them."

45%

of small businesses worldwide identify IT and security team staffing as a challenge to cloud security

Netwrix, 2020

60%

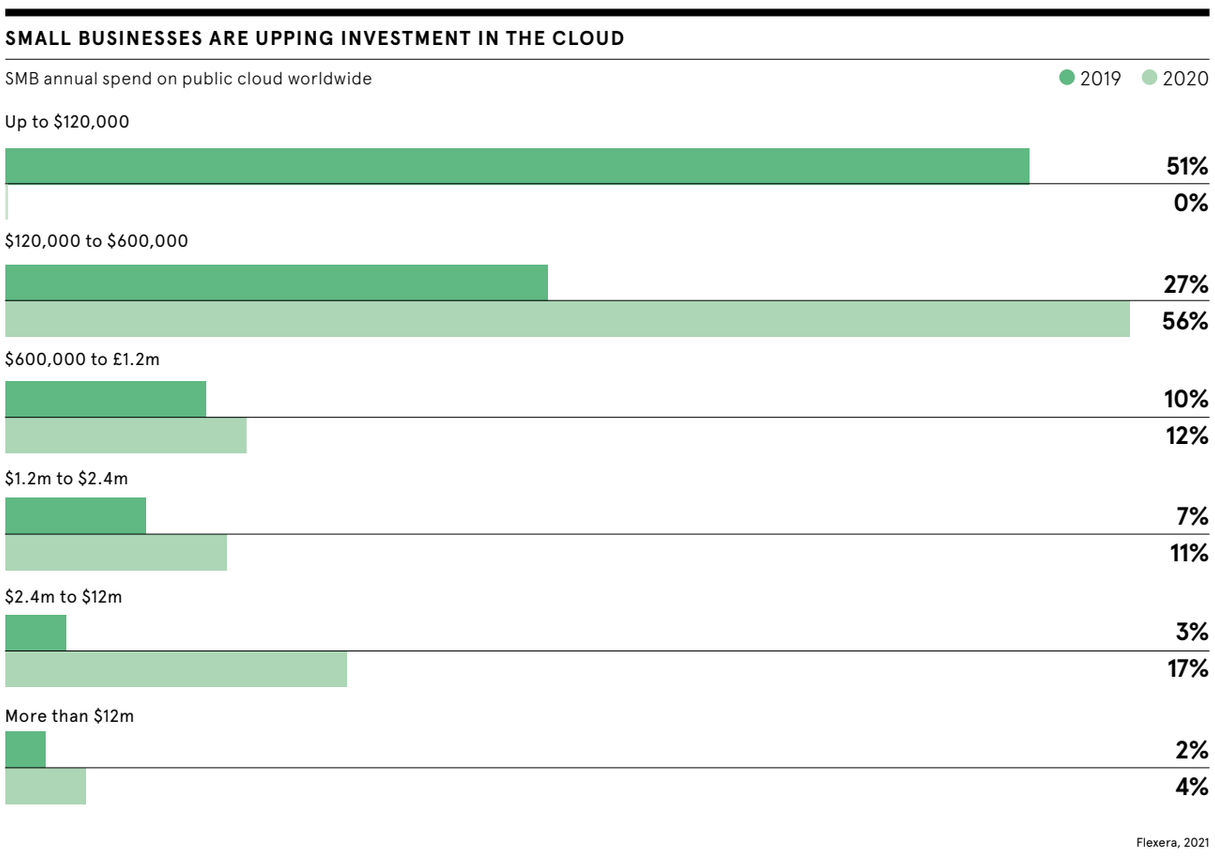
of small businesses worldwide have adopted multi-cloud solutions

HashiCorp, 2021

$863bn

amount spent by SMBs on IT services worldwide in 2021

Statista, 2021



The fourth key factor to consider is the likely level of service and tech support required. Despite the hurdles involved, migration to the cloud can yield many benefits, as The Partnership and Dakota Hotels have discovered.

Using subscription cloud services eliminates the need to maintain and upgrade technology, which can be costly and time-consuming for SMEs. But it is vital to establish exactly how much support you expect from your cloud provider and to be realistic about your own IT abilities.

The provision of adequate tech support is key for smaller firms, stresses Charlie Dawson, marketing and channel director at cloud provider Imscad Global. "There will be some SMEs with the resources to support their own cloud migration and provide ongoing support. Bt they should ensure the provider they choose offers a good level of support, including the ability to have issues resolved using in-person communication," he says.

Security is the fifth major consideration. For Ambrose, his decision to use a cloud service was prompted by the ongoing challenge of protecting The Partnership's in-house servers. Yet price and performance are often the first considerations for many SMEs, even though a loss of data could have catastrophic ramifications.

While factors such as affordability and capacity are clearly fundamental, most cloud providers offer only the most basic security features, especially at the budget end of the spectrum, warns Trevor Morgan, who is a product manager at data security specialist Comforte.

"This simply won't be enough if your highly sensitive information – on finances, intellectual property and customers – is destined for the cloud," he says.

Concerns about regulatory compliance will come to the fore here, especially for businesses in industries that require very strict risk controls – for example, defence, healthcare and financial services.

> **The time savings we've accrued by moving to the cloud have freed our people up to focus more on innovation**

"Each market will present different constraints, but companies operating in the same space may still have different appetites for risk," notes Dean Clark, chief technology officer at digital consultancy GFT Group. "The ideal balance between security, compliance, cost and functionality will depend on the individual organisation."

SMEs should also determine whether the solution they are considering has the right level of security for them in place. Two-factor authentication (2FA) should be a minimum standard, according to Lee Wrall, who is a director at managed services provider Everything Tech.

"We're seeing that some cloud solutions are putting 2FA into their future roadmap, but we believe it should already be there," he says. "For more robust infrastructure requirements, we'd recommend opting for bigger, more established solutions such as Microsoft or Amazon, as these provide features such as security, compliance and the ability to scale up as standard.

"For businesses using simpler cloud applications, the primary driver should be functionality, followed by security, compliance, scalability and cost."

Database requirements constitute the sixth and final key consideration. In the cloud, storage capacity is one of the measures that service providers use to charge for their offering. If you do not have significant volumes of data, the cloud may not provide value for money.

"For any company that needs some level of scale and availability, the cloud is usually the best option," says Andrew Oliver, senior director of product marketing at MariaDB, an open-source database provider. "For a very small database with merely internal users, hosting in house might be more cost-effective if the company has the time and expertise – and a careful plan for off-site backup." ●

OPINION

'We will need the insights and innovation that digital transformation brings if net zero is to be achieved'

The COP26 climate summit may be over, but the pivotal dialogue around how technologies such as cloud can help businesses achieve climate goals will remain at the forefront of the digital transformation discussion in 2022. Now, more than ever, businesses will be thinking carefully about their own net-zero strategies and how they can use technology to be more sustainable. The good news is that the cloud can be a big part of the solution.

At techUK, we work with our members to showcase how the latest development in cloud services can empower businesses to be effective, efficient and sustainable. In doing so, we are helping build that bridge between the cloud industry and end users, so they can work together to mitigate climate change. But how can cloud really empower UK businesses in the move to a more sustainable future?

Moving operations to the cloud means taking advantage of the higher use rates of on-demand infrastructure; more efficient cooling and newer hardware optimised by cloud providers; and the potential for more sustainable, flexible and resilient supply chains.

In fact, Accenture estimates that an infrastructure as a service (IaaS) migration could save the average business 65% on energy use and reduce carbon emissions from their IT systems by up to 84%.

However, unlocking the full potential of a sustainable cloud requires proactive engagement and shared responsibility between cloud providers and end-users to ensure efficient and effective deployment. Working together, they can navigate re-engineering legacy applications and developing the best procedures to measure carbon emissions associated with cloud workloads.

But at the heart of this approach must be effective data management, which can help businesses be proactive in identifying redundant or rarely used data.

This collaboration between cloud providers and end-users is crucial. Working together toward net-zero targets not only ensures efficient and effective cloud deployment, but also places end-users in a favourable position to expedite the sustainable adoption of exciting emerging technologies such as high-performance computing, machine learning and quantum technologies.

These emerging technologies will open access to previously unattainable services and solutions that could enable and drive innovation in areas such as pharmaceutical research and drug discovery and the development of next generation communications infrastructure. But it will also provide the technological architecture for areas supporting the climate change fight including battery optimisation and even carbon capture.

While the future for the planet is still uncertain, what is clear is that as we move forward from COP26 we need the insights and innovation a cloud-powered digital transformation will bring if a thriving modern economy and net zero is to be achieved. Cloud can be a catalyst for discovery in fields like energy, transport, and climate science by opening access to other emerging technologies like AI and quantum computing.

But we also must remember the fundamental ways in which the effective and efficient adoption, deployment and use of cloud services can help support and empower businesses to achieve their net-zero ambitions and help us all build a more sustainable world. ●

48%

of global companies identify cloud migration and going cloud-first as a priority for IT and tech teams

Flexera, 2021

64%

of global businesses expect cloud infrastructure to be one of the most impactful industry 4.0 technologies

Deloitte, 2020

Sue Daley
Tech and innovation director
techUK

CLOUD CONCENTRATION

Stormy skies ahead for financial risk?

The tech underpinning the world's financial system is dominated by three cloud operators. Regulators believe that new laws are necessary to manage this concentration of risk

Mark Taylor

In ditching their outdated, expensive and inefficient operational software for advanced cloud platforms, our tech-addicted banks may have swapped one set of risks for another.

Regulators worry that so-called cloud concentration – relying on a tiny group of providers to provide key services – could trigger the next global economic meltdown if left unaddressed.

"If the world's financial market infrastructure ultimately sits with two or three cloud providers, the risk of one of those going down could easily pose a bigger threat to financial stability than the collapses of Lehman Brothers or Northern Rock, if not managed correctly," warns Bradley Rice, financial services partner at Ashurst.

In the past decade, banks have flocked to three main providers: Microsoft Azure, Amazon Web Services (AWS), and Google Cloud. These three behemoths have the scale and resources to handle the security, maintenance and data processing demands of the global financial system.

Research by S&P Global found that about 45% of financial services firms use AWS as their primary provider, with Azure clocking a similar percentage. Those with more than one cloud provider employ a second from the same trio. Azure is used in some form by 79% of financial services firms.

Regulators are concerned. In the UK, the Financial Conduct Authority (FCA), the Prudential Regulation Authority and the Bank of England have all warned of cloud concentration risk. They are meeting industry representatives to stress the dangers of relying too much on outsourced services.

What happens if a cloud provider is taken out by a hostile force or otherwise fails? There are also competition concerns: given the amount of responsibility and power the trio hold, there are fears that they could hold firms to ransom.

"If significant numbers of companies in the industry are running on one cloud provider, that provider becomes a systemically important part of the financial system by default," notes Bo Svejstrup, executive vice-president of COO functions and data at Danske Bank. "If that provider has an issue that causes services to become unavailable for an extended period, this could create systemic problems at national or even regional levels."

Cloud adoption has soared during the pandemic. But Covid isn't entirely to blame for the present situation, according to the head of resilience at one UK investment bank. Commenting anonymously, he says that the City has been shifting operations into the cloud to save money for many years.

"This move has taken place in isolation without wider design or consideration for systemic operations," the executive says, adding that little thought has been given to what would happen should a cloud provider pull the plug or suffer a widespread failure.

"Nobody is doing anything. That's because most big players – Amazon, Google, Microsoft and so on – do not care about some UK bank dictating that they need to send resilience assurance," he claims.

Given the software giants' reluctance to undergo the same forensic examination that their finance clients face, regulators "will have to row back on some of their expectations and deadlines", the exec says.

"I hear the same thing – 'my third parties aren't playing ball' – on industry calls I go on," he adds. "It's not realistic to ask banks to consider alternatives to their cloud systems, because the cost and scale of doing that is not sensible."

Microsoft, Google and AWS are all declining to comment on this issue, as is the FCA. The Bank of England is making no official comment either, but a Bank executive will at least confirm that it has spoken "a fair bit" about the cloud and its respective risks in the past year. It considers the matter "significant" and is meeting industry representatives, the executive says, adding that new policies and laws will be needed to mitigate the stability risks.

Such legislation will invariably try to catch up with new technology by adding to operational resilience demands, says Jonathan Emmanuel, partner at Bird & Bird. But he says firms should continue to think in terms of perceived risk versus the actual risk of retaining archaic legacy systems.

"Regulators are trying to ease firms into a new way of thinking, but it will not be long before we see some major enforcement action over an operational resilience failure," Rice adds. "Ultimately, I think we will see regulators around the world regulating critical infrastructure providers, like the cloud providers, data providers and other market infrastructure providers."

> **It's not realistic to ask banks to consider alternatives to their cloud systems, because the cost and scale of doing that is not sensible**

For banks themselves, there is no future scenario where the cloud becomes less important or central to operations. "Many financial services organisations now see themselves more as technology companies that happen to operate in a regulated sector," Emmanuel says.

Some have no physical presence whatsoever. Their data is spread across geographies rather than hosted on the premises, as was the norm a decade ago. Starling, for example, offers a 100% digital service; it is acutely aware of concentration risk.

"From conception, Starling has deployed its systems and services across multiple clouds which work to back up our data in real time," says Steve Newson, the bank's chief technology officer. "By doing this, we ensure that we aren't dependent on one single third-party supplier and we reduce risk."

Danske Bank also operates with a multi-cloud strategy, accessing various services from different providers.

"For any service provider, we must have an exit strategy allowing us to migrate the service to another provider or to an in-house solution at any point," says Svejstrup. This covers the hazards of services being unavailable for whatever reason, including a contract dispute between the bank and its cloud operator.

The way forward is to employ a more rigorous approach to resilience, Svejstrup says. The degree of exposure to different providers should be transparent for both regulator and industry, adding transparency to some complex relationships.

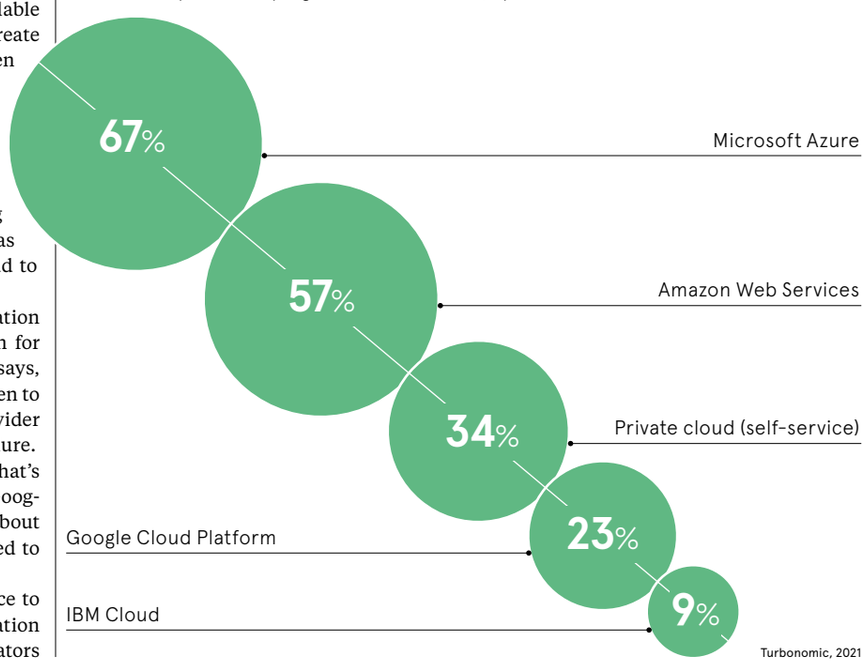
"Every institution needs a clear overview of its exposure to cloud providers as well as clearly defined and well-tested exit plans," he says.

Industries beyond financial services should heed the lesson and avoid becoming seduced by a single big-name cloud provider promising to take care of everything.

"This fundamental practice is also good for other sectors that provide systemic and critical functions," Svejstrup says. "It reduces the risk of outages, instability and poor service quality, whatever you provide."

MICROSOFT AND AMAZON DOMINATE THE CLOUD MARKET

Use of cloud providers by organisations worldwide, by vendor



Turbonomic, 2021

HOSTING ENVIRONMENTS

Contrary motion: the case for staying single

If companies such as Netflix and Spotify don't see much value in adopting a multi-cloud approach, why are so many smaller firms so keen on the model?

Charles Orton-Jones

Without the mavericks who are prepared to challenge received wisdom, the business world would be a lot less dynamic – or interesting, for that matter. Take Paul Graham, co-founder of the startup accelerator Y Combinator, for instance. Renowned in Silicon Valley for his ability to pick a winner, he recently admitted that he'd never read one business plan or balance sheet supplied by firms seeking an investment from him.

Graham's justification? "The reason I don't care about business plans is that I can learn more from five minutes of interrogating the founders than I can from reading the 10 pages of fluff they've written."

And consider fintech unicorn Bolt, which broke its industry's norm of long working hours by adopting a four-day week in September 2021. Acknowledging that it was an experiment, the firm's founder and executive chairman, Ryan Breslow, explained at the time: "People are done working like cows for five days. They are ready to work like lions for four."

There are contrarians in the cloud computing world too. When the consensus overwhelmingly favours hosting applications using a multi-cloud solution (the use of two or more computing services from any number of vendors), a small minority resolutely back the single-cloud model.

But why? The multi-cloud model offers clear advantages for users. For instance, it makes it possible for them to haggle on prices and select the best-value vendor for each service required, because some providers are better than others for certain tasks. In essence, it gives users the choice and modular flexibility that a single-cloud approach clearly cannot provide.

Of the 1,700 IT decision-makers polled in a survey for US cloud computing firm Nutanix in September last year, 83% agreed that a hybrid multi-cloud approach was ideal.

Do the refuseniks have a convincing argument? Is the single-cloud model worth sticking with if no one provider can offer the best value for all services?

> **For some, multi-cloud is essential. For others, it's an aspirational money pit**

Scott Riley, founder of consultancy Cloud Nexus, is proud to be a contrarian. He blasts what he sees as three widely held myths associated with the multi-cloud approach.

"The cost differences between the main hyper-scale cloud providers are not that significant unless you're prepared to make a multi-year commitment," he says. "You have the price or you might buy through a distributor for a 10% discount."

The concept of using multi-cloud to geolocate data is also wrong, argues Riley, who says: "All hyper-scale providers have multiple geographical data centres with individual fault-tolerant platforms."

It's a fair point. Where in the world is beyond the reach of the major cloud hosts these days? The Pitcairn Islands, perhaps?

Then there's resilience. Is it really correct to say that multi-cloud is inherently better in this respect?

"Load distribution has to happen somewhere," Riley says. "Take an inbound request and pass it to the nearest, or least busy, server in any given cloud. Where does this sit: cloud A, cloud B or a third cloud? Wherever it sits, whenever that platform has an issue, no one is getting to the application, regardless of how many cloud platforms you've deployed it to."

Security is one of the biggest aspects of cloud strategy. There's a widespread belief that using several providers is a more resilient approach than relying on one.

But that's another popular fallacy, says Tim Erlin, vice-president of strategy at cybersecurity company Tripwire.

"There are good and valid reasons to have a multi-cloud strategy, but security is not usually one of them," he says. "The security advantages are dubious at worst and require significant investment at best. Most often, the security benefits are ascribed to the protection that multi-cloud gives against distributed denial-of-service [DDoS] attacks, which is really a rehash of the resilience argument."

Achieving resilience requires a substantial outlay – and there are better ways of doing so than adopting a multi-cloud approach, Erlin argues.

"Building a multi-cloud infrastructure that allows for seamless failover [the facility to switch automatically to a back-up system] across providers requires specific investment. It's not simply an emergent quality of having multiple providers," he says.

"This might be a worthwhile investment for businesses that require that level of availability and/or are at a high risk of DDoS attacks, but it should be considered alongside alternatives that might mitigate the risk at a lower cost."

Maybe the biggest argument in favour of a single-cloud strategy is the simplicity it offers. David Liddle, senior cloud security consultant at Adarma Security explains: "In addition to insider threats, cloud misconfigurations are one of the biggest issues facing users. These misconfigurations, which range from overly permissive policies attached to identities to poorly configured security groups, can be introduced in several ways.

"Spotting them in a single hyper-scale environment can be extremely difficult. With a multi-cloud approach, the problem of eliminating misconfigurations becomes even more difficult."

Then there are the risks of migration. Moving from a single host to multi-cloud is a serious undertaking. It requires virtual machines (VMs) to be stripped out, because cloud hosts, while similar in functionality, have their own quirks. A VM that runs on Amazon Web Services (AWS) may not run on Microsoft Azure, for instance.

Companies need to be sure they've got the right monitoring tools in place to run a multi-cloud spread. Every extra element is a point in favour of the simplicity of the single-cloud approach.

Perhaps the most convincing evidence is from the tech giants. Netflix, for example, runs computing and storage exclusively on AWS. It trialled a multi-cloud operation briefly in 2018 before committing to a single provider. Netflix is no ordinary customer – at one point it accounted for 15% of all global internet traffic. If it felt that using only one provider were too much of a risk, it surely would have diversified by now.

Spotify prefers one provider too, having migrated from AWS to Google Cloud in 2016. The company's vice-president of technology, Tyson Singer, said last year: "There's simplicity in having a single cloud. It saves us a lot of hassle and complexity."

The approach Netflix and Spotify have adopted is still unfashionable. Multi-cloud is the default option, but it's useful to know the arguments for and against.

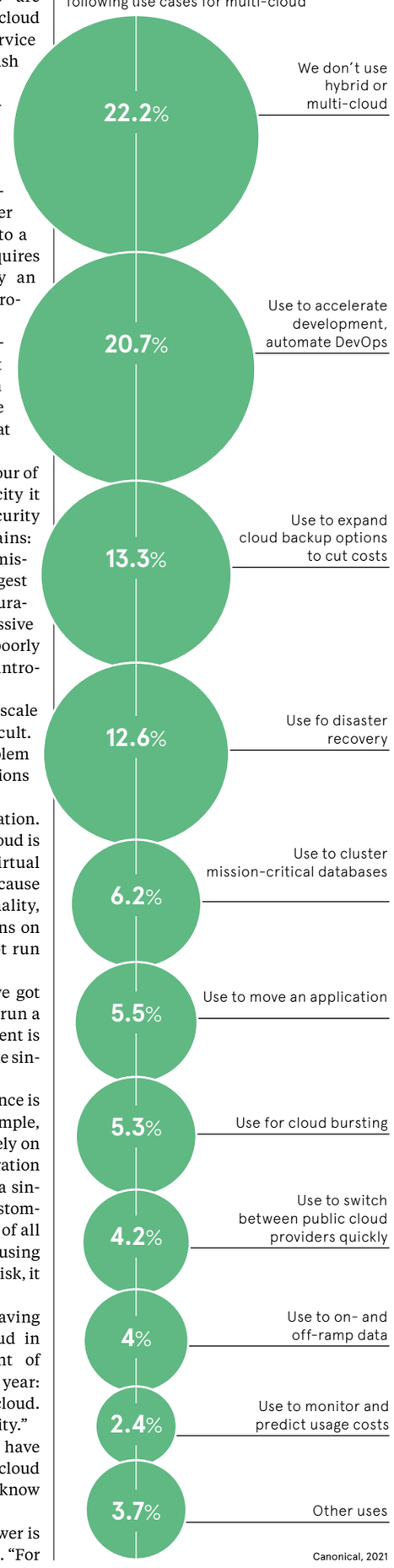
"Is multi-cloud advisable? The answer is far from straightforward," Liddle says. "For some, multi-cloud is essential. For others, it's an aspirational money pit."

Smaller companies in particular may feel emboldened to keep things simple. If they do, they can take comfort in pursuing a strategy that suits a pair of digital giants.

Trends don't last forever in business. Contrarians act and followers emerge. Running a single-cloud strategy may feel awkward, but you may simply be ahead of the technology curve.

MANY USES FOR HYBRID SOLUTIONS

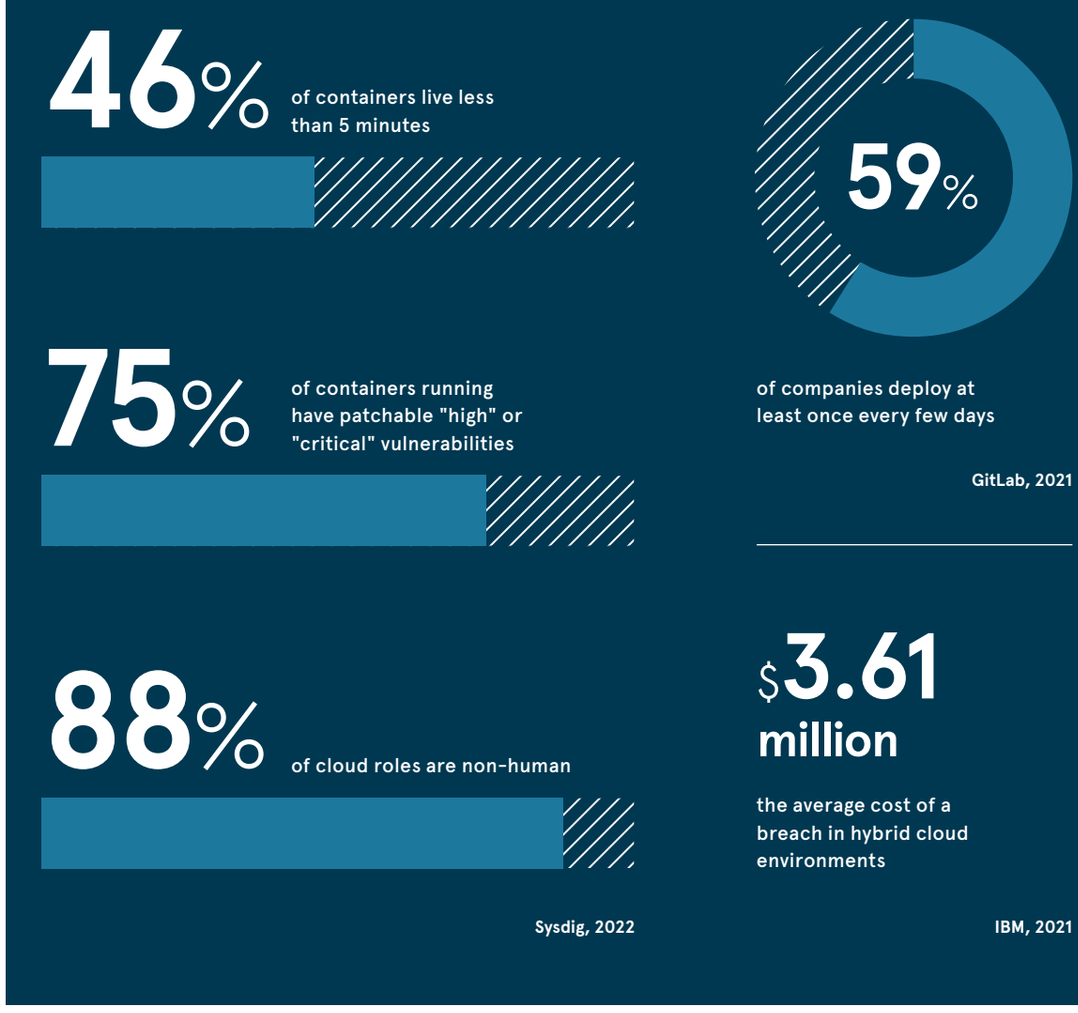
Percentage of IT professionals who cite the following use cases for multi-cloud



Canonical, 2021

MOVING AT THE SPEED OF CLOUD

Transforming Development for Cloud Has Security Implications



A new horizon for cloud security through DevOps collaboration

An effective cloud strategy enables development and security teams to work in tandem. Such cross-departmental collaboration is crucial as cloud-related security threats grow

The benefits for companies when moving software and application development to the cloud are well documented, chief among them being speed, agility, scale and potentially lower costs. But when undertaking this powerful transformation, a huge opportunity must not be overlooked - the chance to reinvent your company's mindset around security.

According to the GitLab 2021 Global DevSecOps Survey, 59% of companies deploy in the cloud at least once every few days. This makes it no longer viable to have dev teams who only develop and release, with security teams working in a separate silo to test for bugs and threats afterwards. Instead, the cloud offers an exciting new age of collaboration, embedding security considerations into the development process itself to ensure these no longer represent a barrier to the speed of a release.

As use of the cloud by organisations matures, three themes are fundamental to success: embracing a more frequent methodology for continuous software releases; breaking application development into microservices, connected via APIs; and recognising the wider risks due to increased resources and broader access in the cloud.

All three themes have security implications and require important decisions to be made. But all can be tackled by moving security upstream, identifying vulnerabilities, and implementing fixes much earlier in the software lifecycle. A mindset change to continuous monitoring will also be critical.

When working in the cloud, greater real-time monitoring is crucial to safeguarding a company's cloud operations. This is due to the dynamic nature of cloud-native, where - according to Sysdig's 2022 Cloud-Native Security and Usage Report - nearly half of microservices running in containers live for less than five minutes.

DevOps and security teams must think very differently about how they do their jobs and collaborate using a common set of tools. Tighter interactions will allow them to grow more confident in each other's responsibilities and outcomes, addressing risks earlier in the software development process.

Meaningful change is then driven from two directions.

First, the mindset of the chief information security officer (CISO) must move from guarding the perimeter to accepting there are no defined boundaries to control in the cloud. You cannot keep track of everything that happens, so you need the right protocols to continuously look for unusual activity, allowing security and developers to react in real time.

In parallel, the developer mindset must change too, from building to get functionality out fast at any cost, to considering security during the development process itself.

It is in nobody's interest to compromise security for speed. One data leak, or cyber-attack, causes huge reputational damage. IBM found the average cost of a breach in hybrid cloud environments to be $3.61m.

Developers are usually responsible for functionality, performance, and user experience, but the cloud allows them to also become guardians of security. Trust is key here; trust between security and development teams and trust within the C-suite. However, it takes a counterintuitive approach to achieve it. The more you build automated checks to confirm processes are followed, the easier it will be for developers and security to collaborate and trust each other.

> **Embracing the cloud, with its more automated development processes, is a huge step forward in mitigating security risks**

The cloud makes it easier for developers to address vulnerabilities before releasing applications, collaborating with security teams to prioritise issues and continuously monitor compliance with policies.

Implementing these further upstream in the development process is a huge change in process and mindset, but the risks involved mean it's far better than raising issues months down the line and hoping they get taken care of. Everyone benefits from having less fixes to implement. Nobody wants to hold up a release, so this is a shared goal.

The cloud also allows a switch from a command-and-control approach to a trust-but-verify one.

Prevention of risk is never complete. Sysdig's 2022 Cloud-Native Security and Usage Report found 75% of containers running have patchable "high" or "critical" vulnerabilities.

This necessitates a mindset of acceptance that not every risk can be prevented, and that detecting and responding rapidly becomes key.

Implementing continuous monitoring in real time gives security teams confidence that they can find threats and anomalies before they do any damage, rather than after a breach has occurred.

Covid-19 forced many companies to develop new apps and services fast. For Worldpay by FIS, contactless payments by voice, retina, and digital mediums were reprioritised quickly. This pivot was only possible because they already worked in cloud environments. As new applications were developed, time was saved by adopting tools like Sysdig to scale visibility across environments and accelerate identification and remediation of vulnerabilities.

Scanning for vulnerabilities in the development pipeline ensures the most appropriate devs – those responsible for particular areas of the code – can focus fast on the right priorities for a fix. Both sides can also combine their experience to quickly understand if a problem is real or not.

Due to the fact that containers have short lives and they may quickly disappear, it is critical to keep a detailed record of what happened to investigate incidents down the line.

This is a new age of shared responsibility where the gatekeepers and builders no longer spend six months developing software or applications, only to be slowed by vulnerabilities or bugs.

Importantly, businesses should not fear a move to the cloud simply because of highly publicised security breaches. Sticking with current on-premises solutions is risky. Breaches still happen on-premises, they are just less public.

Embracing the cloud, with its more automated development processes, is a huge step forward in mitigating security risks.

Security teams therefore should become empowered to sit alongside developers, so they can understand how to make something happen, rather than forcing devs to roll back weeks of work.

If your company is willing to change its mindset to recognise the benefits of collaboration between developers and security teams in the cloud, you will soon speed innovation, enable agility and deliver scale. Those are compelling reasons why any company should move to the cloud in the first place.

For more information please visit sysdig.com/cloudreport

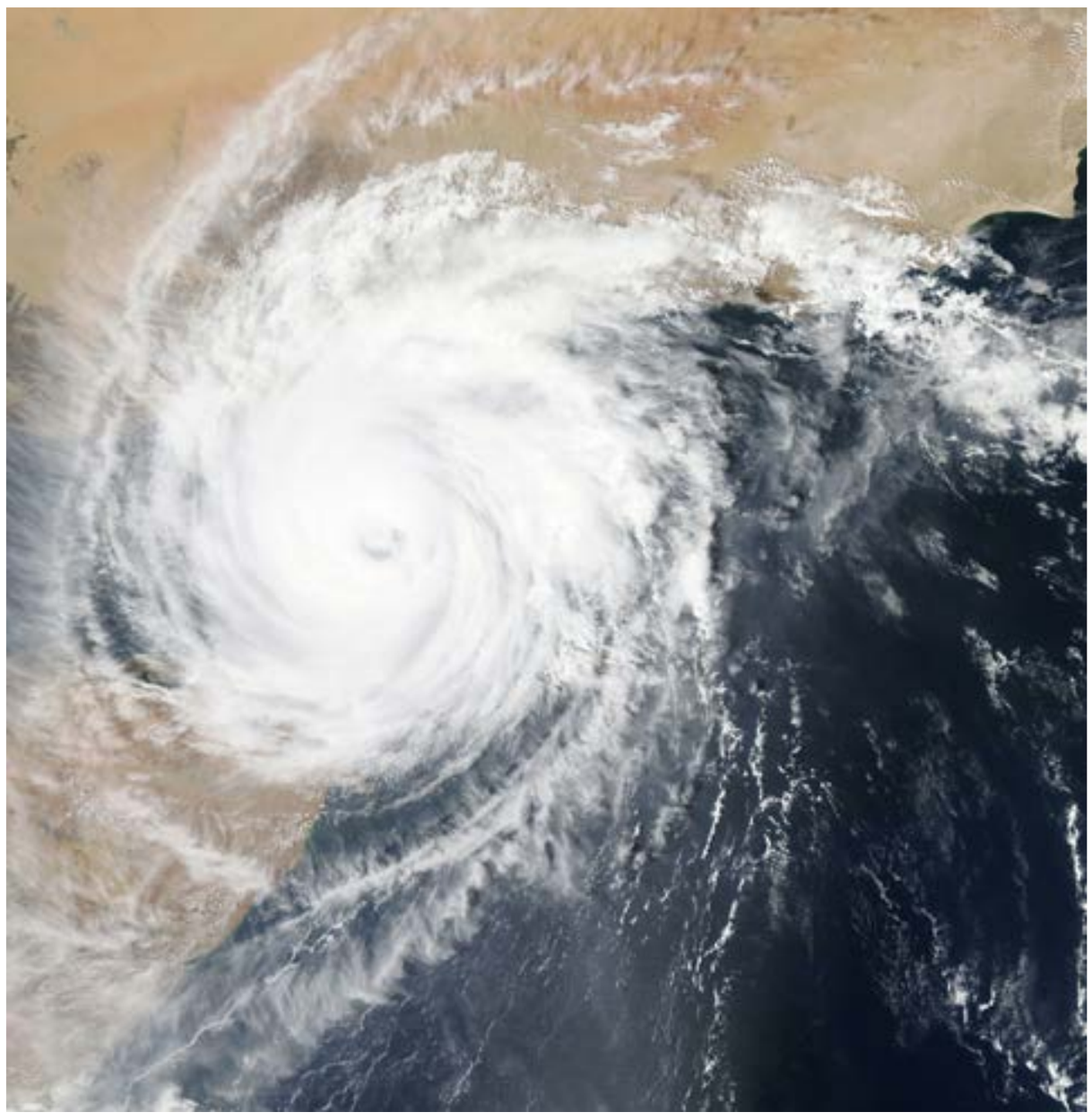
sysdig

OPINION

For cloud users, there is a struggle to predict the weather

Cloud computing is becoming more democratic and open yet predicting where it will go next remains difficult even for experts

Adrian Bridgwater



Cloud computing has grown up. In the past two decades, the technology industry has fought against an occasionally brittle approach to security provisioning with an increasingly sophisticated set of cloud functions.

We now have access to a far more evolved notion of software-as-a-service technology. This is the era of 'cloud native'. Natively built cloud services – which never existed in any kind of terrestrial version – are now coming to the fore. What factors, then, should you consider when working with cloud computing?

Adam Selipsky is CEO of Amazon Web Services (AWS). He's been candid about cloud computing's somewhat difficult adolescence: at the start, he says, it was expensive, slow and inflexible.

Cloud vendors sought to achieve customer lock-in where they could, with interoperability far from an engineering imperative. That time has thankfully passed, and a new, more democratic and open approach to the cloud has prevailed.

"People used to question me about Amazon Web Services and ask what the connection with books was, but I think things have moved on," said Selipsky, who was speaking at his firm's AWS re:Invent conference in December 2021.

Vendors large and small are putting a huge effort into making cloud services more consistent and easier to consume and use. Cloud specialists like to call this a simplified unified platform experience, but we could just call it cloud that works.

One of the companies talking in these terms is enterprise cloud specialist Nutanix. The firm has described its latest platform refresh as a simplified portfolio that brings together 'rich product capabilities' across private on-premises and public clouds. This aims to deliver consistent infrastructure, data services, management and operations for applications in virtual machines and containers.

Senior vice-president of product management at Nutanix, Thomas Cornely, has said the firm has focused on delivering a simplified portfolio that delivers a consistent infrastructure with data services, as well as management tools.

This theme resonates throughout the cloud vendor glitterati. It further echoes in the wider enterprise software platform space, which includes services such as enterprise resource planning (ERP) and customer relationship management (CRM).

It's easy to see why it matters. Enterprise software is often too complex to purchase, let alone run; sometimes that is down to acquisitions, or because of product launch sprawl or relabelling existing services.

> **Cloud computing offers flexibility, scalability and changeable manageability, but only if we understand which direction the wind is blowing**

The resounding message coming from the cloud industry is a promise. The vendors tell us they understand that customers need to work across private and public clouds with a simplified application and data services product portfolio that is charged with more straightforward billing.

In practice, while cloud billing might be a dry topic, it's a hot issue. Let's remember, there is no actual cloud, as such. It's just a global collection of server units housed in international data centres, running management software with various different optimisation parameters to make different virtualised cloud services behave and perform in different ways.

But how that's all packaged and sold matters a great deal. The cloud industry has worked hard to simplify its packaging, metering and pricing structures. Take the use of so-called 'reserved instances', where customers agree to a specified amount of cloud based on knowledge of their own predictable IT workload requirement. That's helped in some cases, but not in all.

Facebook's founder and CEO Mark Zuckerberg famously complained that cloud is too expensive back in 2019. Still, the reality of cloud that can be turned on and off, providing the ultimate OpEx-only flexibility, is still something of a pipe dream.

Not everything is quite as perfect as the branding claims would have us believe. Even the most ardent evangelists typically agree that cloud perfection – and indeed cloud-native – is still a work in progress.

We should also remember that enterprise cloud is not just for Christmas. Customers need to think about ongoing supporting services, from load balancers to specialised accelerators to advanced security monitoring – and that's just a start. Then there's upgrades, testing and system maintenance: just like Windows, clouds need patch updates, too.

If cloud computing has been guilty of anything, it has been too shiny and new. The idea that we might all be able to tap into hyperconnected computing services built on virtual 'machines' running in cloud datacentres was always quite radical. Giving everyone massive computing power in the palm of our hand was a dramatic amplification of the internet's initially promised freedoms. In short, it was a lot to take on.

The drive to cloud migration is, of course, one of the central moves repeatedly cited in the oft-discussed journey to digital transformation most companies are on. But to make this journey, enterprises need a plan, a toolset and a capability arsenal.

Brent Schroeder is chief technology officer for enterprise-grade open-source solutions specialist SUSE. He says his firm has seen companies dramatically shrink their cloud migration windows. With the effects of the Covid-19 pandemic still playing out, Schroeder reminds us that 'traditional' IT deployment windows of 90, 60 or even 30 days are now too long.

The way forwardis process, planning and precision-engineered software production, he says. SUSE insists customers work with private cloud and public cloud infrastructure that is consistently deployed within robust security and governance guidelines.

In other words, organisations shouldn't make the change to cloud without change management. As we make these changes, we can now shoulder a good deal of our total cloud software application lifecycle by using infrastructure as code (IaC), though that's another subject for analysis in itself.

Cloud computing offers flexibility, scalability and changeable manageability, but only if we understand which direction the wind is blowing. The power of this weather system is still forming, so please make sure you wear a coat.

284%

increase in public cloud application SaaS end-user spending worldwide from 2015 to 2020

Proofpoint, 2021

£366bn

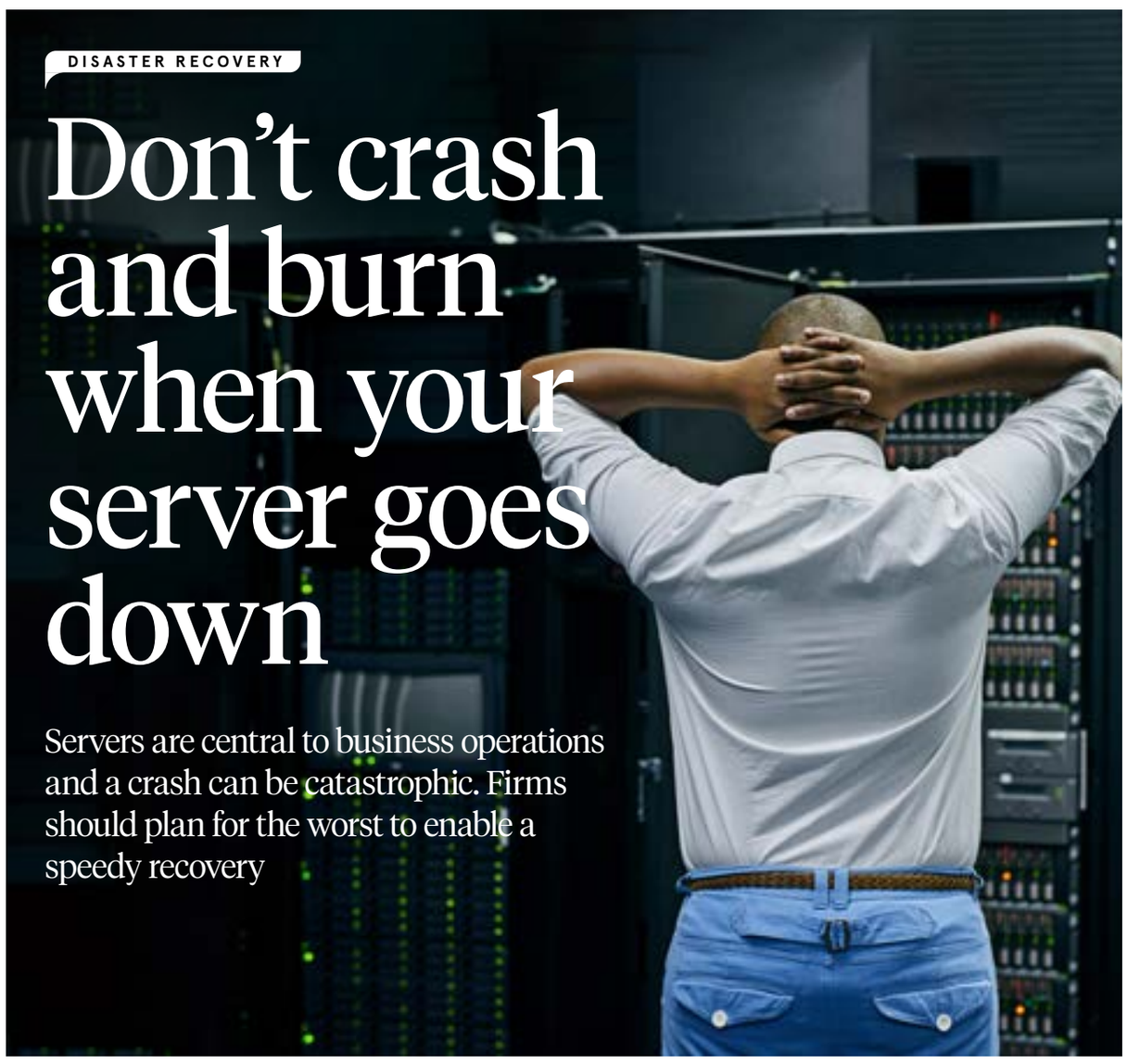
projected spending on public cloud services worldwide in 2022

Gartner, 2021

DISASTER RECOVERY

Don’t crash and burn when your server goes down

Servers are central to business operations and a crash can be catastrophic. Firms should plan for the worst to enable a speedy recovery



Peter Archer

Nationwide customers faced repeated disruption to their banking services around Christmas, unable to access their funds or pay their bills. While the building society described the outage as a “technical issue”, some experts identified a server failure.

The disruption demonstrated just how much damage a tech crash can cause and the salient importance of servers for smooth business operations, with millions of users unable to receive or make payments.

Whatever the causes of a server crash – ranging from simple hardware failure and power outages to software glitches, cyber-attacks and natural disasters – the consequences can be catastrophic. Businesses, big and small, rely on connectivity; in a digital age, it’s the lifeblood of commerce. The result is that organisations have become increasingly reliant on servers.

As screens go blank, digital and human connections are cut. The afflicted organisation loses productivity, orders and profits, while customers are affected, causing reputational damage and possible loss of future business. In addition, if private data is lost, regulatory fines and penalties can result, as well as class-action lawsuits.

Servers support essential connections, which facilitate business operations including interaction with staff and customers. Their importance means more and more companies use a network of cloud servers.

These servers now play a vital role in business technology. They provide a central repository to receive, store, retrieve and send data, ensuring all team members have timely access to the information they need.

Web, email and file servers, to name just a few, are essential for employees, teams and systems to perform the tasks that make up their jobs. The pandemic and resulting shift to remote and hybrid working have necessarily accelerated data-centric, cloud-based digitalisation, so businesses have become increasingly dependent on the uninterrupted operation of their servers.

But have servers – a computer with advanced hardware running a server program – become an Achilles’ heel? Essential to business operations, what happens when servers crash? How can an organisation recover quickly and get back to work?

Azeem Javed is a consultant at Creative Networks, managed IT and telecoms specialists. He says that encapsulating backup as part of a business continuity and disaster recovery (BCDR) strategy “is critical for all businesses, ensuring continuity of their operations and suitable recovery.”

Contingency planning and a system backup strategy – installing locally based or remote backup servers or backup to an external hard drive and disaster recovery software – can certainly help the chief technology officer sleep more soundly at night. If a business has alternate backups for its files, it can quickly bounce back and resume operations.

A full backup is a complete copy of an organisation's data assets. This process requires all files to be backed up into a single version. However, the dataset should be copied in its entirety and stored in a separate location, away from the server.

Such an offsite backup, which can be accessed, restored or administered from a different location, guarantees high-level security and peace of mind as it allows data storage offsite and online.

> **If your data is critical to your business, backup servers are vital to ensure business continuity and avoid data loss**

“If your data is mission-critical to your business, backup servers are absolutely vital to ensure seamless business continuity and to avoid data loss,” says Jake Madders, a director at Hyve, a managed cloud hosting provider.

“We now live in an ‘always-on’ world, where just one hour of downtime can cost anything from thousands to hundreds of thousands of pounds, depending on the size of a company. Time is money.”

Irrespective of the location of the server, it is essential to have a BCDR plan in case the worst-case scenario occurs.

“The pandemic has forced companies to realise that being prepared for even the most unlikely situation can no longer be treated as an optional part of business planning,” says Madders.

“While it might seem difficult to measure the return on investment of a disaster recovery solution, because it’s a precautionary feature that ideally would never need to be used, it shouldn’t be seen as a ‘luxury’ add-on service solely for larger companies. It should be a fundamental part of every business’s IT strategy.”

A disaster recovery plan is a documented, structured approach that describes how an organisation can quickly resume work after an unplanned incident. It is an increasingly essential part of a business continuity plan and should be applied to the aspects of the operation that depend on a functioning IT infrastructure - likely most of it.

The step-by-step plan consists of precautions to minimise the effects of a disaster so the organisation can continue to operate or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs.

Before generating a detailed plan, an organisation should perform a business impact analysis and risk analysis, and establish recovery objectives.

All strategies should align with the organisation's goals. Once a business continuity strategy has been developed and approved, it can be translated into a disaster recovery plan, with an incident response team and list of important contacts.

The plan should be reviewed by management, tested, audited and regularly updated. It should be substantiated through testing, which identifies deficiencies and provides opportunities to fix problems before a crash occurs.

Additionally, it is important for businesses to monitor and protect their servers with the latest software that can flag up any potential problems.

And before calling in the tech experts, there are a few basic housekeeping tips that can lower the possibility of servers crashing in the first place. Prevention measures include keeping the server room isolated and cool with air conditioning. It should also be clean because dust can cause overheating and a blackout.

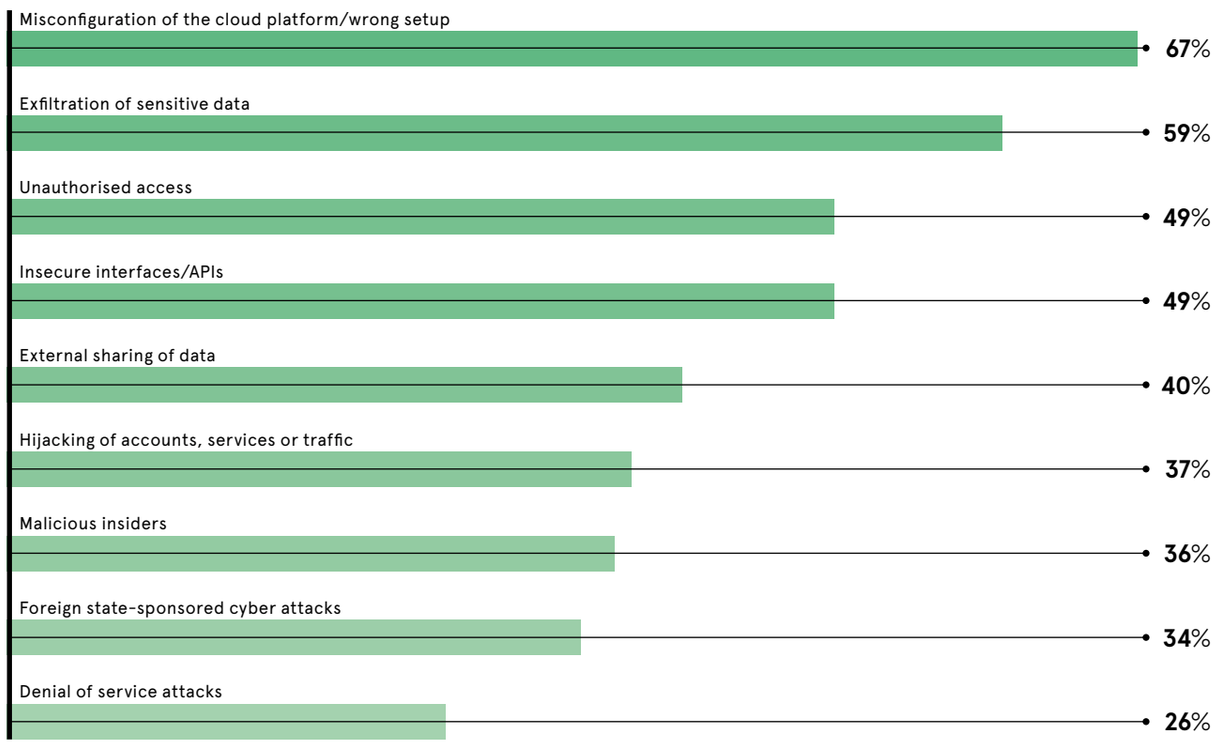
In-house tech staff may be able to troubleshoot a server failure, but more complex issues could require outside help. This means that adequate training of tech staffers in how to deal with a failed server in the first instance is a good investment, as is maintaining a working relationship with an external IT specialist.

Of course, if the server is in a remote data centre, the organisation is at the mercy of the good practice of an outside agency and reliant on their speedy action to get systems back up and running – so choose your provider carefully.

THE RISKS OF CLOUD MIGRATION

Biggest perceived security threats in public cloud adoption

ISC2, 2021



Daisy Mossop, GTM manager, Softcat

The recipe for cloud success? Sustainability and talent

Matt Larder, head of cloud, explains the philosophy behind the growth of Softcat, a challenger in cloud transformation

Cloud skills are in short supply. Three-quarters of organisations cite a lack of skills as a challenge on their journeys.

Other barriers include the IT delivery gap, a taxing landscape of cloud partners and a growing imperative that investments align to a sustainable future.

Given these pressures, why is Softcat quietly confident for the future? It's because the company’s ethos and vision for cloud are firmly grounded in its culture and the way it works.

People first

Cloud journeys depend on people; those with a passion for outcomes built on rapidly evolving technology. Yet as cloud technology has rapidly grown, so have the gaps in talent and recruitment.

As of early 2022, Softcat employs 1,700 people across nine locations to serve its customers with their digital workspace, cybersecurity and hybrid cloud needs in the UK and Ireland. The company’s growth is attributed to our culture, which started 29 years ago and is built on our ethos that people come first.

This powers our focus to annually bring through the next generation of talent and ensure that irrespective of age, gender, or experience, we provide equal opportunity for development. We work with schools and universities to raise awareness of what the technology industry has to offer. As a result, we are seeing many more young people drawn to the industry.

Daisy Mossop, GTM (go to market) manager at Softcat (pictured) is a product of Softcat’s commitment to young talent. A graduate of the company’s award-winning apprenticeship scheme, Mossop is also just one example of Softcat’s commitment to diversity in the tech sector. Incidentally, the company’s emphasis on sustainability was an important factor for Mossop in choosing to work at Softcat.

Indeed, we have observed that young people want their employer to provide an environment that not only educates and nurtures, but also demonstrates values they can relate to; values such as community, social responsibility and sustainability.

Thanks to the rise of digital channels and 24 months of lockdowns, many younger employees are self-taught, having learned a variety of new skills from their sofa. It’s here our approach bears fruit: Softcat achieved fifth position in the 2021 Super-Large Category of the UK’s Best Workplaces Awards; won the top apprenticeship employer in the UK award in 2021 and 2022 by RateMyApprenticeship; and has also grown its tech starter programme, which continues to promote women in technology.

Evolving career motivations

Engaging young talent isn’t enough when they face significant hurdles starting their careers. The cost of living is rapidly increasing, and experience is still a primary factor for many recruiters.

So, providing opportunities to mitigate these pressures is important, as is understanding and making a progressive effort to address the evolving expectations of not just younger members of our team, but also our customers and the wider society.

It’s here that the sustainability imperative is impossible to ignore. Global e-waste is growing at a staggering rate. UN research found that the world discarded a record 53.6 million tons of e-waste in 2019, of which only 17% was recycled. By 2030, it’s predicted this will increase to more than 74 million tons a year.

So what is the link between finding new talent and sustainability? In recent surveys by Global Tolerance, 42% of employees want to work for an organisation that has a positive impact on the world. Research from fastcompany.com highlights that nearly 70% said that if a company had a strong sustainability plan it would affect their decision to stay long term.

It’s this context that underpins Softcat’s commitment to be a responsible employer and business partner. As our CFO, Graham Charlton, recently commented: “The IT industry needs to lead the way toward a net-zero future. As technology and its place in society proliferates, the requirement for it to be sustainable becomes paramount.”

> **Young people want their employer to provide an environment that not only educates and nurtures, but also demonstrates values they can relate to**

This is why, through a range of initiatives that have gained total employee buy-in, Softcat has reduced its emissions by 37% over the past five years, while growing revenue and expanding our workforce.

Cloud: a different approach

While the new breed of ‘born in the cloud’ partners have attracted the industry’s top talent and accomplished well-publicised transformations, this has left an undesirable legacy: a skills bubble slowing the growth for the whole market and an oversight in the components of cloud adoption that are considered less exciting, regardless of their importance.

Flexera research highlights that 55% of organisations are having challenges with cloud software licensing and 59% of organisations are still to focus on cloud migration.

This creates divisive views that cloud can positively or negatively impact sustainability. A cloud journey can reduce IT infrastructure, cutting energy output and lowering emissions. But conversely, 30% of cloud spend is wasted according to Flexera research. This ultimately means someone else’s equipment contributing to your Scope 3 emissions – perhaps less than it originally was, but not as low as it could be.

Softcat has taken a different approach. Armed with an appreciation of sustainability, both climate and commercial, we help customers get maximum results by emphasising the importance of managing commercial relationships and providing intelligence regarding cloud usage to avoid waste and sprawl, which supports sustainable change. We do this with small and mid-sized businesses as well as enterprises, across private and public sectors. This gives us a breadth of experience that provides a platform to support digital transformation.

A recent example is Softcat’s partnership with a leading public cloud provider to support UK Police as part of the One Government Cloud Strategy to transform legacy IT. Digital forensic units are experiencing an exponential increase in demand for data processing on live and archive storage. Our partnership has demonstrated an 80% reduction in analysis time for a single mobile phone image and a 90% reduction in storage costs versus on-premises. This increases department efficiency and reduces carbon footprint using modern cloud technology in place of ageing on-premises equipment.

The future: no dreamwork

The cloud scene is teeming with providers. Much rarer are partners prepared to build and invest in a lasting community that embraces young talent and reflects the values of its people and customers.

In the long-run, it’s a people-first ethos, with a sustainable attitude that delivers cloud outcomes that support lasting growth.

It’s here we measure our success. We have maintained annual customer satisfaction results at 95%, and despite the challenges of a global pandemic, we hold a Net Promoter Score of 59 - a great position in the technology industry.

For more information please visit softcat.com

Softcat

CYBERSECURITY

The biggest cloud security risks business must address

The rise of cloud computing represents a potential bonanza for cybercriminals, who are constantly probing for weak links in defence. Could your firm be doing more to protect itself?

Chris Stokel-Walker

Cloud computing has become a key part of how businesses operate in the West. Research conducted for the European Commission in 2021 found that 41% of EU companies with more than 10 employees were using some form of cloud service, for instance.

But with wider use of the cloud comes a greater likelihood that more things will go wrong. Cybersecurity should therefore be a prime concern for adopters. Here are five key issues that all cloud users would be well advised not to ignore.

1 Ensure that configurations are... configured

"Misconfigurations remain a top risk for cloud applications and data," says Paul Bischoff, privacy advocate and editor at Comparitech, a website that rates technologies on their cybersecurity.

A misconfiguration happens when an IT team inadvertently leaves the door open for hackers by, say, failing to change a default security setting. This is often down to human error and/or a misunderstanding of how a firm's systems operate and interact.

If misconfigurations happen on a non-cloud-connected network, they're self-contained and, potentially, accessible only to those in the physical workplace. But, once your data is in the cloud, "it is subject to someone else's security. You do not have any direct control or ability to test it," notes Steven Furnell, professor of cybersecurity at the University of Nottingham. "This means trusting another party's measures, so look for the appropriate assurances from them rather than making assumptions."

Bischoff adds that oversights in this respect can "leave data vulnerable to unauthorised parties from the public internet. Attackers frequently scan and find cloud services with common misconfigurations.

Comparitech's 'honey-pot' experiments show that attackers can steal data from unprotected servers in a matter of hours. Our security team often finds and discloses exposures that occurred because of misconfigurations," he says.

2 Mitigate the risks of phishing

According to the government's most recent annual Cyber Security Breaches Survey, more than a third (39%) of businesses in the UK experienced a cyber attack and/or breach in the year to March 2021. Of those firms, in excess of a quarter said that they were being targeted at least once a week, showing the scale of the problem.

The most common attack method they reported was phishing, which accounts for four in every five attempted incursions. Phishing occurs when a criminal impersonating a well-known brand contacts people online and tries to fool them into visiting fake websites designed to extract key information from them.

Furnell notes that cloud services have become among the most common phishing lures, because of their ubiquity and importance in business. They are places where users would expect to have to share information, including passwords.

Education is crucial in tackling phishing, says Furnell, who adds: "A combination of technical measures and interventions to improve user awareness are necessary to provide an effective safeguard."

There is plenty of room for improvement in the latter area: the government survey found that only 20% of UK firms had used mock phishing exercises to test their employees' knowledge.

3 Limit the amount of data shared to the cloud

It can be tempting for firms to outsource all their data to a cloud service provider. Doing so removes the need to manage data in different locations and eliminates a lot of maintenance hassle. But such convenience comes at a cost. Supply chain attacks – in which cloud providers are probed for weaknesses – are becoming more common.

Big players in the market are investing heavily in their defences. Google Cloud, for instance, recently added a feature called Virtual Machine Threat Detection. This continually scans tenants' virtual machines for signs of crypto-mining operations, which can covertly hijack the processing power of their computers.

But even the most diligent providers cannot say with certainty that they are 100% invulnerable. For that reason, it's vital that their clients audit what information they're willing to share in the cloud. Thinking that the security of any material held in the cloud could be compromised is a useful – if pessimistic – way to approach this issue.

"Careful attention should be given to the extent and level of access to cloud data and resources that is granted to third parties," Furnell advises.

4 Keep a lid on the internet of things

Whether you have production lines that are connected to a cloud server for their instructions, a packing operation that monitors stock using cloud-based data or simply a smart fridge in your office kitchen, the threat to business continuity grows as more data is connected to the cloud.

The internet of things (IoT) has enabled the smoother running of many processes, but it's worth bearing in mind the risks if you've come to rely on the constant availability of a given cloud service, say, or if you're storing proprietary manufacturing information on hackable servers.

66%

of UK companies experienced a successful phishing attack in 2020

Proofpoint, 2021

81%

of tech professionals worldwide identify 'security' as a primary challenge to enterprise cloud computing

Flexera Software, 2021

Don't be surprised if such data disappears or ends up in the wrong hands, warns Christopher Boyd, lead malware intelligence analyst at Malwarebytes Labs.

"Basic errors in cloud security will happen throughout 2022," he says. "With so much IoT data stored in the cloud, there is no limit to what an attacker could do if it managed to compromise services."

5 Lock up your application programming interfaces

It's not only the cloud server and the data on it that businesses need to be concerned about. It's also the way in which their business interacts with the cloud.

That connection is often brokered through application programming interfaces (APIs).

"These are often an initial attack vector, if not one of the most critical vectors, in complex attack chains," says Michael Isbitski, technical evangelist at Salt Security. "Depending on your overall enterprise architecture, the potential security risks are numerous. They include data exposure, privilege escalation, system compromise, lateral movement within networks and the planting of malware or ransomware."

APIs are a weak link that's often overlooked. Several of the vulnerabilities identified in Microsoft Exchange Server in the first half of 2021 have been attributed to APIs, according to Isbitski.

"Attackers regularly plant malicious software by accessing unprotected services via APIs or compromising dependencies and Git repositories that make up software supply chains," he says.

To stop the attackers in their tracks, IT professionals must monitor all API calls to and from cloud servers and contextualise them within normal business web traffic.