MAY 2024
networkingplus.co.uk

NETWORK+

IN DEPTH: Managed services, p9-10

Recovery and continuity

The modern environment is more risk-laden than ever

Paul Scott-Murphy, Cirata, p5

Zero Trust security

It's more complicated than it first looks

Chris McKie, Kaseya, p6

Questions and answers

I really wanted to be a superstar in sports

Mattias Fridström, Arelion, p16

Securing the General Election

On 6 May, it was reported that the details of 270,000 service personnel working for the UK Ministry of Defence (MOD) had been accessed in part of an operation targeting a contractor responsible for managing the MOD's payroll system.

"The armed forces personal data that was accessed is extra valuable because they will be highly security cleared individuals which means the data can be used for blackmail/extortion purposes," warns Patrick Wragg, head of incident response, Integrity360. "The system that was breached being managed by an external contractor highlights the need for extra levels of security when dealing with third-parties."

Indeed, the breach highlights the critical issue of supply chain security. The presence of third-party contractors and vendors in the supply chain of large and complex organisations like the MOD is almost inevitable, however, making it challenging to always ensure security. Having multiple parties in the supply chain increases the potential points of vulnerability, requiring comprehensive security measures and practices to mitigate risks effectively.

"Earlier this year, a government report highlighted the risk of legacy IT systems to government departments, with 11 out of 42 'critical' systems operating within the MOD," says Mark Jow, EMEA technical evangelist, Gigamon. "Now more than ever, the institutions behind national stability and security must be as robustly defended as possible, without room for security blind spots. This includes securing supply chains to prevent these attacks."

When it comes to data protection, organisations must identify the most sensitive data assets that require the highest level of protection and implement appropriate security measures to safeguard their most valuable assets effectively. This is especially important in the run up to the UK's 4 July General Election, in a context marked by global election manipulations/fraud and cyber-threats.

"The [MOD] breach reiterates a key security lesson for the public sector: cyber-attacks can have far more malicious intentions than just the threat actor's financial gain," explains Mark Jow, EMEA technical evangelist, Gigamon. "Failure to secure and defend critical data is no longer acceptable. Perhaps this latest breach will show that now is the time to implement comprehensive, robust, and punitive legislation, ensuring all commercial and public organisations finally take cyber protection seriously."

Cybersecurity must become a core priority as hostile state actors continue to ramp up their attacks on key ministerial departments that are central to modern society, agrees Kev Eley, VP sales UKI & Europe, LogRhythm: "staying ahead of threat actors requires governments to adopt a proactive cybersecurity approach that encompasses employee training and regular cybersecurity assessments, including third-party services. Deploying an advanced security solution to monitor and identify anomalous network activity also provides another crucial layer of defense against ever-evolving attacks."

"The current geopolitical situation is likely to lead to an escalation of this kind of activity, and we should expect to see similar events in the months ahead," adds Paolo Passeri, cyber intelligence principal, Netskope. "For the UK public sector, which is already struggling with legacy IT debt, this is an important reminder that a comprehensive zero trust approach is vital, and that it must necessarily include the supply chain into the process if it is to be effective." ■

Thales and Nokia to support critical comms on the Tube

Thales, in collaboration with Nokia, has been awarded a contract by Transport for London (TfL) to deliver a comprehensive communications renewal to support the safe operations of the Tube network.

This renewal will ensure that TfL's multi-services network (MSN) operates at peak performance, minimising functional risks, journey disruptions and costs for TfL.

The MSN serves as the underlying infrastructure that supports Connect, Thales' system responsible for the critical communications ecosystem that underpins the London Underground. This includes radio, transmission and operational CCTV technology used by TfL staff to maintain smooth operations, making the MSN vital to efficiency on the rail network and ensuring a safer and smoother passenger experience.

Nokia's mission-critical IP/MPLS network solution is the backbone and complements this system by providing secure, reliable, and scalable connectivity, ensuring that the foundation for this communications ecosystem is robust and sustainable.

"We are delighted to be working with Thales and Nokia on this renewal of our multi-services network, which supports a number of key systems such as the Connect radio system and access to CCTV across the network," said Rebecca Bissell, director of Information Technology, TfL. Delivering this comprehensive communications renewal will support the operational demands of our extensive Tube and rail network and ensure it operates at peak performance while reducing costs, journey disruptions, and ultimately providing the best service possible to our customers."

"Transport for London plays a vital role in the city, carrying up to four million passenger journeys a day on the London Underground network," said Matthieu Bourguignon, senior vice-president and head of Europe for network infrastructure business, Nokia. "Renewing and preparing the communications network for the future is essential to maintain and improve this critical London infrastructure. Together with Thales, we will use our expertise and technology to provide a reliable, secure and efficient solution that will enhance TfL's operations and services for years to come."

"We're delighted to partner with TfL and Nokia on this critical project. Renewing the multi-services network, in a way that minimises disruptions to services, is essential for maintaining a safe, reliable and efficient underground, without putting the burden on passengers. This partnership demonstrates our commitment to continuous innovation in rail and prioritising passenger mobility and operational excellence," added Andy Bell, vice president, Thales Transport in the UK. ■

Sunderland's service users to benefit from transformed networking delivery

Social and health care support delivery is set to be transformed across Sunderland, thanks to the rollout of a new innovative software aimed at enhancing reablement, planned care, and telecare services across Sunderland.

The project is a collaboration between Sunderland Care and Support (SCAS), Boldyn Networks, and Totalmobile.

With over 5,000 service users to benefit, the software from Totalmobile significantly increases SCAS operational capacity, enabling caregivers to provide a better service to a greater number of individuals per shift, per day - facilitating improved access to vital services for residents.

The project will not only increase service efficiency, but it will also enhance the work-life balance of over 500 caregivers. By reducing administrative tasks, streamlining processes, and optimising workflows, SCAS staff can focus on delivering high-quality care to residents, enhancing the care experience, and providing timely information and support to staff while retaining vital skills in the support sector. Supported by Sunderland's extensive public WiFi networks, the project is another milestone in the wider commitment to enhance the quality of life for communities across the North East.

"We are proud to collaborate with Sunderland City Council and Boldyn Networks to drive positive change in the care and support provision. This project exemplifies our commitment to using technology to enhance the lives of both caregivers and service users, ultimately fostering healthier and more resilient communities," said Chris Hornung, Totalmobile's managing director of public sector.

"Sunderland City Council is committed to improving the lives of our residents through innovative solutions. This project is a game-changer, enhancing the efficiency and quality of our social and health care services," said Graham King, director of adult social care at Sunderland City Council and chief operating officer for Sunderland Care and Support. "By leveraging the power of Sunderland's smart city infrastructure alongside cutting-edge technology from Totalmobile, we are not only increasing the capacity of our caregivers but also ensuring they can focus on what truly matters – delivering exceptional care. This initiative underpins our dedication to creating a smarter, more connected city that prioritises the wellbeing of its community."

"This new project shows the significance of technology in enhancing the health and wellbeing of residents. Thanks to the new partnership, both caregivers and service users across Sunderland will have access to more efficient care delivery that will contribute to higher-quality services," said Claire Venners, director delivery UK & Ireland at Boldyn Networks. ■

UK's chief executive officers report tech imposter syndrome

The majority of UK chief executives are experiencing tech imposter syndrome in the boardroom, with 64% admitting they secretly feel out of their depth when it comes to digital skills. The findings were revealed in a new report from AND Digital: 'The CEO Digital Divide: are you accelerating enterprise value or slowing it down?'

As well as confessing to feeling like an 'analogue CEO in a digital age,' 34% of business chiefs feel they do not have the digital knowledge to take their company to its next stage of growth. In response to this looming digital skills gap, the report revealed that 78% of all CEOs are looking to improve their skills and have signed up for digital training this year.

Despite currently lacking critical digital skills, most CEOs still feel they need to be ahead of the curve when it comes to data and technology to ensure growth. As a result, 59% of respondents indicated that they're pouring a large portion of their budget into cyber security this year. The investment in cyber security is driven by an increasing anxiety around security breaches, with four in 10 CEOs reporting that they live 'in constant fear' of a cyber breach (42%). Across the board, CEOs are recognising the pressing need to digitally upskill and making conscious efforts to prioritise this to drive lasting change.

"It's clear that the continual pace of technological change is leaving CEOs feeling somewhat out of their depth, triggering tech imposter syndrome in the boardroom," said Stephen Paterson chief for technology and people at AND Digital. "For business leaders suffering from digital anxiety, the way forward means evaluating the role that technology will play in accelerating your business strategy. When you start to consider technology as an enabler to your commercial objectives, it becomes far simpler to identify the digital skills you'll need to support your growth. It's important to remember that improving digital skills isn't a one-off activity, it requires sustained focus and investment to ensure long-term success." ■

EDITORIAL:
Editor: Amy Saunders
amys@kadiumpublishing.com
Designer: Ian Curtis
Sub-editor: Gerry Moynihan
Contributors: Lee Myall, Chris McKie, Paul Scott-Murphy, Duncan Swan, Kristan Torode, Mattias Fridström, Harry Bowlby, Lee Todd

ADVERTISING & PRODUCTION:
Sales: Kathy Moynihan
kathym@kadiumpublishing.com
Production: Karen Bailey
karenb@kadiumpublishing.com
Publishing director:
Kathy Moynihan
kathym@kadiumpublishing.com

Networking+ is published monthly by:
Kadium Ltd, Image Court, IC113, 328/334 Molesey Road, Hersham, Surrey, KT12 3LT
Tel: +44 (0) 1932 886 537

ISSN: 2052–7373

UK firms to cut costs in 2024 to combat rising business challenges

Almost two-thirds of UK organisations say they will focus on reducing their costs this year, according to new research from Daisy Corporate Services.

This represents an increase from 42% in 2023, as 46% of organisations confirm that rising costs currently present the biggest challenge to their business.

The study found that financial constraints (37%), legacy technology (31%) and cybersecurity concerns (27%) were the biggest barriers preventing them doing their job effectively. Nearly a third (32%) of respondents said enhancing their cyber security provision, including cyber security resilience plans, was a priority this year. A further 32% stated that building or improving their digital business model was a key focus. Many organisations recognised the need to streamline their current technology supply chain over the next 12 months, with three-quarters (76%) describing this as important or essential.

"IT and business leaders are acutely aware of the challenges posed by rising costs. While doubling down on cost savings, organisations are also attempting to build long-term resilience to future proof their operations. It's no surprise that many enterprises are looking at adopting new digital models and strengthening their cyber security posture, but these upgrades must be done in a cohesive and cost-effective manner," said Lyndsey Charlton, COO at Daisy Corporate Services.

Two-fifths (40%) of respondents confirm that technology should help their business improve operational performance over the next year. Almost two-thirds (63%) of organisations said cloud services would be their investment priority over the next 12 months, followed by cyber security (47%), and mobile and wireless solutions (40%). With a growing number of artificial intelligence (AI) use cases and benefits emerging, over a third (37%) of organisations see AI technology as an investment priority.

Beyond budget constraints, concerns over data security were cited as the biggest barrier towards making technology investments in the next year according to nearly half (45%) of the respondents. A changing workforce (36%) and unclear benefits (33%) were the other main reasons which would prevent organisations from making significant technology investments.

The research reveals that organisations are committed to their environmental, social and governance (ESG) responsibilities. More than three-quarters (78%) state the ESG commitments from suppliers is a high or very high priority. In addition, 46% of enterprises confirm they try to extend the lifespan of devices by repairing or refurbishing as needed.

"Technology will continue to play an important role in helping organisations to become more efficient and meet their ESG goals. However, without a solid strategy underpinned by the right skills, organisations may fail to fully realise all the benefits. At a time where budgets are coming under increased scrutiny, it is vital that organisations work with trusted partners that can help them optimise and future proof their IT investments," said Charlton. ■

SFRS adopt LTE cameras

Shropshire Fire and Rescue Service (SFRS) has implemented a new state-of-the-art Portable LTE Rapid Deploy Camera provided by Excelerate.

This technology is set to significantly enhance emergency response capabilities, providing SFRS with a versatile and powerful tool for a wide range of scenarios.

The Rapid Deploy Camera is designed for quick deployment, providing exceptional flexibility in dynamic emergency scenarios. With its easy setup and LTE connectivity, it can be swiftly placed for optimal effectiveness. Equipped with high-quality video capabilities, it offers a clear 360-degree view for enhanced visibility.

Responders, whether on-site or off-site, can remotely access video feeds from any authorised device and/or via their Incident Command Unit - ensuring safe assessment from a distance. This accessibility is made possible through Excelerate's Exstream Video Application, which guarantees the highest level of protection for customer data through full encryption. This robust security measure provides peace of mind during sensitive operations, safeguarding the integrity and confidentiality of information whilst enhancing overall situational awareness.

"The addition of Excelerate's Rapid Deploy Camera marks a significant advancement for Shropshire Fire and Rescue Service," said Richard Groom, station manager at Shropshire Fire and Rescue Service. "With its intuitive setup and remote access features, this tool amplifies our ability to adapt to evolving emergency scenarios."

"We are proud to support long-standing customers SFRS and are confident that the portability, LTE connectivity, and advanced features of our Rapid Deploy Camera will contribute to more effective and efficient emergency response operations," said chief operating officer, Bethan Evans, at Excelerate. ■

Protect vital IT infrastructure and NVIDIA AI investments from the growing risks of cyber-attacks

ZPE Systems launches new Nodegrid Serial Console Core Edition and the Nodegrid Gate SR platform with embedded NVIDIA Jetson Orin Nano™ module.

ZPE Systems new Nodegrid Serial Console Core Edition is a cost-effective third generation console server that resolves the vulnerabilities left by legacy console servers. It leverages drop-in Isolated Management Infrastructure (IMI) to fully separate management traffic from production networks. The creation of a separate management network provides physical and logical isolation from unauthorized users and cyber threats.

"The first step in cybersecurity resiliency is proper IT hygiene, starting with the right architecture to remove anxiety from automated patching and recovery," said Koroush Saraf, VP of Products and Marketing, ZPE Systems. "The Core Edition simplifies IMI, providing secure, isolated management access from any branch office or remote location via any LAN or WAN link type, including cellular connections. This gives customers a safe environment for patching or configuration rollback even during an outage or cyberattack."

Though IMI has been used primarily by hyperscalers and big tech brands, the Core Edition enables businesses of all sizes to build their own IMI networks and reap the benefits of a layered security approach at an affordable price.

ZPE is also releasing the **Nodegrid Gate SR with embedded Jetson module.** This new platform internally hosts the NVIDIA Jetson Orin Nano™ module, serving as an out-of-band device for initial bring-up, patching, and upgrading when running NVIDIA workloads. ZPE's Gate SR with embedded Jetson module offers a dual-CPU platform that uses the same IMI concept for provisioning AI workloads via out-of-band path and allows customers to deploy, manage, and upgrade remotely via ZPE Cloud. This new Nodegrid platform enables organizations to improve industrial floor safety, campus security, and manufacturing quality control, by deploying 3rd party computer vision software at the edge. Organizations can now add resilience and recovery to the fleet of their NVIDIA AI workloads with ZPE embedded or external AI hardware devices.

For further information visit: www.zpesystems.com

itim Group renews Majestic Wine SaaS contract

itim Group plc has signed a five year multi-million-pound contract renewal with Majestic Wine, the UK's largest specialist retailer with over 200 stores.

The subscription renewal for itim's UNIFY platform supports retail, B2B and direct to consumer sales covering processes such as EPOS, e-commerce, PIM, stock management, merchandising, supplier management, pricing and promotions, customer order management, customer management, B2B customer accounts and website & business intelligence. UNIFY provides a single view of customer, product and real time stock across all channels.

"In 2021, Majestic selected itim's UNIFY platform as its technology partner. Together we have turned Majestic into what we believe to be one of UK's leading Omni channel retailers. I am pleased to extend this partnership to cover Majestic's next five year digital journey," said John Colley, CEO Majestic Wine.

"We are delighted to be continuing our relationship with such a prestigious retail brand. This five year renewal is an endorsement of Majestic's confidence in our UNIFY platform which seeks to help retailers achieve omni-channel excellence by driving sales and profitability by putting 'the customer' at the heart of Majestic's unified retail business model," said Ali Athar, CEO itim Group plc. ■

Rubix VT supports Together Co scores new systems

Rubix VT has stepped up to help beat social isolation by extending a helping hand to Brighton and Hove loneliness charity Together Co with telecoms and volunteers. The company has allocated free telecoms services to 20 users at Together Co, a contribution valued at £10,500.

Together Co received a new telecoms system tailored to its specific needs and integrated with existing systems, which have helped to speed up internal processes and made the charity operate more efficiently. Rubix VT also provided the charity with training and ongoing support to ensure staff could use the new system easily, minimising disruption during the transition period.

Team members from Rubix VT have also volunteered to become Telephone Befriending Volunteers for people supported by Together Co. After undergoing comprehensive training, five employees are now poised to provide regular companionship and support through weekly phone calls to those in need.

"Rubix VT's telecoms services align perfectly with Together Co's mission to 'create connections' and combat loneliness, so we're especially proud to play a part," said Nick Poyner, managing director of Rubix VT. "It means a lot to our team to have an opportunity to volunteer and collaborate with Together Co and help people who are struggling. Helping people and giving back is a core part of Rubix VT and it's wonderful to know that thanks to our team, we will be brightening up someone's day."

"The smooth changeover allowed us to continue connecting with people using Together Co's services, which was particularly important as many of the people we support do not have access to the internet or email," said Emily Daniel, head of insight and involvement at Together Co. "Rubix VT are genuinely passionate about our mission as a charity, and their dedication is reflected in their proactive efforts to ensure our telecommunications solutions are perfectly aligned with our needs." ■

Parliament sounds alarm over major skills shortage

Members of Parliament have warned that a UK skills shortage is jeopardising the delivery of crucial infrastructure projects, as the government braces to allocate a staggering £800 billion towards major initiatives.

According to the Public Accounts Committee (PAC), the UK finds itself ill-equipped to execute ambitious infrastructure plans over the next half-decade due to a significant deficit in essential skills. The report underscores the urgent need for 16,000 professionals to undergo accreditation via the government's major project leadership academy, yet only 1,000 have completed this process thus far.

"The pressing issue of the UK's skills shortage highlighted by the Parliamentary Committee extends far beyond infrastructure concerns. It's a challenge impacting all industries from finance to tech and beyond," said Michael Thornton, director of public sector at Investigo, part of The IN Group. "Organisations must evaluate and have a clear understanding on the resources they need to deliver critical projects, prioritising the recruitment and training of digitally skilled staff to lead innovation initiatives. Different projects require different skill sets and different levels of experience, so organisations, whether in the public or private sector, should work with partners to bring in the staff they need. These staff can be critical to overseeing technology such as AI, which can significantly boost efficiency by automating repetitive tasks and ensure project deadlines are met. In fact, our Tech and the Boardroom survey revealed that 62% are prioritising hiring AI experts to capitalise on the advancements of AI technology. As the PAC's report highlights, unlocking the power of people is a crucial part of driving operational efficiency." ■

Blackpool eyes up data centre market

Civic leaders in Blackpool have invited data centre operators to view their plans to convert former aircraft hangers at Blackpool Airport into a high-performance data centre campus.

Feasibility studies are also taking place to connect the Silicon Sands project to a district heat network, with waste heat from the data centres being re-used to heat surrounding businesses.

"Silicon Sands has the potential to be a complete game-changer in our plans to make Blackpool better. With the power supply, land availability and ultra-fast internet access, we can sit at the heart of a new digital revolution not just for the town, but for the entire region," said Cllr Mark Smith, cabinet member for Levelling Up (Place) at Blackpool Council. "For Blackpool, this could mean significant inward investment and thousands of well-paid new jobs across the Fylde Coast, which in turn will retain the talent of our young people in Blackpool rather than losing them to other parts of the country, as well allowing high performance businesses of the future to grow fast on the Fylde Coast. For the data centre industry, Silicon Sands offers the chance to reduce its impact on the environment and on the National Grid and show a modern climate friendly future that can bring major regeneration benefits."

A first data centre is set to start construction next year on a cleared area of land and Blackpool Council is hosting an expression of interest for data centre developers and operators to build and run the site, which would also include a research and office facility on upper floors. To develop the Silicon Sands site, work is progressing to relocate and rebuild old hangars and administration buildings at Blackpool Airport closer to the main runway. ■

Word on the web...

Networks: a crucial piece of the AI puzzle

Lee Myall, CEO, Neos Networks

To read this and other opinions from industry luminaries, visit www.networkingplus.co.uk

Managing recovery and business continuity in an unstructured data environment

Paul Scott-Murphy, CTO, Cirata

Disaster recovery and business continuity must function now in a far more risk-laden and complex environment. While ransomware threats continue to plague organisations, those executives responsible for ensuring their company meets compliance and business continuity goals face several added challenges.

CIOs and their teams are refining their business continuity strategies to address the magnitude of unstructured data. They are seeking practices that are capable of efficiently managing data analytics fed by large language models (LLM) while providing the replication safety net that supports business continuity.

The GenAI juggernaut

Huawei estimates global data volume will reach 180 zettabytes by 2025, 80% of which will be unstructured data; and by 2030, some 25% of unstructured data will be used for production and decision making, eventually reaching 80%. GenAI is driving this volume by aggregating text, voice, documents, videos, emails and messaging platforms.

While GenAI is beginning to exhibit value in various use cases, its rapid development, broad use of large data sets, potential for misapplication and lack of robust security controls make it a rich target for cyber criminals. As Gartner says, 'enterprises must prepare for malicious actors' use of generative AI systems for cyber and fraud attacks, such as those that use deep fakes for social engineering of personnel and ensure mitigating controls are put in place.'

Protecting large data sets

Executives are not yet confident that GenAI can help protect against data breaches or business continuity, even while it contributes to the explosive growth of unstructured data and more possibilities for cyber attacks. As businesses continue to assemble large data sets using GenAI-powered processes, and transform this data into applications, there is an immediate need to ensure these data sets are protected and adhere to business continuity standards.

Contributing to the security challenges is the fact that different functional teams are using and generating unstructured data in their own fashion and with varying degrees of security in place. IDC warns that application sprawl and fragmentation of unstructured data, 'often with diverse sets of identity and authentication models and different administrative features,' contribute to more potential attack surfaces. Analysing the cost of a data breach, IDC estimates that greater fragmentation leads to doubling of annual costs of security breaches, $4.5 million versus $2.2 million.

To avoid fragmentation, businesses must set enterprise-wide standards on such practices as authentication and policy controls, and work with functional teams to accommodate specific needs like recovery point in time standards. Like any other use of data, unstructured data use must adhere to security compliance standards. IT security teams must also conduct regular audits to ensure standards and policies are being followed.

Integrating GenAI into business continuity

Large language models offer the potential of significant business value but still must be subject to the same security and data protection practices as any other application or data asset. *To ensure recovery and business continuity, there are several immediate considerations:*

Visibility is a priority. The principle that you can't manage assets you don't know about holds true for unstructured data. Functional teams, or lines of businesses, must have visibility into the unstructured data in their environment. It is a fundamental practice to avoid cyber attacks, data privacy breaches and budget impact. By having visibility, teams can make a judgment as to which GenAI data and/or models are critical and need to be categorised as such to support continuity.

The cloud is king. Large language models are built on data that needs to live in the cloud, requiring best practice in being able to securely store the data and execute recovery as needed. The expense and lack of hardware support for datasets needed to train large language models makes on premise storage highly prohibitive. If a business has adopted a multi-cloud strategy, it needs to consider a solution that can support large data set migration across multiple cloud providers.

Recovery is the point. GenAI has changed the amount of data flowing through an organisation and to the cloud. In refining a business continuity strategy, to integrate GenAI, functional teams need to review their recovery time objectives (RTO) and recovery point objectives (RPO). These set standards which will ensure they have backup and recovery processes in place to accommodate recovery of any critical GenAI large data sets or applications.

Replication is imperative. To support near-zero RTO and RPO objectives, replication technology can help enable compliance and fast data recovery by providing real-time cloud replication of actively used GenAI data. This method reduces costs and further ensures continuous data accuracy should recovery be necessary.

No downtime is a must. Any data movement can hamper business continuity if it requires application downtime. Data migration solutions that can facilitate large-scale data changes and migration to the cloud will help minimise disruption.

Automation is the answer. In the event of a system failure, IT teams can use active-active replication over multi-cloud environments, as necessary, to ensure automatic failover and recovery, minimising data loss and downtime.

Practice secure GenAI use

Now is the time to review business continuity practices.

Updating security practices will help avoid the costs attributed to a data breach – both direct monetary costs, and reputational costs. Stringent compliance requirements regarding data protection, privacy, and continuity of operations are an important cost and trust factor. It is too easy to introduce confidential data into training large language models, perhaps unwittingly.

Security and functional teams will need to work together to set limits on unstructured data that pose a privacy threat. IT teams must also avoid policy controls fragmentation, update recovery practices, and use replication technology to take the lead in ensuring business continuity. ■

"CIOs and their teams are refining their business continuity strategies to address the magnitude of unstructured data. They are seeking practices that are capable of efficiently managing data analytics fed by large language models (LLM) while providing the replication safety net that supports business continuity."

"Updating security practices will help avoid the costs attributed to a data breach – both direct monetary costs, and reputational costs. Stringent compliance requirements regarding data protection, privacy, and continuity of operations are an important cost and trust factor. It is too easy to introduce confidential data into training large language models, perhaps unwittingly."

Improving security with Zero Trust networking

Chris McKie, VP product marketing, security and networking solutions, Kaseya

With cyber risks steadily growing, organisations are increasingly looking to Zero Trust as a strategy to help defend their networks and boost their cyber resilience. The underlying principle of Zero Trust is well known by now: to never trust anything or anyone by default, including internal network devices, and to only grant verified users access to the data they really need.

It sounds simple enough. But for many organisations, putting Zero Trust into practice proves less straightforward than it sounds.

This is because implementing it involves several different capabilities, requiring resources and skills that smaller businesses often lack: an 'assume breach' mindset, strict access controls, continuous monitoring across the IT infrastructure and proactive threat hunting are all essential parts of a Zero Trust strategy.

Zero Trust Network Access (ZTNA), meanwhile, has emerged as an important subset to Zero Trust. Rather than requiring every single process to follow Zero Trust, it focuses on the network: imposing strict controls on network access to protect data and users, including those working remotely. This network focus makes it much more achievable.

There are five core elements to implementing ZTNA. They help ensure that only trusted entities working on secure devices are accessing the company network and in addition, that they only use the data and applications they have explicit permission to access.

This is achieved by always verifying users and their context, continually validating devices and their status, authorising the applications used, files and data, restricting access to cloud and SaaS resources and finally, enforcing an organisation's security policies and controls.

SASE solutions can help deliver Zero Trust

Secure Access Service Edge (SASE) solutions play an important role in delivering ZTNA as some of the required functionality is already built in. While their main use case up until now has been to replace VPNs in remote access scenarios, SASE's potential goes far beyond simplifying remote access. These solutions combine the necessary networking and security-as-a-service capabilities that can help organisations achieve Zero Trust networking.

Following the principle of 'least privilege,' SASE solutions work by only connecting identified users and devices to specific resources in the cloud or on-premises. In line with Zero Trust, access is granted based on the verified identity of the user, device, or entity, considering important real-time context such as the device's security posture.

SASE also delivers next-gen firewall protection with policy enforcement and content filtering across branch offices, remote users, and on-premises workers. This helps businesses implement fundamental ZTNA security controls. And, whereas VPNs tend to expose a lot of information on the internet that could be useful for would-be attackers, with a SASE solution, networks and resources remain hidden from sight.

What's more, the cloud-based management of a SASE solution makes the ZTNA security model very achievable even for smaller companies – allowing easy deployment and management. There are scalable, easy-to-use SASE solutions on the market that can cater to organisations' specific requirements and individual budget constraints, bringing Zero Trust networking within easy reach.

Greater control and reduced risk

Zero Trust Network Access is just as vital for small and medium-sized businesses (SMB) as it is for enterprises – especially considering that the fallout from an attack can be even greater. In the Datto 2022 SMB Cybersecurity Report, around 70% of SMBs admitted the impact of a ransomware attack would be 'extreme' or 'significant.' In fact, an attack can be so devastating that almost a fifth (17%) said it would be difficult for them to recover.

Zero Trust Network Access addresses this by providing a modern and robust approach to network security that helps businesses limit the damage of an attack. If they embrace it, they will benefit from greater control, improved visibility, and reduced risk.

The first step is to put in place a cyber security framework that aligns with the organisation's needs and goals. The principle of Zero Trust is then added as an overlay, with the necessary policies and controls to achieve ZTNA – encompassing not only remote workers through a SASE solution, but also internal users and devices sitting within the network boundaries.

Due to the perceived complexity of Zero Trust, businesses can find the prospect of deploying a solution by themselves daunting. While implementing ZTNA is not complicated, many businesses – SMBs in particular – will want to engage an MSP partner who can help them define a least-privilege access strategy with appropriate controls. The MSP can not only supply and manage the right verification and identification solutions including SASE, but also take responsibility for the 24/7 monitoring of the network via a remote monitoring and management system (RMM).

Organisations are increasingly prioritising security measures to combat the growing number of cyber threats. Zero Trust is here to stay – and starting with Zero Trust networking is a great first step to strengthen an organisation's security and cyber resilience. ■

Predictive maintenance: how IoT SIM connectivity can transform manufacturing

Harry Bowlby, managing director, Spitfire Network Services

We are living at the beginning of the era of 'connected' things. The applications of such technology are serving to improve life in general by advancing positive change across a wide spectrum of economic and social factors globally. Diving a bit deeper into the world of connected things we can find a whole range of IoT connectivity solutions with IoT SIM connectivity a huge growth area for the purpose of managing IoT assets.

For example, a smart controller can help retailers to manage their stock of refrigerated real estate more effectively. Such a device feeds back regular status reports (data) which can predict whether a refrigeration unit is likely to fail allowing it to pre-empt a service. And farmers (using a variety of sensors) can manage their crops much more efficiently, considering everything from soil moisture levels through to vehicle maintenance management.

IoT connectivity refers to how an IoT device (a simple sensor taking temperature readings or a self-driving vehicle, for example) connects to the cloud, to other devices or even IoT gateways. These IoT connectivity solutions can help customers across all industries, across all geographies and can easily scale up from smaller, unique scenarios to industrial behemoths - customers can be as varied as the devices that get connected. The technology is proving to be flexible, resilient, and secure giving unprecedented control over IoT assets. Today's mobile IoT solutions can combine optimised and competitive data bundle packages with business grade routing and core network capabilities.

Predictive maintenance

There are numerous examples of predictive maintenance that span many different industries. For example, predictive maintenance in the manufacturing industry could involve preventing valuable machinery from breaking down by using predictive maintenance software and data analytics for manufacturing. IoT predictive maintenance uses data gathered through IoT technology to assess equipment to predict potential breakdown or outages more accurately. Such technology offers invaluable help for organisations by gathering real-time asset data that can be used to design effective maintenance strategies.

Making things efficient

Heavy industry and manufacturing rely on a mobile workforce to keep plant and machinery maintained and in good working order. Rotational rolling maintenance programs can be inefficient and usually don't keep pace with localised nuances where usage dynamically changes. With so many factors involved that require a technician's attention to keep services running smoothly, finding a solution to identify issues as they arise on site can help with service planning, building efficiencies and ultimately optimising revenue potential.

And, specifically, an IoT SIM connectivity solution is ideally placed to help in these scenarios - after all, connecting hundreds or thousands of devices in the field through a fixed line and router combination can be impractical due to device and sensor location and infeasible from a cost perspective.

"Using IoT connectivity solutions in an industrial/manufacturing scenario can help to reduce costs by prioritising and reducing the impact of productivity congestion via process optimisation and analysis. This can also help to ensure that people and machines are working in perfect harmony."

A SIM connectivity solution can use data via the mobile network. Being able to remotely monitor and predict maintenance requirements in the field enables a more efficient service. By using IoT data SIMs, businesses can greatly reduce the data connectivity costs (by a factor of 10) paying only for what data is used, compared to that of a fixed internet connection.

Data is key

Data is at the heart of everything. Within any IoT ecosystem you have smart devices with a variety of sensors and hardware that serve to collect, send, and act on any data that they collect from their environments. Devices then share the data collected from sensors to be analysed (in the cloud or locally). And the beauty is that machines are doing all the legwork here - very little human interaction is needed as devices can communicate with other related devices and act on the information accordingly. Let us be clear though, people can still interact if they wish to access the data for any reason. With the staggering volume of data that can be expected to be generated in these growing ecosystems, Artificial Intelligence (AI) will have a key role to play in the analysis (and subsequent action-taking) over all this data. At the end of the day all this data is only as useful as the decision-making that it empowers.

The bottom line

Using IoT connectivity solutions in an industrial/manufacturing scenario can help to reduce costs by prioritising and reducing the impact of productivity congestion via process optimisation and analysis. This can also help to ensure that people and machines are working in perfect harmony.

Where you have a largely mobile workforce (teams of engineers or trouble-shooters), having useful and workable data can help prioritise and manage how and where they work which can result in considerable cost savings. The security element is also critical, with secure private networks facilitated by the right provider.

If you are a business that monitors equipment or are regularly repairing products for customers, IoT solutions can save money by reducing the number of unneeded call outs. Historically, a business would have to physically send an engineer onsite to assess things. If everything was fine with the kit, it was an unnecessary trip that still cost the business money. These days, data and alerts can be sent to you directly giving a clear picture regarding the condition of your equipment. Problem-solving from a desk is much less costly than pointless servicing appointments.

It doesn't matter how big your business is or which industry you serve. Chances are that there is a mobile connectivity solution for you that can provide significant improvements in efficiency, that can truly extract value from data and, ultimately, deliver positive results for your bottom line. ■

Cutting costs through circularity

Lee Todd, head of advisory services within electrification service, ABB

Digitalisation is now essential for day-to-day operations in most industries. Companies use it to maximise uptime and efficiency while cutting costs as much as possible, and for data centres in particular, digital technology helps to support the 'always-on' mindset.

The cost of outages in data centres has increased exponentially. Entire companies, currencies and markets now depend on uninterrupted service from information systems. Every second of downtime is revenue lost, and every disposal of otherwise perfectly good hardware brings carbon emissions with it. The costs to the data centre operator are threefold: environmental, financial, and reputational.

Faced with these, circularity is key. Circularity can inform data centre operations at every level. A combination of well-timed retrofitting and specifying systems for high energy efficiency, preventive and predictive maintenance, and even augmented reality, can ensure guaranteed uptime — for the long term, and at the lowest possible cost to you and to the environment.

Retrofitting

One of the greatest opportunities for carbon and cost savings is upgrading outdated components. This enables existing electrical equipment to last much longer, uses minimal energy in production and prevents downtime from breakdowns.

When a typical power distribution system reaches the end of its life, more than half of components remain in excellent or as-new condition. For example, the cabinets, steel plates and busbars still retain their value and contain embedded carbon dioxide emissions, even when the working parts of a circuit breaker like electrical switches, fuses and contactors need to be renewed. With this approach, facilities can reduce the cost of operating equipment by a third while extending their life cycles by as much as 30 years.

By retrofitting or upgrading systems, data centre operators can keep the value of existing hardware while achieving the performance of the latest technology. Actively revitalising and reusing assets, rather than relying on the manufacture of new ones, reduces reliance on fluctuating lead times and potentially volatile global markets. In addition, it reduces the extent of site work, helping to avoid the risk of downtime.

Data centres built in modular setups can help to streamline servicing. Modularity supports both specification and installation processes: constructing a data centre in segments (e.g., 20MW sections for a projected 200MW facility) enhances cost efficiency by constraining the effects of component failures to specific blocks, while allowing retrofits to be more targeted.

Smart maintenance

Data centre operators must also conduct regular monitoring of their facilities, particularly mission-critical equipment, to guarantee the reliable provision of services. The more intensive the operations, the more regular service activities are needed to avoid unplanned outages. In a data centre, running equipment to the point of failure may cost up to 10 times more than investing in a program of regular maintenance, not to mention the inherent reputational risk.

A preventative approach, replacing older, non-digital circuit breakers with more intelligent, sensor-enabled breakers linked to cloud-computing platforms, is necessary. Real-time data and analysis on asset condition and performance prevent potential issues before they arise. The carbon cost of replacing fully worn-out machinery is also higher than keeping existing infrastructure operational.

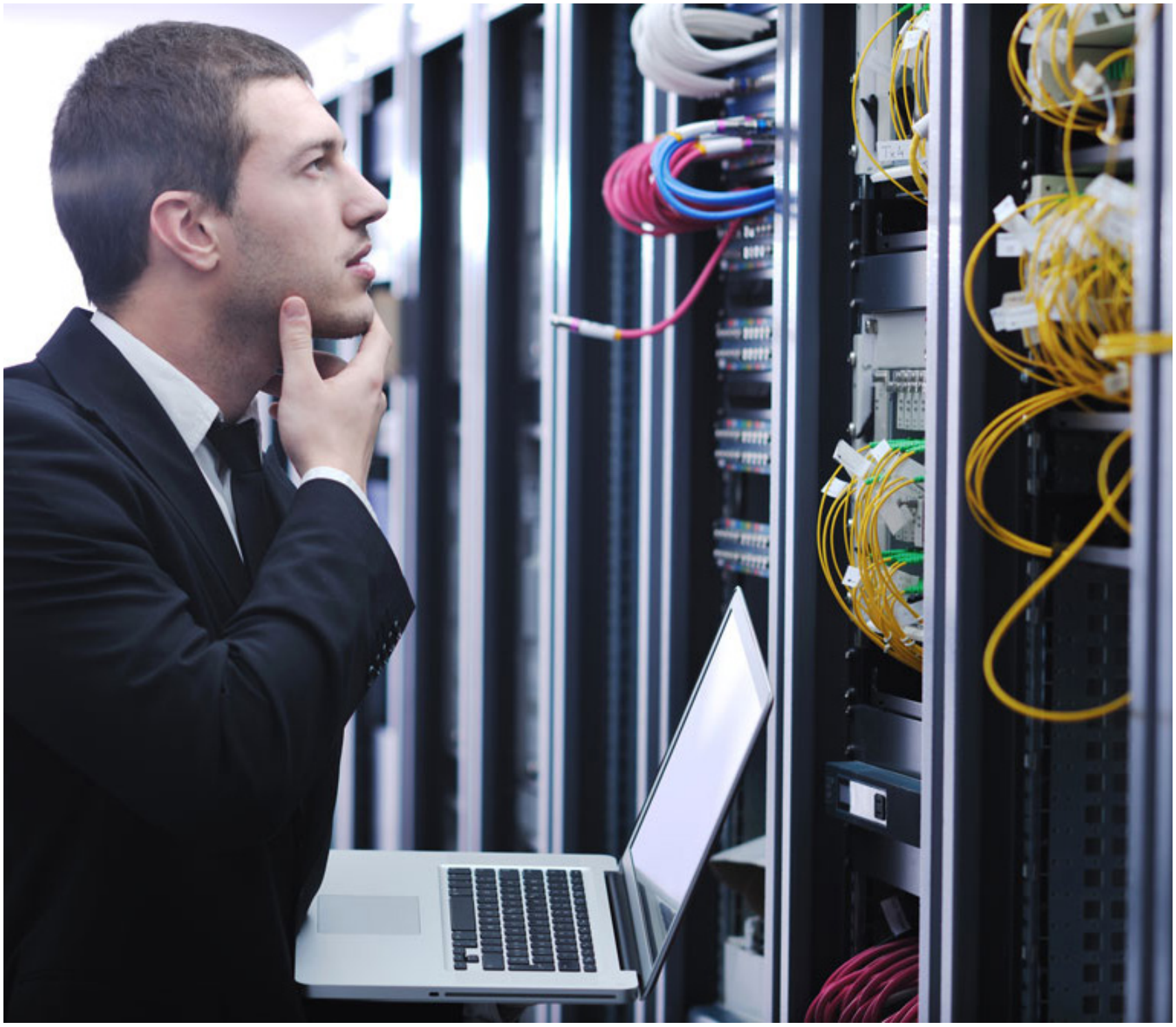
Research by the Deloitte Analytics Institute reveals that on average, predictive maintenance increases productivity by 25%, reduces breakdowns by 70% and lowers maintenance costs by 25%. Despite this, only 47% of global manufacturers use predictive maintenance technologies. Early adopters in the data centre industry, meanwhile, are leading by example.

Augmented reality

One tactic that can help to service equipment more efficiently is augmented reality (AR). AR helps technicians on the ground gain more insight into the physical equipment in front of them.

When a site technician uses an AR app to view a piece of equipment via their smart phone, the app will overlay technical information and servicing guidance in the form of images, instructional videos and documentation.

In turn, the technician can order the right spares and carry out maintenance operations within hours without needing to call a specialist to site. This saves up to 171g of CO2 emissions per passenger-kilometre and enables site-based technicians to carry out unusual tasks with confidence. ■



Getting the best from your network

Managed services are high on the agenda for IT teams – but how can organisations make the best choice for their specific circumstances?

A managed service can make or break an enterprise, and with significant variation in what constitutes the managed portion of the services between different managed service providers (MSPs), it can be a challenging prospect to identify what's best for business…

Separating the wheat from the chaff

Selecting a MSP is no mean feat – after all, the success of the enterprise is at stake.

"Enterprises need to select an MSP that can demonstrate that the services being deployed are doing what they say they will on the tin," says Martin Hodgson, director Northern Europe, Paessler. "In 2024, business leaders are more discerning than ever when investing into any area of the organisation – whether that be IT, marketing, or even talent. Customers want to know that any service they invest into is one that is going to demonstrate good ROI and be performant."

"Organisations should seek a provider who has experience, knowledge and understanding of the technology they need to look after and can deal with any problems," adds Martin Saunders, COO, Highlight. "They should also have economies of scale with greater purchasing power, use equipment more efficiently as well as having the breadth of staff to deliver 24/7 coverage."

To ensure the provider supports specific business objectives effectively, the organisation must consider several salient points, including the range and customisation options of services and capabilities; compatibility with existing infrastructure; specific industry experience and qualifications; security measures and industry compliance; scalability and flexibility; onboarding and support; SLAs and accountability; and, of course, cost and value.

Overall, a holistic approach is recommended.

"Rather than focus on the terms of a managed service, an enterprise should look for a provider that can act as a virtual member of their IT team with the overall aim of improving the customer experience," asserts Saunders. "Discussions should focus on what the provider will be doing, who they will work with, what information they will provide and what elements they can take off the enterprise IT team. If discussions focus on basic uptime SLAs, it will miss the point."

"Cost is a factor in any business investment, but simply comparing monthly invoice numbers will ignore some important points," says Jordan MacPherson, director, product operations, Entuity. "The right MSP will have expertise in the technologies that matter to your business and have enough resources to support you beyond the ideal steady state we all dream of. Another important consideration would be scale

of the engineering teams. Do they have the resources to support you at the most critical times?"

Considering these factors will help an enterprise choose an MSP that not only meets its immediate needs but also supports long-term business goals and growth. When it comes to separating the wheat from the chaff, Saunders says that the provider must supply the visibility to demonstrate how they will manage the proposed solution and then communicate the successful delivery.

"If a provider can include a Service Observability Platform as part of their managed service package, then the customer is more likely to have a strong working relationship with their service provider for the long term," says Saunders.

MacPherson reports that the decision should be based upon thorough procurement process, but the answer to this one question - "Do I trust them?" – must be a resounding 'yes.'

Meanwhile, Hodgson recommends asking prospective new providers: "what steps are you, as a service provider, going to take to deliver an exceptional service? How will you prove that you are meeting those deliverables?"

Happy enterprise, happy customers

Fostering a good working relationship between organisation and MSP relies upon clear communication, mutual trust, defined expectations and goals, regularly reviewed SLAs, accountability, and continual improvement.

"The relationship between an IT organisation and provider depends upon a virtuous circle of open collaboration between organisations," says MacPherson, director, product operations, Entuity. "Success of the engagement and be driven by a thorough understanding of the technical, commercial and business strategies of the organisations it partners with. The MSP should appreciate the unique nature of each of our customers' businesses and requirements, with services designed to provide flexibility, and understand and organisation's technical, commercial and business strategies through a dedicated and highly skilled team that delivers services on time, to scope and in budget."

"Customers want their providers to act in a competent, reliable, and honest way. If they cannot trust their provider in any of these three areas, they will simply change to another," surmises Saunders. "The customer's perception of how well their provider can meet these criteria is often dependant on the quality and transparency of the information they provide."

"To ensure a good relationship between an enterprise and a service provider, you need to set realistic expectations and then deliver against them. If customers are at the heart of everything we do, it makes sense to structure monitoring systems around them," adds Hodgson.

SLAs are one way to keep the service provider accountable, reports Hodgson: "if your organisation strives to deliver a very high uptime of the devices used in your offering, then the service level objective is set to 99.999%. This being said, it's important that there's still some flexibility in the relationship between the enterprise and service provider if the relationship is going to be mutually beneficial. 100% availability isn't always possible due to maintenance and outages. But there is a world of difference between an unplanned outage, and one that is mutually scheduled to benefit both parties. The key to happy customers is keeping them informed about planned outages in advance."

Moreover, having a shared understanding of how network and application services are performing will encourage productive communication between the service provider, the enterprise's network management staff and end-users at all levels.

"With users on both sides of the relationship able to understand how systems are performing, they will be able to easily identify potential problems, reducing the need for escalation and leading to a longer-term association," explains Saunders.

The effort is well worth the result, with good enterprise-provider relationships delivering numerous benefits for network performance and organisational efficiency.

"In a managed service scenario, the provider takes responsibility for a particular area of the network with, for example, a service manager turning up to monthly meetings to fight the corner of the network," says Saunders. "With a strong and effective relationship, the enterprise IT team will be free to deal more with their users and the application side of things whilst the service provider manages the infrastructure underneath. Ultimately, this will enable the organisation to focus on being more efficient, sustainable, competitive, and profitable."

Indeed, quantifiable benefits of the healthy relationship include enhanced network reliability and uptime as a result of proactive monitoring and fast response; improved network performance with optimal resource allocation and regular updates; enhanced security via proactive measures and rapid incident response; and optimised, predictable costs. Additional benefits include a better user experience with consistent performance, and data-driven decision making aided by insightful reporting.

"Rather than focus on the terms of a managed service, an enterprise should look for a provider that can act as a virtual member of their IT team with the overall aim of improving the customer experience."

Martin Saunders

Jordan MacPherson

"A good relationship between the organisation and its service provider should always be rooted in high levels of transparency. This enables IT teams to be highly reactive when it comes to issues that affect network performance."

"A good relationship between the organisation and its service provider should always be rooted in high levels of transparency. This enables IT teams to be highly reactive when it comes to issues that affect network performance," outlines Hodgson. "Much like a doctor on call, who is able to respond at speed when provided with clear locations and directions to a given incident, effective communication and collaboration speeds up the digital 'diagnosis' process."

From good to great

Once the enterprise has selected the right MSP, and cultivated a healthy relationship – how do they know whether they're getting the best service they possibly can?

"Like a business leader that delivers on key performance indicators (KPIs) to clients, SLAs enable MSPs to clearly communicate to their customers how service standards are being upheld," says Hodgson. "Therefore, a great managed service will be one that exceeds the expectations of the customers/users. Whilst it's good to thrill, it is always vital to ensure consistency. Once you've delivered exceptional performance, you've set the bar higher in terms of expectation, so need to have a strategy in place to deliver on the uptime levels promised."

While transparency is important, it is not good enough to blast information at customers, says Saunders. A provider needs to know if anyone is looking at the information and that it makes sense, which means communicating in an intelligible way and ensuring the information is valued.

"A great managed service is therefore one where both provider and customer have a shared view of how all services are performing, with the provider able to show that they are competent and delivering a reliable and trustworthy service that matches what they have promised," opines Saunders.

Hodgson agrees that the best managed services will be able to provide admins and users with clear visualisations of their IT environments: "sharing dashboards with users, which can be defined based on different objectives, sites, or vendors, is highly effective. These simple digital pictures, where green indicates 'performant' and red indicates 'requires resolution' speak a thousand words. Nobody needs to be trained to understand a traffic light!"

In-house tools

Every enterprise should fully examine whether a managed network is right for them, or whether house-owned optimisation tools and teams also have their place.

Indeed, Hodgson calls for every organisation to consider leveraging tools that provide an understanding of the performance and availability of their networks, no matter their size: this is even more vital if the provision of communications usually occurs via a third party.

"Any organisation that relies on one or more service providers to deliver their networks will benefit from having an in-house tool that gives them observability of the services they receive and then deliver to their users," concurs Saunders. "Ideally, in house teams should have access to a location and service-centric view of their network data presented in a standardised way, that is both understandable and comparable, to ensure they can deliver more uniform support to all their users."

Hodgson explains that smaller enterprises with modest budgets and infrastructure must ensure maximum ROI from resources, despite tighter financial constraints, by considering tools that offer a broader, non-vendor specific set of capabilities.

"For organisations with more complex environments, IT teams may benefit from tools that offer increased 'noise cancelling' capabilities. Such tools can help in reducing mean time to resolution (MTTR), ensuring that system alerts related to root causes do not leave admins swimming in a sea of notifications," adds Hodgson.

With access to persistent network data, IT and network managers will be far better equipped to pinpoint the source of problems immediately.

"Look for tools that will capture the Digital Experience, utilising persistent performance metrics and native SLA scoring (including maintenance windows and exceptions) for both individual connections and grouped services. IT and network managers can then hold their service providers to account and reclaim credits where required," says Hodgson. "IT and network managers should also seek a flexible alerting suite with customisable sensitivity to ensure that problems are flagged long before they become outages, with alerts integrated with support ticketing platforms. Look for a tool that will identify broadband speeds, SD-WAN performance, WiFi AP utilisation and analyse trends alongside a reporting engine that will take all the guesswork out of capacity planning."

Even with an excellent MSP in hand, in-house tools deliver unmistakable benefits for the enterprise – and thus should not be overlooked during cost-cutting exercises. ■

Critical communications – what's occurring that's new today?

Duncan Swan, chief operating officer, British APCO

Critical Communications World (CCW) was back for it's 25th anniversary in May returning to Dubai and a chance to see how east meets west on the exhibition floor and in the conference rooms.

The move towards using commercial mobile networks to deliver broadband critical communications is primarily based upon this being the most affordable way for most countries to deliver 4G and 5G based solutions. However, in Dubai it is a little different – with Nedaa, the Dubai Government secure networks provider, enhancing their mission critical TETRA radio network with a self-built 4G LTE network that offers 3GPP MCX broadband functionality for the Emirate amongst other Safe and Smart City applications. Their network supports both government and private clients – but specifically supporting key aspects of public safety and security.

"The move towards using commercial mobile networks to deliver broadband critical communications is primarily based upon this being the most affordable way for most countries to deliver 4G and 5G based solutions."

Listening to representatives of Nedaa was a bright spot in terms of mission critical mobile network use cases – around Europe and North America in particular much is said to be happening but getting real nuggets or soundbites as to tangible delivery progress was as difficult as actually delivering these incredibly complex programmes of work – be that technically, financially, or from an end-user change perspective.

Technically complex to build and deliver, LTE based mission critical solutions still face questions around their underpinning design philosophy. New to CCW2024 were a series of focus group discussions, opportunities for experts and interested parties to debate specific topics. Supporting communications for large user groups at, say, a major incident remains a topic that polarises discussion – mobile networks tend in the main to be unicast, supporting one-to-one communication. Multicast on the other hand was designed to deliver streaming services but provides the ideal one-to-many communication platform; a possible key to unlock the unicast limitations for very large groups. But it has cost implications to build and deliver – and there are use cases where unicast would be a preference. It's fair to say discussion on the topic is polarised and undoubtedly some blend of technology will emerge.

As building the LTE mission critical solutions continues, exciting developments were announced on the exhibition floor by several major players in relation to user devices. Sepura launched their SCL3 hand portable that can be deployed as a hybrid TETRA and 4G/5G device, enabling a pathway for the migration to LTE based mission critical communications. And with a launch customer – the UK Ambulance Radio Programme – in place, then we will soon be seeing the SCL3 in action. It certainly represents the best of British with a well thought through form factor; is incredibly lightweight; and, importantly, uses many existing accessories to ease both implementation and the cost burden.

Motorola Solutions were also making a splash with their new MXP660 multi-bearer hand portable TETRA radio which has built-in LTE and Wi-Fi allowing automatic switching to broadband thus staying connected when out of TETRA network coverage (e.g. when deep inside buildings or in heavily built-up areas). Also with a launch customer in mind, SINE (the Danish public safety TETRA network) will be among the first networks deployed that can support the MXP660. Whilst AI has been a key topic at most critical communication conferences this year, and to a degree at CCW 2024, it was fascinating to learn more about the MXP660's AI-trained background noise suppression capability.

Satellite communications are already playing an important role in critical communication networks, even though there remain challenges to overcome; security, throughput, and latency topping the list. At CCW 2024 we saw the unveiling of a Rapid Deployment Solution by Rohill that integrates Starlink satellite connections with land-based networks. The product is a response to the need for rapid deployment of trusted communication networks during major incidents and large-scale events – but underpins the essential need to support multi-bearer communication to ensure mission critical solutions are robust.

The 3GPP standards body has specified capabilities of relevance to mission critical communications in the 4G and 5G standards; and it was never going to be long before talking started in earnest around 6G. So, no surprise to find a couple of sessions at CCW 2024 on the 6G standard and its relationship with critical communications. Whilst society and the economies of pretty much every country have become hugely dependent on mobile communications supporting such as e-commerce, government, safety and security, 6G should introduce new capabilities that leverage the current ecosystem with seamless integration with 4G and 5G networks. The TCCA believe strongly that 6G should enhance the level of trust users have with systems supporting mission and safety critical operations – and that the 6G standard should simplify the introduction of solutions for critical communications.

"The 3GPP standards body has specified capabilities of relevance to mission critical communications in the 4G and 5G standards; and it was never going to be long before talking started in earnest around 6G."

A final highlight from CCW 2024 was recognition at the International Critical Communications Awards of the ongoing work between Alea, Softil and Qualcomm to deliver a solution for off-network LTE communications. First announced at the end of 2023, Softil, together with Alea, demonstrated the first ever interoperable direct mode communication using devices powered by Qualcomm 5G-Sidelink technology. With devices able to discover each other and communicate without network connectivity then a key critical communications user requirement looks to be finally on the path to resolution. This could be a real game changer for user organisations not only during transition to mobile broadband networks from traditional mobile radio networks but also in areas where it is simply not possible to provide mobile network coverage (or when base sites are down).

Delivering critical communications remains a vibrant industry sector; Critical Communications World returns to Europe in June 2025, and will be hosted in Brussels. At the home of the European Union, it will be interesting to see if the BroadEU. net initiative is showcased alongside the host nations Astrid Network, and all that it can offer. BroadEU.net is a European Union initiative working to develop a pan-European mobile broadband system that interconnects each participating Nations' 4G/5G MCX critical communications network – essentially a virtual pan-European network for all first responders, emergency, and security agencies. ■

Roundtable: is hybrid multi-cloud the future of networking?

In a rapidly-evolving world of interconnected networks, which cloud solution is right for your enterprise?

What are the key benefits of public vs private cloud?

Jonathan Smith, solution area expert, Net Insight: Private cloud enables us to curate exactly the architecture needed for a particular kind of workload enabling full control and allowing for increased efficiency or specialised performance. In comparison, public cloud comes with a lot of pre-baked services that accompany the basic infrastructure offering, allowing immediate access to a lot of potential features and services.

Sandip Channa, CTO, CSI Ltd: The key benefit is convenience - with public cloud there is no capital expenditure required and the billing model of pay-as-you-go is convenient. You don't have to worry about security or resourcing.

Stewart Laing, founder and CEO, Asanti: Many businesses will be tempted by the perceived lower costs of public cloud, however it is essential that they take the time to fully understand their organisation's requirements and the required IT systems and applications, before moving on to developing a cloud strategy that considers all costs, usability, and functionality.

Is hybrid truly the best of both worlds?

Channa: In one sense - it deals with challenges like cost optimisation, regulation and compliance, complexity, and flexibility.

The real challenge is how you migrate between two platforms. Although it is made out that the toolsets are very easy to migrate, there are lots of peripheral systems that must collaborate and connectivity between these is always a challenge. It's all very good switching between a public hyperscaler and your own private cloud, but every time you switch there is disruption.

Hybrid cloud is the way forward to save money as you can place workloads where they are best suited based on resource requirements and to help compliance requirements. Moving data back and forth between cloud platforms is hard, and costly due to egress charges and time required by teams to manage these changes. Organisations overlook these charges and must consider whether they outweigh the cost benefits of public cloud. People may argue the agility and scalability outweigh the other challenges, but ultimately, it's the rightsizing and right-placement of workloads that is driving people to look at hybrid cloud.

Laing: There will be some systems that simply can't exist in the public cloud, either because they are legacy systems or because they have stringent compliance requirements, in which case, they need to reside on a private cloud infrastructure. By looking at each application and system individually, you'll be able to ascertain the requirements for your business and therefore develop the right hosting strategy.

Smith: A hybrid approach can often be the best of both worlds allowing for the operational optimised benefits of private with the flexibility that a public cloud provides.

If we take on the ground media production as an example, the best way to achieve the lowest latency is to harness private infrastructure, enabling the creation of a specialist network to give the optimal bandwidth that would provide the best technical result. Although when moving to the distribution of that production where the need is to extend reach away from operational hubs and venues, it's important to take advantage of the flexibility a public cloud can provide.

The only pitfall is the increased complexity a hybrid approach brings. A hybrid approach means there is a need to create an interface between the private and public environment, requiring architectural expertise across both.

What role is hybrid multi-cloud playing in the UK?

Channa: Organisations are finding it hard to use multi-cloud platforms because of the cross of skills needed. Despite what the big providers say, their platforms require different knowledge and skill sets – it's not as seamless as you would expect. Few IT departments have all the skills for each platform so there is often a need to use MSPs.

Smith: It's a battleground of cloud providers which will continue to be fierce as players try to achieve better market share. If Oracle, for example, is offering attractive egress charging for their private cloud environment, you might want to exit your existing provider, but you must architect to allow this to happen easily.

The relatively small size of the UK means point of presence is not a decision-making factor — making commercial position crucial. Unique offerings will continue as providers try and position themselves more and more aggressively to grab different shares across industry segments.

Laing: Hybrid multi-cloud strategies are adopted to get the balance between infrastructure costs and compliance. We expect this blend of solutions to continue to grow as businesses grapple with the balance of costs, skillsets, legacy applications, and ever-changing business requirements, such as those brought about by the growth of AI.

Do the security risks of public and hybrid cloud outweigh the benefits?

Laing: The challenge with being in a public cloud environment is that you may have no control over where your applications or data reside. This can cause issues with data sovereignty. That's where colocation data centres come into play because they can securely host or replace the on-premise infrastructure, providing organisations with the ability to connect to public cloud solutions appropriately via our network 'on ramps' to public cloud providers, ensuring security and compliance meet with scalability requirements.

Smith: In theory, a very secure private cloud environment can be created; but when you need outbound connectivity, that security becomes a risk. If you're working in an environment where you can truly be a closed ecosystem, then potentially you can create the most secure environment without hemorrhaging flexibility and cost. Conversely, public cloud providers give the best solution to the problem of needing ubiquitous connectivity to that environment because they have the very best practices for potential risk and mitigation.

There is also a pressing need for globalisation and consolidation. The need to centrally hold resources that multiple global entities connect to remotely is becoming more prevalent. The public cloud approach from a security perspective is immediately well-positioned to provide this connectivity, whereas to achieve the same result in a private environment, there is a steep learning curve.

Channa: Public cloud providers put huge amounts of time and money into security and it's hard for smaller organisations to do this. So, there are some major advantages for smaller organisations to using the big providers, but for other organisations like banks who want more security around data, a hybrid cloud provides a better option.

How can an enterprise establish which cloud is right for them?

Laing: It can take 4-6 months to thoroughly assess your requirements but in doing so, will reduce costs and ensure there are no nasty surprises. There are two critical things for enterprises to do. Firstly, you need to understand what the business strategy is for the next five years. Secondly, you must carry out an honest evaluation of the resources in place and whether they meet the requirements of the business strategy.

Businesses should look to deploy appropriate cloud governance framework controls to proactively manage their cloud adoption and avoid losing control of systems, data, and cost. These controls will ensure that businesses utilise the appropriate solutions to maximise value, whether this be on-premises, hosted or public cloud.

Smith: It all comes down to the workload. From that, you identify your infrastructure and your supporting service requirements. It is also dependent on whether a business is making a long-term capital investment over a traditional 3–5-year business term, or whether this investment is a reaction to a very dynamic change in the market which requires a very flexible commercial model to meet that.

Channa: Some organisations want a specific technology from a specific cloud provider. But for 9 out of 10 decisions it will be based on the skill sets they have in-house. For example, if they know Microsoft, they'll likely go with Azure. Organisations usually take the path of least resistance, driven by their current internal resources and their knowledge base, as it's simpler to go with what you know. ■

Jonathon Smith

Sandip Channa

Stewart Laing

Unifying frontline communications at Heathrow Airport

Heathrow is Europe's largest airport, powered by 6,500 employees, and welcoming more than 78 million passengers every year. The airport is home to more than 80 airlines and is Britain's largest cargo port.

From engineering, customer relationship managers, and security personnel, to health and safety, baggage handlers, and other essential airport operations team members, the nature of work for Heathrow's dispersed workforce is around the clock, 24/7/365, and necessitates a reliable, easy-to-use, and operations-focused mobile communication platform.

Moving beyond paperwork

One of the primary difficulties for Heathrow's frontline airport teams revolved around shift scheduling and coverage. It was challenging for employees to trade shifts or find last-minute or coverage, and Heathrow's shift management process involved substantial paperwork. Moreover, airport employees had no reliable way to track that requests were received or accepted by colleagues.

There was no digital access, including no email correspondence between Heathrow's frontline colleagues and teams. This left staff largely reliant on word-of-mouth information sharing or constantly having to monitor and check break room bulletin boards. For shift-based, full-time employees, with teams working in three shifts per day who are on their feet all the time apart from rest periods, this was especially difficult.

After deploying an assessment to gather feedback from frontline workers on pain points and researching technology that could deliver solutions to address them, the airport's internal communications team saw that Heathrow needed an operational communication tool to ensure employees felt connected, informed, and engaged.

Heathrow identified the most important criteria when researching, assessing, and implementing an operational communications tool for the airport's workforce. These included a way to improve communications between airport operations staff; and to ensure a constant flow of communication between these teams and management. The airport also wished to address shift scheduling and coverage inefficiencies; all with an easy-to-use, mobile solution, to help drive bring your own device (BYOD) policy and optimise accessibility.

Creating busy bees

Heathrow decided that what was missing from its internal communications was real-time capability. Heathrow opted to pilot Beekeeper – referred to internally as 'Buzz' – to assess usability and mobile functionality as key features. The team noted that whereas alternative solutions aren't as well-suited to frontline colleagues, feedback pointed towards Beekeeper as a 'very easy to use' communication app that can be accessed directly from a mobile phone.

With Beekeeper, the airport created a digital workplace including an operational communication platform designed expressly to connect and engage the mobile workforce while being desktop accessible for the organisation's office-based employees.

The rollout process was duly conducted by department, with each department having its own communication stream. Department champions launched the stream by posting content over a couple of weeks, and then facilitated training to launch the operational communication tool with other staff. Aided by a launch guide, content guidelines were developed and shared with department champions and staff.

Beekeeper is now an integral part of Heathrow's digital workplace, used primarily for airport operations staff and for employee engagement purposes. Since implementing the operational communication platform, Heathrow's company culture has improved, and has made Heathrow a more proactive organisation to measure and respond to feedback efficiently. Deploying Beekeeper as a delivery mechanism has made communication faster, and has made two-way, horizontal communication possible.

Given that employee engagement and providing a way for staff to weigh in on their daily experiences at work specifically, was a core priority for Heathrow, Beekeeper allowed employees to share photos and comments about what could be improved. Beekeeper provides 'eyes on the ground,' and the ability to surface issues. With employment at historic lows, improving work conditions allows Heathrow to better maintain employee loyalty and enables increased transparency. Conversations started within Beekeeper communication streams allows the organisation to make necessary changes to improve engagement.

In addition to sharing customer success stories and announcing new hires, management encourages employees to use the popular label, #lifeatheathrow, to tag photos from terminals, the runway, and all-around work at Heathrow as a fun and engaging way for airport employees to share what goes on during their shift.

Digitising the experience

The BYOD rollout has gone well for Heathrow, and the importance of good digital security is a key component of this. Aside from providing the workforce flexibility in how they receive and share work information, Beekeeper enables mobile, agile working for Heathrow's operations teams. It ensures Heathrow's employees are always up-to-date with any and all airport operational information, such as weather conditions, and passenger forecasts.

In addition to maintenance reporting, another core operational use case for Beekeeper is shift management. Formerly paper-based, since moving the process online with the app, the organisation has greatly reduced the time this process takes from a week to just a day or two. Push notifications ensure that the shift exchange happens quickly, and coverage can be facilitated peer-to-peer.

In alignment with one of the core priorities for implementing Beekeeper at Heathrow, the organisation now leverages the operational communication platform for employee recognition initiatives. One of the primary ways Heathrow uses Beekeeper is to demonstrate and promote excellent service. Another way Heathrow accomplishes this is to use Beekeeper to communicate airport safety messages directly with colleagues across departments and teams. This has improved safety by notifying employees instantly when safety communications are posted.

Coordinating schedules for in-person meetings for a rotating 24/7 workforce is extremely difficult, not to mention costly from a business perspective. However, Heathrow now ensures that frontline workers receive the need-to-know information for their shift by distributing daily briefing sheets directly through Beekeeper. Posted in dedicated communication streams, these briefing documents are accessible directly from their mobile device. From security personnel and gate agents to airport runway and maintenance teams, this form of digital distribution delivers on Heathrow's goals to make internal communications easily accessible when they need it. ■

easyJet enhances cloud and internet visibility

easyJet is one of the largest low-cost, European point-to-point airlines on the planet. The company operates 336 aircraft across 34 countries and 156 different airports. Reliability is everything in the airline segment, which is why the IT operations teams abide by a proactive approach in monitoring its complex hybrid networks, taking extra steps to keep flights running smoothly.

The warmest welcome in the sky

easyJet is an extremely busy eCommerce and retail business that wants to deliver 'the warmest welcome in the sky' by providing excellent travel experiences at a reasonable cost.

"On top of selling the seats, we need to operate the flight," said Simon Challis, senior technology manager for platform design at easyJet. "The resilience of the airline and our network is critical to ensure we are flying all our customers on time where they need to be."

One thing that differentiates easyJet from other carriers is its operations as a point-to-point carrier. This transportation model means its aircraft fly from one base to another rather than always going through a central hub.

As the company's routes have expanded and its ability to handle thousands of flights per day has grown, so has its network of bases. easyJet relies on bases to store aircraft, and crew members report to or sleep at them overnight. These bases can be seasonal, and the airline must be able to spin them up quickly based on demand. In the past, easyJet connected its bases to the network using traditional MPLS links, which can take up to 90 days to provision.

Embracing SD-WAN

When a customer books a flight, there is a concurrent behind-the-scenes process where the airline schedules crew and aircraft. On top of that, airlines have a responsibility to submit reports of who is traveling where to agencies and authorities. Some airlines are having a tough time keeping up with so many intricacies. Additionally, outdated systems and network outages can add to the difficulties by leading to cancelled flights.

"With how our network works, any small disruption to our operation can have a knock-on effect," said Challis. "It's vital that we assure our services from the very get-go."

As the airline moves to the cloud, easyJet's IT team is not looking to own physical assets or networks but instead wants to provision as much of its infrastructure as possible. As a result, the company has leveraged the public internet and Direct Internet Access (DIA). It is also moving away from its reliance on data centres towards the cloud.

The airline is embracing WAN modernisation as it transforms its network infrastructure from MPLS to SD-WAN and moves many of its applications and services into the cloud. easyJet wanted visibility into how provider networks were routing their applications, how they performed, and the quality of those connections. They also wanted to measure the latency of connections between anything that remains within the data centre and anything that moves through AWS. Since the apps manage such core business functions, easyJet recognised there were challenges in indiscriminately relying on DIA or the cloud provider's fabric when migrating applications into the cloud.

"We want to make sure that the services we provide meet the SLAs that we're given," said Challis.

Faster access, better monitoring

easyJet's applications sit at the core of its business; customers use the apps to book flights or check; airport operations use them to check bags and order planes; and crew members use them to manage tickets and process payments.

During easyJet's transformation, the airline has relied on Cisco AppDynamics for application performance management (APM) to ensure that its customers can make and manage bookings through all its commercial entities. easyJet wanted a better understanding of how its customers and employees were experiencing its apps from their perspective. The airline turned to ThousandEyes to strengthen cloud and internet visibility and improve the monitoring of digital experience from the customer and employee standpoint.

Since its implementation, ThousandEyes Enterprise Agents and Cloud Agents have given easyJet a holistic view of how the applications perform for customers and employees. ThousandEyes helped the company understand what is happening across its estate, which has been valuable for preventative maintenance and cost optimisation.

The company has deployed ThousandEyes Enterprise Agents into its Cisco devices and virtual machines. Combined with its upgraded SD-WAN and cloud architecture, easyJet now has more flexibility and spends less time setting up network connectivity at bases. For instance, when easyJet realises that the fault resides outside its network with a provider, it can conserve engineering resources otherwise spent on troubleshooting.

"We've been able to reduce our mean time to respond to a number of incidents by going to ThousandEyes in the first instance to actually find out where those faults lie," said Challis. "[Our engineers] can then continue improving our services or delivering new services for our customers."

Faster access also means better monitoring of these core systems — enabling easyJet to fortify its competitive advantage and flexibility, making it a point-to-point airline better prepared for growth. ■

Selecting a unified communications platform

Kristian Torode, director and co-founder, Crystaline

Undoubtedly, unified communications (UC) is the way to go for the future of work, combining several communication tools into one system for better productivity and easier working. When selecting a system, organisations must ensure they understand their requirements — the number of users, types of communication channels, integration needs with existing systems, mobility requirements, security and compliance considerations and scalability.

Large enterprises are constantly evolving, and therefore require a solution that's dynamic enough to change with the organisation itself. Look for a platform that can accommodate increasing numbers of users, devices, and locations without compromising performance or requiring significant reconfiguration. Platforms with robust mobile applications are key; they're downloadable on any device, meaning employees can stay connected and productive from anywhere, whether they're in the office, working remotely or on the go. By providing employees with the flexibility to access communication and collaboration tools from any location or device, you can empower them to work more efficiently and effectively, regardless of their physical location.

Integration with existing business applications is key to maximising the ease of implementation and ongoing use of the UC platform. Choose a platform that seamlessly integrates with your organisation's existing systems, such as CRM applications like Microsoft Teams, Outlook 365, Salesforce and Google Workspace. Integration capabilities enable you to streamline workflows, enhance productivity and leverage the full potential of your existing investments. Many UC platforms offer application integration as part of their package, but it's worth checking your existing systems and seeing if integrations exist to ensure that the shift supports employee productivity rather than creating a clunky, difficult-to-navigate system.

Security is paramount when it comes to UC solutions, especially for enterprises that handle sensitive information and operate in regulated industries. Prioritise UC solutions that offer robust security features, including authentication mechanisms and access controls, as well as compliance with relevant regulations — IPSOS 27001, SOC2, GDPR and C5 standards. For confidential comms, a solution that offers end-to-end encryption for video and phone calls and messages could be another worthwhile feature. By choosing a secure UC solution, you can protect sensitive data and mitigate the risk of security breaches or compliance violations.

Large enterprises rely heavily on uninterrupted communication to drive business operations. Therefore, it's crucial to choose a UC solution with a proven track record of reliability and high availability. Look for features such as failover mechanisms, geographic redundancy and 24/7 technical support included in the service level agreement to minimise downtime and ensure business continuity. A reliable UC solution enables your organisation to maintain seamless communication and collaboration, even in the face of unexpected disruptions or outages.

Cost isn't everything, but it is something to consider. Evaluating the total cost of ownership (TCO) of a UC solution — both upfront costs and ongoing maintenance fees — as well as potential savings from increased productivity and efficiency can support you to select the right solution. Are you charged additional fees for removing or adding accounts to the system? Most UC systems work on a subscription-based model, meaning this shouldn't be an issue, but it's something worth checking.

Consider how futureproofed each UC platform is. Technology is constantly evolving, and it's essential to select a UC solution that can adapt to emerging trends and technologies. Look for platforms that demonstrate a commitment to innovation, continuous product development, and support for emerging technologies such as AI and Internet of Things (IoT).

One key feature to look for is a cloud-based system. While on-premise UC systems do exist, a cloud-based platform is by far superior as it gives employees choice on where and how they work, and additionally aren't affected by the upcoming PSTN switch off. Any old-school copper-based technologies, such as PBX phone systems and even FTTC broadband, won't be fit for purpose after 31 December 2027. So, opting for a cloud-based UC system means your business is prepared for 2027 and beyond.

Selecting the right UC solution for a large enterprise requires careful consideration of various factors. Shifting company-wide technology is a challenging move, but by carefully selecting the right UC partner, the shift can be seamless, lead to greater team efficiency and job satisfaction and ultimately greater business success ■

PRODUCTS

Avaya Enterprise Cloud delivers everything needed to create effortless and complete experiences for employees.

Running on a dedicated instance of Microsoft Azure, the business can launch and add extensive unified communications that include video, conferencing, calling, messaging, mobility and workstream collaboration.

Avaya provides a seamless hybrid cloud experience that combines the best of on-premises and cloud solutions without any interruptions to operations. This includes an extensive set of unified communications functions for the modern way of work, from video meetings and conferencing to messaging, mobility, and workstream collaboration.

The complete, simple, flexible, secure, and immersive employee experience drives business forward and offers enterprise-level industry-leading workforce communication and collaboration. The unified communications solution offers streamlined implementation, full-featured personalisation and self-administration, and no limits on user scalability. It enables the enterprise to take advantage of the pay-per-user pricing model and investment protection options.

Cisco UCM Cloud is part of Cisco's cloud calling portfolio, powered by Cisco's Unified Communications Manager collaboration (CUCM) technology, and is hosted in Cisco's Webex data centres across the globe.

The enterprise-grade dedicated cloud calling and collaboration solution provides a simplified, enterprise-class migration path for existing on-premises deployments

Cisco UCM Cloud provides enterprise-class call control, session management, voice, video, messaging, mobility, and conferencing services that are scalable, customisable, reliable, private and highly secure. A secure and scalable unified messaging and voicemail solution with flexible message access from email inbox, web browser, Webex App, Cisco Jabber, Cisco endpoint, smartphone, or tablet with simple administration.

View dynamically generated presence and securely exchange instant messages between individuals or groups using the Webex App or Cisco Jabber instant messaging client. The client also supports click to call, voice, video, and visual voicemail.

Moreover, remote workers can be span up efficiently from the cloud, to support a more flexible workplace, using Cisco mobile clients and applications to get better, more productive employee engagement.

Microsoft Unified Communications empowers businesses with a comprehensive suite of communication and collaboration tools, streamlining work processes, promoting seamless integration, and enhancing productivity. Its flexibility, mobility, and user-friendly interface provide employees with the tools they need to work efficiently, regardless of location.

At the centre of Microsoft Unified Communications is Microsoft Teams, a powerful collaboration tool that offers chat, video conferencing, file sharing, and integration with other Microsoft services. Teams' intuitive interface makes it easy for individuals and teams to communicate, schedule meetings, and work together on projects regardless of their physical location. Meanwhile, Exchange Online handles email, calendars, and contacts, all of which are tightly integrated with other communication tools. This integration streamlines scheduling and ensures that users have a consistent experience across all services.

Teams Calling is another integral part of the suite, offering a powerful and seamless telephony solution. By combining traditional voice calling with modern communication tools, Teams Calling enables users to make and receive calls from any device, whether a computer, smartphone, or desk phone. Teams Calling not only enhances connectivity and accessibility but also offers advanced features like voicemail, call forwarding, and interactive call controls.

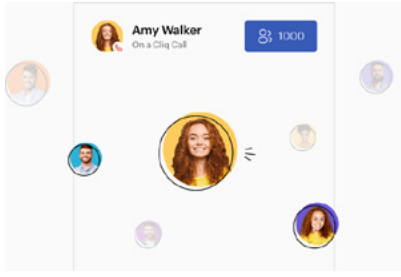
Microsoft Unified Communications streamlines workflows and reduces the time spent switching between applications. This efficiency boost translates into increased productivity for individuals and teams. Employees can work from any location, on any device, without compromising on quality. Consolidating communication tools into a single platform reduces the need for multiple licenses, integrations, and maintenance costs.

Zoho Cliq is a secure business communication and collaboration solution that actively unifies all types of communication – messaging, voice, video, and telephony. Users can collaborate seamlessly within and outside your organization with Zoho Cliq's UCaaS tools.

No matter what Zoho app is in use, the user can access all Cliq chats, make calls, join meetings, and interact with colleagues from the easy-to-access chat bar. The real-time status updates keep users aware of teammates' activities, while the audio and video meetings accommodate up to 1,000 participants in any location – perfect for training and live event broadcasting.

Business calls can be recorded for revisit as needed, to coach sales and support teams, capture essential meeting highlights, and improve operational efficiency. Zoho Cliq also offers real-time screen sharing for audio and video calls. A variety of mobile apps enable on-the-move communications for both Android and iOS devices.

Zoho Cliq offers quick scalability – since it's cloud-based, an IT team is not needed for set up. It delivers 99.99% uptime for a consistent, seamless connection. It also maximises privacy by keeping conversations encrypted and free from third-party attacks with role-based security, stronger password policies, and enterprise-level mobility management.



Zoom Video Communications, Inc. has announced that post-quantum end-to-end encryption (E2EE) is now globally available for Zoom Workplace, with Zoom Phone and Zoom Rooms coming soon. The launch of the new security enhancement makes Zoom the first UCaaS company to offer a post-quantum E2EE solution for video conferencing.

As adversarial threats become more sophisticated, so does the need to safeguard user data. In certain circumstances, attackers may have the ability to capture encrypted network traffic now, with the intent to decrypt it later when quantum computers become more advanced — a scenario often referred to as 'harvest now, decrypt later.' While powerful quantum computers with this capability are not yet generally available, Zoom has taken a proactive stance by upgrading the algorithms designed to be able to withstand these potential future threats.

When users enable E2EE for their meetings, Zoom's system is designed to provide only the participants with access to the encryption keys that are used to encrypt the meeting; this is the behaviour for both post-quantum E2EE and standard E2EE. Because Zoom's servers do not have the necessary decryption key, encrypted data relayed through Zoom's servers is indecipherable. In addition, to defend against 'harvest now, decrypt later' attacks, Zoom's post-quantum E2E encryption uses Kyber 768, an algorithm being standardised by the National Institute of Standards and Technology (NIST) as the Module Lattice-based Key Encapsulation Mechanism, or ML-KEM, in FIPS 203.

Please meet...

Mattias Fridström, chief evangelist, Arelion

Who was your hero when you were growing up?

All my heroes were sports players when I was younger as I really wanted to be a sports star! Wayne Gretzky and Ingemar Stenmark were big inspirations for me but pretty much anyone who was at the top of their game at the time, regardless of sport, was an idol for me.

What was your big career break?

When in 1999 I went from a subsea cable engineer, building subsea cables, to being manager of the team that constructed the Arelion (then Telia International Carrier) fibre network in North America and Europe. I started at exactly the right time, when the dot.com era completely exploded and almost everyone wanted to build networks everywhere. For a few years I travelled the world, met so many funny and crazy people and learned a lot that even today is still extremely useful in our business.

What did you want to be when you were growing up?

I really wanted to be a superstar in sports. I competed in almost all sports disciplines and was sometimes upset that there were only seven days in the week so I could not do them all! Football, ice hockey, volleyball, badminton, squash, downhill skiing, and golf are just a few examples of where you could find me competing for local glory. At the same time, I had a big passion for school and just loved maths, physics, chemistry, and the rest of it, so I ended up being quite good at everything but unfortunately not a superstar at anything.

What's the greatest technological advancement in your lifetime?

It is kind of a dead race between the mobile phone and the world wide web, if they can be considered technological advancements. When I tell my sons about life before these two 'life changers' they look at me with big question marks. The way we have information at our fingertips today is just amazing.

The Rolling Stones or the Beatles?

Growing up, my idols were Kiss, Helloween and Iron Maiden but later I also grew to love both the Beatles and the Rolling Stones. The way both of them broke new ground and inspired new generations was really cool. Having to choose, I would go for the Rolling Stones but maybe that is a bit biased since they are more or less still alive and playing.

If you could dine with any famous person, past or present, who would you choose?

I would have loved to have had dinner with Severiano Ballesteros. He has unfortunately passed away, but we would have discussed all the tricks and infamous stories behind his Ryder Cup success and how to use your imagination when playing your golf at the toughest golf courses. We would also have eaten great Spanish tapas and enjoyed some good Spanish wine in some warm location in Spain.

What's the best piece of advice you have been given?

My manager during 2001 taught me that when top managers make what seem to be weird decisions - they might actually have more information than you realise. Don't draw conclusions too early. Before this I was a young and upcoming manager and really questioned everything I heard if I did not like it, since I always believed I knew better. That advice is still with me today and helps me to be more understanding and curious when I hear things that sound a bit strange.

If you had to work in a different industry, which would you choose?

It would be really cool to work within the space industry. I still find it amazing that we travelled to the moon more than 50 years ago and even today I find it hard to believe that we can send a rocket to space just to find a space station in orbit that we can connect to and work in. Not too many things in the world are 'rocket science' but this really is rocket science.

What would you do with £1 million?

I would desperately try to find someone who could invite me to play a round of golf at Augusta National in Georgia. I understand you need to be invited by a member but with that money in my pocket, I could try to use my contacts to find someone who would be willing to support me! The rest of the money would be used to buy apartments for my two sons to make sure they end up close by once they finish their current university studies.

Where would you live if money was no object?

I would actually not like to live anywhere else than Stockholm. Even if I sometimes question this on the darkest, rainiest days in November, I love the four seasons that we experience every year. Maybe a nicer house in a better place but being close to friends and family is key at the end of the day to me. ■