FEBRUARY 2024
networkingplus.co.uk

NETWORKING+

IN DEPTH: The outsourcing debate p7-8

Towards Net Zero 2050

Over half of UK businesses are unprepared

Richard Henderson, Critical Power Supplies, p5

Is your team ready for new tech?

The appeitite for all things new is growing stronger

Greg Hudson, M247, p9

Questions and answers

I wanted to travel the world as a jet pilot

Gordon Cullum, Axiologik, p16

LockBit - locked down, but not out

In an incredible storyline worthy of the next modern action movie, on 19 February, the UK's National Crime Agency (NCA), the FBI, and nine other country partners took down LockBit in 'Operation Cronos.'

LockBit, in operation for four years, is/was the world's most harmful cybercrime group. With thousands of victims globally, it has caused losses of billions of pounds in both ransom payments and recovery costs through its ransomware-as-a-service.

"LockBit stands out as the most prolific ransomware group with a brazen willingness to attack hospitals and critical infrastructure, unlike many of its competitors," said Christian Have, CTO, Logpoint.

During Operation Cronos, the taskforce took control of LockBit's primary administration environment, which enables affiliates to carry out attacks, as well as its public-facing leak site on the dark web, on which it hosted data stolen from victims. The NCA also obtained the LockBit platform's source code and a 'vast amount' of intelligence about activities and partners.

As a result of the takedown, Europol has coordinated the arrest of two LockBit actors in Poland and Ukraine, and more than 200 cryptocurrency accounts linked to the group have been frozen. The US Department of Justice has announced that two defendants responsible for using LockBit to carry out ransomware attacks are in custody and will face trial.

"As of today, LockBit are locked out," said National Crime Agency director general, Graeme Biggar. "We have damaged the capability and most notably, the credibility of a group that depended on secrecy and anonymity. Our work does not stop here. LockBit may seek to rebuild their criminal enterprise. However, we know who they are, and how they operate. We are tenacious and we will not stop in our efforts to target this group and anyone associated with them."

Despite near global celebration of this achievement, Melissa Bischoping, director, endpoint security research, Tanium, warned that "the takedown of threat actor infrastructure is always good, but often the actors are quick to regroup and bring themselves back online. The disruption may be temporary but still provides valuable intelligence, access to decryption keys that can be provided to victims, and a temporary shakeup that may result in a group fracturing into multiple new groups or branching out on their own from the parent."

Quickly proven correct, just a few days later, LockBit launched a new leak site claiming to have restored infrastructure and inviting affiliates to re-join. The group's leader, 'LockBitSupp,' confirmed that while a PHP flaw had enabled the seizure of vulnerable sites, it did not impact on those not running the scripting language. LockBitSupp also asserted that the takedown has motivated them to improve protections, including decentralising the operation further. Notably, the leader confirmed upcoming operations would target government infrastructures, and has reportedly begun countdown timers for six victims on the new site, including one for the FBI.

While no longer the seemingly untouchable threat it once was, Have reported that the takedown disruption "can change the threat landscape by increasing fragmentation and decentralisation further. This emphasises the need for security teams to move beyond traditional methods of identifying security breaches based on known Indicators Of Compromise (IOCs). Instead, adopting an approach focused on detecting Tactics, Techniques and Procedures (TTPs) is more sustainable, because it takes the threat actor's dynamic methods and emerging threats into account." ■

Digital Futures Programme expansion addresses IT skills shortage

The Digital Futures Programme - which gives students a head start into digital careers - is rolling out to three Thames Valley schools: UTC Reading, UTC Swindon, and UTC Oxfordshire, following its successful launch at UTC Heathrow.

The Digital Futures Programme, which was developed in close collaboration with leading digital infrastructure industry employers, is a first for any UK school. Aimed at 14-19-year-olds, the programme, which contributes to a BTEC Level 3 National Diploma / Extended Diploma in Engineering (NQF), equips students with the essential knowledge and skills needed to thrive in technical careers within the digital infrastructure industry, comprising the network cabling and data centre sectors and other digital environments.

The programme was launched in 2021 by UTC Heathrow and its supporting employer partners and has gone from strength to strength, with the partnership being recognised with three global awards, including the Education and Employment Project Award of the Year at the Datacloud Global Awards.

Industry partners not only provide support in developing the curriculum but also by giving valuable time to deliver a mix of employer-led projects, challenge days, masterclasses, and skills workshops to the students as part of the programme.

The programme is already having an impact, with the first set of UTC Heathrow graduates taking up apprenticeship roles with industry partners as a direct result of the programme. This is hugely important to the digital infrastructure industry, which is relied upon so heavily by our modern, digitally connected world, but is facing an ongoing skills shortage. Activate Learning Education Trust (ALET) and its supporting partners are proactively working to educate students in these important, transferable skills, helping to build a stronger, more sustainable future for the industry, as well as highlighting a new and rewarding career path option to the students.

"ALET is playing a critical part in building a skills pipeline essential to the UK economy to be competitive in the digital world. The Digital Futures Programme represents a unique opportunity for industry to be engaged at a programmatic level to transform the lives of younger people," said Mike Halliday, head of employer engagement at ALET.

"The UK is facing an unprecedented skills shortage: we need engineers, computer scientists and other digitally-skilled staff. The Digital Futures Programme is focused on equipping students with the skills to succeed in the digital industries, bringing together companies which are serious about acting to address the skills shortage with STEM-focused schools with specialisms in digital, engineering and science prepared to forge a new path for their students," said Jo Harper, CEO of ALET. ■

Mavin delivers prefab DC for Welsh rail testing centre

Mavin is deploying its containerised prefabricated Powercube data centre to the Global Centre of Rail Excellence (GRCE) in Onllwyn, South Wales.

The 550-acre GRCE facility, expected to open next year, is a government-owned site dedicated to the research, testing, and certification of rolling stock, infrastructure, and new rail technologies.

GCRE will deploy a custom-designed and built Powercube – a multi-unit and combined Containerised Modular Data Centre (CMDC), Signal Equipment Room (SER), and an interconnecting Access and Staging Unit – to support the testing operations that will be carried out at the railway site.

The Powercube, which will be pre-built off-site in Neath, will support clients with data analysis as they undertake testing and research on the site's two rail tracks – a 7km track for rolling stock testing, and a second track for infrastructure innovation.

The UK currently has no all-purpose railway testing centre, with most vehicles being tested in Europe at sites such as Wildenrath in Germany or Velim in the Czech Republic.

"We are delighted to agree this partnership with Mavin and to utilise their cutting-edge Powercube design at the Global Centre of Rail Excellence site," said GCRE Limited chief executive, Simon Jones. "The ambition is to establish GCRE as Europe's premier site for rail innovation, becoming a one-stop shop for the rail sector, serving markets not just in the UK but across Europe and the Middle East. In providing world-class research and testing facilities, it's important that the supporting infrastructure that we have on-site is of the highest quality – and is as forward-looking as the innovation we will be doing on our tracks."

"We are extremely proud to be involved with this pivotal project from the start, and are looking forward to strengthening the partnership with GCRE over the next few years, as opportunities for broader engagement with GCRE and other critical industries allow us to evolve our solutions to meet the demands of the future," said Mavin founder and Powercube director, Russ Bartley. ■

42 Dundee schools to gain full fibre connectivity with Commsworld

Commsworld has secured a contract worth £2.6 million over 10 years to radically transform the connectivity to 42 schools in and around Dundee.

Dundee City Council's City Governance Committee has given its approval for Commsworld to plan, design, migrate and manage a completely new fibre network service. The future-proofed and enhanced service will be underpinned by a new robust security solution that will boost digital education provision for pupils across the city.

The proposed new high-speed fibre internet service is replacing Dundee City Council's ageing infrastructure currently in place in primary and secondary schools in the city which, due to the rapidly increasing use of digital devices and internet for online learning, is under increasing strain.

It will see Commsworld invest in 40km of new fibre infrastructure across Dundee, with schools gaining access to the fastest full fibre internet connection with initial speeds at a minimum of 1Gbps and scalable to 10Gbs per school.

The new infrastructure will allow each school to boost their digital learning capabilities, enabling greater use of cloud-based services. This includes full reliability, enhanced security, and safeguarding support, plus fully filtered real-time connectivity to ensure all pupils are kept safe online.

Commsworld will also build in extra capacity that will be able to easily absorb any future increases in demand in the years to come.

The new fibre infrastructure will be linked to Commsworld's Optical Core Network (OCN), a next generation multi-million pound network in which it continues to invest, and which was built specifically to boost security and resilience of digital infrastructure to organisations not only in Scotland but also the length and breadth of the UK.

"These services will allow digital learning to be upgraded even further in schools and enable greater use of cloud-based services. The tender is structured in such a way that spare capacity will be built-in to ensure future growth can be easily accommodated," said Councillor John Alexander, leader of Dundee City Council.

"We are keen to achieve Digital Schools Award Scotland (DSAS) status by next summer and, with digital infrastructure such as high-speed fibre internet as a key plank of digital learning, this contract will be an important step on that journey," said Councillor Stewart Hunter, convener of Dundee City Council's children, Families and Communities Committee. ■

STX Next: human error biggest threat to cybersecurity

Research from STX Next has found that 59% of CTOs believe human error to be the biggest cybersecurity threat facing their organisation.

Human error, which can range from downloading a malware-infected attachment to failing to use a strong password, was found to be the more threatening than both ransomware (48%) and phishing (40%) attacks.

Accordingly, CTOs are deploying a range of tactics to protect their teams and wider organisation and are taking advantage of the many solutions on the market. 94% of companies have now deployed multi-factor authentication (MFA), 91% are using identity access management technology (IAM), 58% are using security information and event management (SIEM) technology and 86% are using single sign-on (SSO) solutions.

Some 24% of CTOs said that security was their biggest challenge across the organisation, the fourth most popular response. Despite the growing threat of attack, only 49% of companies surveyed said that they currently have a cyber insurance policy in place, while 59% of businesses have implemented a ransomware protection solution. In-house security teams are still in the minority: just 36% of companies have a dedicated team or department providing security services, whereas 53% of companies are using the services of external specialised companies for security.

"The data from this year's survey indicates that employees are still the weakest point of company security. Despite deployment of comprehensive technology, poor implementation, substandard support processes or lack of governance can render these efforts useless. In recent years, the frequency and severity of cyberattacks across all industries has risen extraordinarily, and employees are often carrying the burden of being an organisation's first line of defence," said Krzysztof Olejniczak, CISO at STX Next. "While the threat of ransomware remains high, in many cases, cybercriminals aren't in fact relying on incredibly advanced and sophisticated methods of attack, but on human error and social engineering techniques to gain access to an organisation's systems. And this method of attack is still the most popular and successful. Human error can also include internal fraud, where employees intentionally do not follow procedures and expose critical information. In response, it's crucial that management teams focus not only on educating staff to recognise and respond to new threats but also on periodically testing their resilience through simulated attacks or phishing and ransomware tests. Frequent testing also encourages good cyber hygiene practices and behaviours. On top of testing and education, solutions such as MFA, IAM and SSO are quickly becoming an industry standard for the modern business and can provide an additional line of defence to limit the risk of human error.". ■

EDITORIAL:

Editor: Amy Saunders
amys@kadiumpublishing.com

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Andy Thompson, Richard Henderson, Jonathon Wright, Greg Hudson, Chris Jones, Duncan Swan, Stuart Dealing, Gordon Cullum

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

rSIM: 43% suffer IoT connectivity loss every week

Global businesses are suffering major financial and human costs from critical IoT connectivity failures with almost two thirds losing sales and customers as a direct result, according to a new report from rSIM.

The rapid growth of cellular-based IoT devices is set to explode as 5G networks roll out worldwide, with 7 billion expected to be online by 2033. However, this is increasing pressure on network providers and businesses are struggling to cope with the current lack of resilience, with two-thirds stating it has become more business-critical in recent years.

The survey found that reliable connectivity is essential for operations in 87% of companies. In fact, connectivity was stated as the number one issue currently faced by businesses in every region, deemed more problematic even than securing and retaining business or staff.

Almost all the businesses in the survey revealed they suffer from some form of connectivity loss every month, with 16% experiencing a network incident every day and 43% at least once a week. The total outage time during a month clocked up to an hour for 60% of the respondents, with more than a third (37%) experiencing even more time offline, and a quarter (25%) saying that they have been hacked due to connectivity issues.

Almost 1 in 2 (43%) of those surveyed also said that connectivity problems have caused "life affecting changes" to either staff or the users of their products.

The biggest concern is with the connectivity of IoT devices, which businesses and individuals increasingly rely on for day-to-day tasks. More than 80% of these are deemed either mission, business, or life critical, yet over half of the companies surveyed (58%) revealed they have suffered connectivity problems with their IoT devices (e.g. payment machines and remote patient monitoring devices).

"The results of the survey did not come as a surprise. Our business lives and breathes connectivity and we understand the pain points that companies experience when they are without it," said Richard Cunliffe, director, rSIM. "The incredible growth of IoT devices that we have experienced is putting huge demands on network resilience, and future expansion will be simply impossible with the current levels of reliability provided. The results of the survey back up that view, and the call to arms to do something about it is a challenge we have been delighted to take on. People currently accept that mobile connectivity is just not reliable. That is the norm. And that is why the term 'critical connectivity' has come up. In the past, the requirement for always on, real-time data from devices has not always existed; there was a time where businesses could live with bad connectivity. But the more connected the world becomes, the less we can live with the outages we see day to day, and the more critical connectivity becomes to daily life. New solutions are never usually developed until the pain points become bigger and need fixing." ■

BT launches NB-IoT for smart city applications

BT (EE) has launched a new multi-million-pound Narrowband Internet of Things (NB-IoT) network, which is a low-power and long-range fixed wireless network that claims to cover 97% of the UK's 'outdoor population' (not geography) and will be used to connect sensors or other smart IoT devices.

The new standards-based NB-IoT network is a type of Low Power Wide Area Network (LPWA), which is similar but different from LTE-M and will harness EE's licensed 1800MHz spectrum band. It can also co-exist with existing 2G, 3G, and 4G mobile networks.

The new network is envisaged to cost-effectively support smart city initiatives across the public sector, utilities, construction, etc. Indeed, the network will allow BT to help fast-track smart cities of the future through use cases that include monitoring and optimising energy use, storage, and distribution. The agricultural industry will also stand to benefit from IoT connectivity, with BT having previously trialled sensors to monitor haystack temperature and prevent fire risks, as well as safekeeping of livestock through gate sensors.

"Growing numbers of businesses are beginning to realise the benefits of IoT applications, and our UK-wide NB-IoT network opens up a wide range of connectivity solutions for monitors, sensors, and other smart devices," said Chris Keone, MD of division X, BT. "Whether it's building the smart cities of the future or reducing carbon emissions, our network will provide customers with the reliability and efficiency they need." ■

Convert uncertainty into a business advantage

As customer and investor requests for sustainability reporting increases, so does the importance of accurate measurement of IT loads, all the way down to the device level. Reducing the environmental impact of enterprise IT begins with collecting data and reporting metrics to establish a baseline. But with dozens of potential metrics this can be a daunting task. For many CIOs, the main problem is they aren't sure where to start. Data centre space and energy costs require you to make the most of every square meter and kW. This will also enable you to avoid underselling floor space and be better equipped to keep up with increasing demand. As pressure mounts to measure energy consumption, DCIM becomes an essential tool for sustainability.

By utilizing a DCIM solution, you can now increase revenues through better space, cooling, and power capacity management. This will also enable you to avoid underselling floor space and be better equipped to keep up with increasing demand. And that is where EcoStruxure IT becomes an essential tool.

Start measuring power consumption today so you can display progress, identify issues, and improve performance. All of our DCIM solutions measure the power consumption of your IT. For example, EcoStruxure IT Expert has measurements on power and history for changes, e-conversion recommendation, and battery wear models. EcoStruxure IT Advisor and Data Center Expert are our on-prem solutions with DCE measuring power consumption and temperature history for changes. IT Advisor has an energy efficiency module and more.

With EcoStruxure IT DCIM software, data captured at a granular level, aids your business in sustainability reporting. A tenant portal also allows your customers to monitor energy use and emissions within their own leased space. Furthermore, you can plan and model changes to power and cooling, estimating efficiency improvements.

Like to know more? Join Schneider Electric at stand No: D730 at Data Centre World, London, on 6-7 March, 2024, to find out how EcoStruxure IT can aid in improving sustainability.

DATA CENTRE WORLD

VIRTUS unveils new 75MW DC for Saunderton

VIRTUS Data Centres has announced plans for a new state-of-the-art data centre campus that will be built on a recently acquired 50 acre freehold plot in Saunderton, Buckinghamshire, close to the existing data centre hub of Slough, west of London.

This strategic initiative is in direct response to the rapidly evolving needs of AI and marks a significant leap forward in delivering AI-ready, mega-scale, high-capacity data infrastructure.

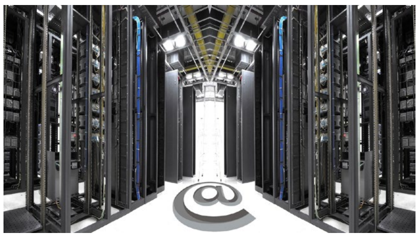
The current design comprises four data centres capable of delivering IT capacity of 75MW to meet the escalating demand for robust data infrastructure that is being driven by the proliferation of cloud and Artificial Intelligence applications. The site has approved planning and is cleared in preparation for construction, with building works due to commence in the fourth quarter of 2024 and be ready for service in the second quarter of 2026. The VIRTUS Saunderton campus has a National Grid contract for 120MVA.

"The acquisition of this new 50 acre campus is a significant step in VIRTUS' strategic growth plans. It demonstrates our ongoing commitment to provide advanced data centre facilities in the UK, whilst also expanding our operations in Europe," said Neil Cresswell, CEO, VIRTUS Data Centres. "Our focus is to support the evolving requirements of our customers, wherever they need them, and the burgeoning demand for AI-ready data infrastructure. We are dedicated to being at the forefront of supporting businesses on their digital transformation journeys, whilst ensuring that our data centres are built to the highest sustainability standards, aligning with our target to be carbon neutral by 2030."

The new campus further demonstrates VIRTUS' commitment to ESG initiatives, making this project not only a technological advancement but is also positive for environmental and societal good. The campus will feature 100% renewable energy consistent with the rest of the VIRTUS portfolio. VIRTUS has committed to a zero-waste-to-landfill principle during the facility's operation and aims to achieve Leadership in Energy and Environmental Design (LEED) Gold accreditation for sustainability.

Other sustainability features include implementation of rainwater harvesting and exploration of waste heat use for adjacent farming. Additionally, an annual carbon offset payment will be made to the local authority for ten years, contributing to local environmental improvement projects.

With the new site, VIRTUS will create skilled jobs, invest in the community, and improve local infrastructure. ■



Keepit opens HQ

Keepit has opened a UK headquarters in London expanded its UK team, led by industry veteran Jerry Mumford, VP for UK, I, and MEA.

Launched in 2007 and built exclusively for SaaS applications, Keepit is the only vendor-independent cloud dedicated to SaaS data protection.

This announcement builds on a recent $40 million refinancing package from HSBC Innovation Banking and launch of the Keepit Partner Network as the company evolves to a partner-only strategy. Over the past three years, Keepit has seen 100% YoY growth in the UK and is on target to repeat this in 2024. The opening of a local office highlights the company's plans to expand its local market share and cements its commitment to providing its UK customers with local support.

"Establishing a stronger base in the UK is an important step for Keepit: an opportunity to build on the foundations we already have here, and grow our partner ecosystem and customer base," said Jerry Mumford, Keepit VP for UK, I and MEA. "The UK market is significant, with a robust IT infrastructure and high levels of new technology adoption. But that means it is also a key target for cybercriminals and of course data loss can seriously impact business continuity. Our commitment to vendor independence, broad service coverage, fast recovery times, and dedication to security, will mean that more UK organisations will have the resilience to keep their businesses running, even when disaster strikes."

One of Keepit's UK customers is the National Gallery, which protects its Microsoft365 data within the UK at two separate data centres to meet compliance regulations. Keepit's ease-of-use, the quick initial set-up, and the competitive price appealed to the IT team. ■

ICS.AI and Derby City Council expand smart city plans

ICS.AI and Derby City Council have announced an expansion of their partnership through a £7 million AI project aimed at transforming public service delivery. This four-year initiative marks a significant advancement in applying generative AI technologies to enhance customer service operations across the council's various departments.

The deal will see an expansion of AI capabilities into critical areas such as Adult Social Care, Customer Services, and Debt Recovery, which were selected through comprehensive workshops that identified 54 distinct use cases for AI integration. Following this phase, Derby City Council plans to roll out further phases of AI adoption across other service areas.

Central to this initiative is the deployment of ICS.AI's SMART Copilot AI platform, which uses advanced generative AI capabilities to tackle complex enquiries, mirroring human-like understanding and responsiveness, and setting a new standard in public sector service provision. ■

Segro ponders 24 new DCs

Property investor Segro could develop up to 24 data centres across the UK and Europe after raising £900 million in a share issue.

Segro will use the proceeds to develop its portfolio, and is eyeing the data centre market for growth. Much of its property is currently used for warehousing.

"We appreciate the support from our investor base for this equity placing and the confidence it demonstrates in our business," said David Sleath, Segro chief executive. "In addition to the profitable growth opportunities within our development pipeline, we expect further exciting opportunities to emerge in the coming months which this additional capital will help us to deliver."

Segro said that it could build up to 24 data centres with 1.2GW of IT capacity, constructed on vacant sites in its landbank, as well as existing facilities that have the potential for redevelopment.

Segro has already tested the data centre market with a series of investments at Slough. In December 2021, it paid £425 million for an office park opposite the Slough Trading Center, which it already owned, and merged the two to develop a cluster of data centres. In 2022, Global Technical Realty broke ground on a 40.5MW data centre at Slough Trading Estate, leasing the space from Segro, and in August 2022, Segro announced its application to develop a further data centre park in Thorney Business Park in Iver. ■

Word on the web...

Why your legitimate software is not safe

Andy Thompson, offensive research evangelist, CyberArk

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

UK businesses' journey towards Net Zero 2050

Richard Henderson, senior consultant, Critical Power Supplies

In a landscape increasingly shaped by environmental imperatives, recent data from Critical Power Supplies (CPS) unveils a significant dissonance: over half of UK businesses find themselves unprepared for the looming Net Zero 2050 targets, despite a palpable upsurge in interest in sustainable energy solutions. The findings, derived from a thorough survey conducted by CPS, not only underscore the urgent need for preparedness but also spotlight the evolving challenges and opportunities as demand for sustainable power solutions escalates.

CPS's survey, conducted in October 2023, engaged a diverse spectrum of stakeholders, including business leaders, facilities managers, technology managers, and energy managers. The objective was clear: to gauge the level of preparedness among UK businesses for Net Zero 2050 targets, delve into readiness for potential energy supply disruptions, and unearth the multifaceted challenges encountered in transitioning to renewable energy sources.

Amid mounting concerns over climate change, a staggering 68% of respondents acknowledged the anticipated surge in demand for back-up power solutions, driven by a collective endeavour to meet sustainability targets. Furthermore, nearly half (48%) underscored the critical importance of formulating a comprehensive energy resiliency plan, one that encompasses robust back-up power capabilities. However, despite these acknowledgements, a concerning 57% confessed to being unprepared to handle future energy shortages and disruptions, laying bare the existing chasm between aspiration and readiness.

> **"Amid mounting concerns over climate change, a staggering 68% of respondents acknowledged the anticipated surge in demand for back-up power solutions, driven by a collective endeavour to meet sustainability targets."**

One of the pivotal revelations of the survey was the glaring absence of transition plans towards renewable energy sources. Alarmingly, a mere 13% of respondents reported having a Net Zero transition plan in place, a factor that could significantly impede their capacity to navigate future energy disruptions effectively. This deficit in strategic foresight poses a formidable challenge, demanding urgent attention and proactive intervention from stakeholders across industries.

The survey identified cost as the primary stumbling block to transitioning to renewable energy sources for back-up power, with a staggering 78% of respondents citing initial investment costs as a major deterrent. Moreover, a substantial cohort (33%) anticipated no cost savings, while 28% envisaged only minimal savings, underscoring the prevailing apprehension surrounding the economic feasibility of sustainable energy solutions. Equally concerning is the revelation that 61% of respondents remained oblivious to the government support and incentives available, pointing towards a pervasive knowledge gap that impedes informed decision-making and resource allocation.

Jill Griffiths of Berkshire Healthcare NHS Foundation Trust offered a poignant reflection on the economic challenges inherent in achieving Net Zero goals within the NHS infrastructure. She underscored the imperative for greater government support or local partnerships to mitigate the financial burden and ensure the viability of sustainability initiatives. Similarly, Steve Groom, CEO of Vissensa, sounded a cautionary note, highlighting the delicate balance between environmental imperatives and economic competitiveness. His remarks underscored the pressing need for a nuanced approach that safeguards both environmental stewardship and economic resilience.

Jason Koffler, CEO of CPS, offered a comprehensive analysis of the survey findings, emphasising the dual challenge confronting businesses in their response to climate change. He stressed the imperative of reducing environmental impact while simultaneously building resilience against its cascading effects, advocating for a holistic approach that integrates renewable energy solutions with robust backup strategies. Koffler's insights underscored the pivotal role of businesses in driving the transition towards a sustainable future, underscoring the imperative for collective action and strategic foresight.

In conclusion, the survey findings serve as a clarion call for UK businesses to recalibrate their priorities and redouble their efforts in pursuit of Net Zero 2050 targets. By embracing renewable energy solutions, addressing barriers such as cost and knowledge gaps, and fostering collaborative partnerships, businesses can not only mitigate environmental impact but also safeguard their long-term viability in a rapidly evolving energy landscape. ■

Combatting modern security risks with unified network management

Jonathan Wright, director of products and operations, GCX

As digital innovation evolves across all types of industries, the cyber-attack surface has been expanding in tandem. This is an unfortunate, but unavoidable consequence of increased digital transformation. As a result, enterprises have been forced to seek out networking solutions to match the surge in cyber threats and tackle them head-on.

One such networking solution is Software-defined Wide Area Network (SD-WAN) architecture. Originally designed for on-site work, SD-WAN was fit for purpose at the time, but the post-pandemic workplace has since turned this network solution upside down. Now almost four years on, many businesses favour hybrid and remote working models – which appear to be here to stay.

But, what does that mean for SD-WAN? For me, it's simple. Businesses shouldn't be relying on something that wasn't designed for the modern workplace. Not only because they face falling behind if they don't adapt with the times, but because this technology is now producing a significant risk to network security.

SD-WAN's limitations

Specifically, organisations now have to think about additional security measures, like securing people and devices to applications not just on-site, but also remotely. The authentication process is one example of where SD-WAN falls short, as once a VPN circuit is authenticated (regardless of who opened it), no further traffic analysis occurs within the circuit. This means that networks relying on SD-WAN will have limited visibility over their network subscribers' traffic and behaviour after initial authentication, which hampers an organisation's threat detection capabilities and means that further threat mitigation policies aren't available.

This is non-negotiable in today's cyber-threat landscape. More devices being added to the network means more entry points for cyber-criminals to exploit. So, simply put, relying on SD-WAN as your network access in today's threat landscape just won't cut it anymore.

Combining SD-WAN with SASE

Of course, many organisations have invested a lot of money in SD-WAN. And, yes, it may have its limitations in the modern workplace, but it shouldn't be abandoned altogether. One such alternative measure that we've seen is implementing cloud-centric security frameworks like Secure Access Service Edge (SASE) over their existing infrastructure.

Where SASE builds on SD-WAN infrastructure is that it provides end-to-end protection, which means it is equally effective at enforcing security on endpoint devices as it is with full offices, which is central to enabling organisations to mitigate their growing attack surface, as the increasing number of endpoints no longer presents the same risk.

Supporting with SASE Zero-Trust architecture

Moreover, bringing these two solutions together under one unified network gives organisations deeper inspection capabilities, as together they can be more easily supported with zero-trust architecture. This would also give organisations the ability to apply security policies at more granular levels.

More specifically, organisations would be able to access important data reflecting user mobility, the health of the device accessing the data, user seniority, and location. Where SD-WAN technology doesn't analyse the data within the network connection following authentication, zero-trust works at a more granular level so keeps track to ensure that organisations have the best possible visibility.

Zero-trust architecture is a key feature of the SASE framework. It offers greater visibility in the form of real-time data tracking capabilities, creating a platform for protecting data on its journey from the end user's device to the cloud. Importantly, this enables hybrid and remote working capabilities whilst enhancing security - just what a modern-day business needs.

Relieving the pressure on IT teams

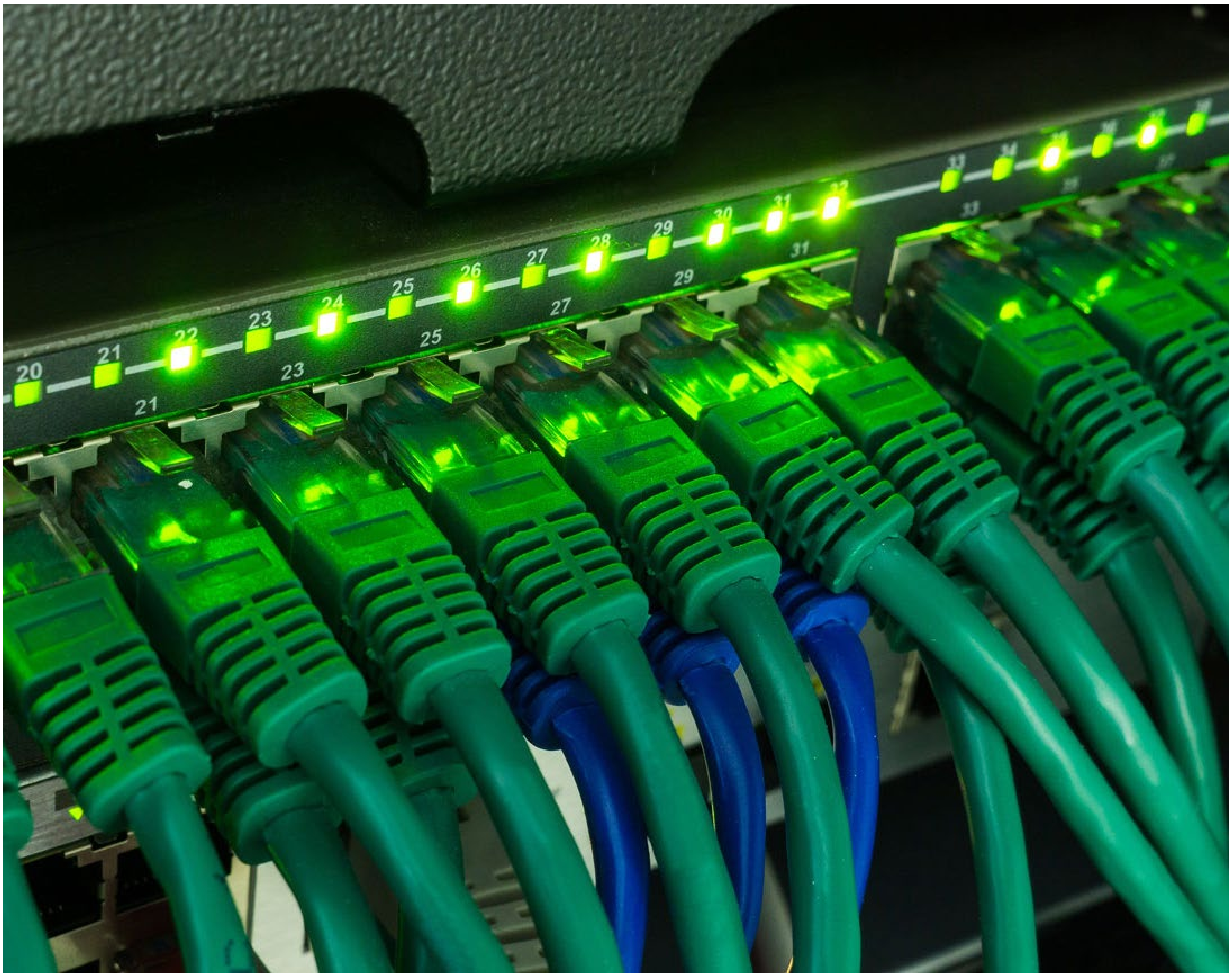
While the security benefits alone should be enough to consider this route, unifying network operations to one platform also reduces the burden on increasingly shorthanded IT teams.

For example, streamlining network management and security significantly simplifies traditionally complex operations, which can help increase efficiency and cost savings as a result. Additionally, unified network management allows for a more consistent application of policies and configurations across the network, whether they be related to security or not.

Moreover, many enterprises span several countries in their operations and are therefore required to meet different compliance standards across the different regions. So unifying network management to a single platform not only bolsters security but also ensures better compliance with regulatory requirements and industry standards, giving peace of mind to teams involved in these processes.

Streamlining modern security operations

In the world of modern business, innovation brings forth countless opportunities but also introduces a whole host of security challenges. To combat these risks, organisations must integrate cloud security infrastructure into their operations. However, a more crucial step lies in consolidating network infrastructure onto a single platform, enabling seamless support for zero-trust architecture. This unified approach I believe not only simplifies IT operations but facilitates a more robust application of security policies, ultimately leading to a more secure and cost-effective infrastructure for businesses across all industries to reap the benefits for years to come. ■



Data centres – the outsourcing debate

The data centre buy vs build debate continues, but how have recent technological developments like AI, edge and cloud affected things? We ask those in the know for their views on the market...

The question of buy vs build is nothing new for data centre (DC) operations. The benefits of each have long been debated, and a hybrid compromise oft reached that considers the specific needs of the enterprise.

"I don't believe either building or buying DC space is universally 'right' – there are always going to be client or application specific factors which apply and, for a specific use case, make one more advantageous than the other," asserts Zac Potts, head of sustainability and innovation, Sudlows.

Build?

Naturally, one of the biggest arguments in the 'buy' column is flexibility and control over the design, operation, and maintenance of the DC infrastructure.

"By building their own DC, network managers can customise it to meet their specific needs, such as security, performance, intelligence, scalability, and reliability," says Matt Salter, sales director, Onnec. "They can also choose the best location, equipment, and vendors, and optimise the costs and efficiency of their operations."

Niek van der Pas, lead data centre expert at Minkels, a brand of Legrand, agrees: "building a DC from scratch provides complete control over the design, layout, and infrastructure specifications. This allows organisations to tailor the DC to their specific requirements and optimise it for their network infrastructure."

Potts adds that it enables the business to "capitalise on opportunities for sustainability which may be present for an individual use case – for example an edge facility with heat recovery supporting on-site demand."

Moreover, collaborating closely with vendors in the initial phases provides valuable insights to define realistic objectives aligned with the company's strategy, says van der Pas. "Achieving ambitious goals for optimal sustainability and maximum security while adhering to stringent budgetary constraints requires transparent and direct communication with all stakeholders."

Or buy?

The argument for 'buy' also contains several compelling points, including savings in time, upfront investment, ongoing expenses for power, cooling, and staffing, and the significant advantages afforded by ready-use infrastructure.

"It's also worth noting that building a facility follows onto operating a facility, maintaining the electrical and mechanical systems, and undergoing repairs and replacements where required," explains Potts. "I believe it is often the ongoing operation of the facility, more than the construction, which influences the decision to lease space over building and operating in-house due to the expertise required to do so and the cost uncertainty associated with unexpected failure of equipment."

Salter highlights the need for network managers "to have the expertise and resources to manage the complex and dynamic challenges of running a DC, such as compliance, disaster recovery, and cybersecurity," a tough ask given today's skills shortage.

"Leasing space requires a lower initial investment, a shorter commitment, and the opportunity to increase and decrease capacity over time. Over the long term, it may cost more, but there is also an element of cost certainty during the contract period," advises Potts.

On the other hand, "purchasing a DC provides network managers with a facility that is already equipped with power, cooling, rack space, physical security measures, and networking infrastructure. This means immediate deployment and management of network equipment without delays," compares van der Pas.

Potts adds that "the colocation market is competitive, and I do think that this has resulted in an increase in quality across service providers in recent years. There are some very well designed and very well operated colocation spaces, which for some end users will outweigh what they could reasonably deliver for themselves without substantial investment, which for a low-capacity requirement could be somewhat disproportionate."

However, that's not without exception: "some colocation facilities do not offer the level of quality, efficiency and service expected, and for some users no matter the quality of the offering, colocation is not going to be a suitable option for their operating model," warns Potts.

Matt Salter

Niek Van der Pas

Zac Potts

Has AI changed the game?

The benefits of outsourcing versus ownership have evolved significantly with the advent of AI. While outsourcing certain tasks has long been recognised to leverage expertise and reduce costs, the emergence of generative AI introduces new considerations.

"The speed of deployment is a critical factor in the success of AI implementations," says van der Pas. "Colocation often has the advantage of having availability over yet-to-be-assigned floorspace. Critical here is the flexibility of the initial design to support high density deployment with high power and cooling demands at the rack level."

Indeed, generative AI and the IT systems which support them impact specific challenges to DC infrastructure which must be factored into the decision for outsourcing. While the technology has the potential to transform various industries and applications by enabling innovation, personalisation, and automation, it also poses new demands, such as high-performance computing, massive data storage, low-latency networking, and enhanced security.

"Therefore, organisations that want to leverage generative AI need to consider whether outsourcing or owning their DC infrastructure is more suitable for their goals, budget, and capabilities," says Salter.

"I don't believe that the use of AI fundamentally means that ownership or outsourcing is now better than the other but will certainly impact choice due to the specific demands," says Potts. "One factor to consider is that AI technology is changing rapidly, and one challenge with building DCs and physical infrastructure has always been forecasting the future requirements. This challenge is significantly amplified by the advent of systems to support AI – what will the requirements in five years look like, and which model can best support that? Invariably time will tell which decisions best served the needs and requirements of individual businesses."

"While outsourcing certain tasks has long been recognised to leverage expertise and reduce costs, the emergence of generative AI introduces new considerations."

What about edge vs cloud?

As organisations increasingly digitise operations, manage larger volumes of data, and adopt emerging technologies such as edge computing, the necessity for robust DC infrastructure is likely to rise.

"As with colocation and ownership, discussions and debates around edge and cloud computing will have different use cases seeing a different balance of advantages and disadvantages," says Potts. "While some users will benefit clearly from one approach, these are not entirely mutually exclusive, and a hybrid model is often possible."

Salter says that edge and cloud computing both have different advantages and disadvantages for DC deployment and management: "edge computing is useful for organisations that want to avoid data transmission delays and enhance data security, reliability, and scalability, especially for time-sensitive or remote applications. Cloud computing is useful for organisations that want to access a wide range of IT services and resources, without having to own or maintain physical hardware and software. Depending on their needs and preferences, organisations can choose to either own or colocate their edge, cloud computing infrastructure, or use a hybrid or multi-cloud approach that combines elements of both."

Indeed, cloud allows users to focus on the application layer, without the need to manage the hardware and associated M&E systems, but this comes at a premium, as well as a compromise in self-sufficiency and control.

"Cloud has certainly allowed for a large number of inefficient on-premises small DCs and comms rooms to be decommissioned, allowing for overall efficiency gains and staff to focus more on the services provided, however the trend towards hosting cloud services in a smaller number of hyperscale facilities delivers diminishing returns from an efficiency perspective, introduces inefficiencies in the transit of data from the user to the facility, and precludes the opportunities for sustainability which an edge DC can deliver," says Potts. "When making decisions with regards to edge, cloud, colocation and ownership, it is important to ensure that all factors are taken into account, and in particular, a wide view of sustainability."

Meanwhile, van der Pas asserts that "as the demand for low-latency applications rises with the emergence of technologies like IoT and AI, the expansion of edge computing is expected to accelerate. Edge DCs that are closer to the sources of data generation will likely see increased investment and development, enabling faster processing, reduced network latency, and improved performance. If latency is crucial the control over the network is essential and is likely operated by a single provider. This can also be solved with more complex infrastructure, multiple providers, and carrier neutral edge DCs. Not close to the edge but in-between the cloud and the far edge."

The future of DC operations

There will always be enterprises with no interest in building and operating their own DCs, just as there will always be those who value the control enabled by ownership.

"Both options will continue to coexist and evolve, as different organisations have different requirements and preferences for their DC infrastructure," opines Salter. "However, in addition to increasing demand for cloud computing, edge computing, and generative AI, there will be a growing awareness of environmental and social responsibility, and the emergence of new technologies and standards. DC providers and operators will need to adapt and innovate to meet the changing needs and expectations of their customers, as well as the challenges and opportunities of the digital landscape."

No matter the outcome of the build vs buy discussion, "facilities within which space is bought or leased, or within which cloud services operate, still require building and it is fair to say that to meet the growing demands, in whatever form they take, a lot of new facilities are required to be built," says Potts.

van der Pas, meanwhile, believes that the next few years will see increased focus on constructing or utilising DCs powered by renewable energy sources to minimise environmental impact.

"Expectations from DCs will include supporting the necessary technology demands and addressing renewable energy and sustainability concerns. Energy-efficient designs and technologies will be prioritised to ensure sustainability and minimize carbon footprints along with market trends and technological advancements that will influence the expectations for DCs in the future," says van der Pas.

Moreover, adherence to regulations will become essential as the market moves from adopting best practices to establishing standards and eventually meeting regulatory compliance.

"Only if you are willing to keep up with these requirements will a new build DC be in your reach. The big advantages of maintaining control can only be attained through close cooperation with suppliers. Therefore, choosing suppliers capable of offering a comprehensive understanding of these new aspects is crucial," shares van der Pas. ■

Is your IT team ready for new technology?

Greg Hudson, chief portfolio officer, M247

There's no shortage of emerging technology available to businesses in today's 'information age.'

The arrival and popularisation of generative AI is just one example that dominated the headlines last year. And in the background, the appetite from businesses to adopt all things new – from digital network connectivity to more sophisticated cybersecurity – is continuing to grow and grow. Research from Gartner this year revealed that 91% of organisations are engaged in some form of digital initiative and for senior business leaders, 87% of those surveyed believe that digitalisation is a priority.

This is great news for business leaders, who seek to drive greater efficiencies and stay ahead of the competition by adopting a tech-led approach. But those tasked with executing their organisation's digital transformation – and working with this technology on a day-to-day basis – may be showing signs of fatigue.

The problem is that every new tech breakthrough is hailed as 'game changing' and it has sparked what's known as the 'change fatigue' phenomenon: a state of exhaustion and resistance in the face of persistent transformation projects.

Research from AlixPartners found that, while the majority (98%) of CEOs expect to transform their business model in the next three years, 72% are concerned about their team's capacity to handle the transformation. And similarly, a report from SolarWinds found that only one in five (22%) IT workers have developed their understanding of how new AI tools, such as ChatGPT, actually work..

Build vs buy

Yet, change fatigue aside, digital transformation remains a key strategic objective for most organisations. CTOs and other tech leaders will need to think about how they can successfully incorporate these new technologies into their business, without displacing or overwhelming their staff in the process.

Often, this is a question of 'build vs buy' – an age-old dilemma that has faced businesses at every technological turning point throughout history.

While some organisations have access to the resources needed to develop, or build, digital technologies in-house (budget to invest in R&D; training to develop new digital skills in staff; and time to roll-out new platforms internally), smaller businesses are without that luxury. In these cases, partnering with a specialist is often the best point of action.

Managed service providers (MSPs), for example, remotely manage their clients' IT infrastructure and end-user systems, including network and infrastructure management, security and monitoring, and implementation of new technologies. MSPs also provide business continuity to their customers and can remedy staff/ skills shortages by taking on the burden of troubleshooting technological issues.

In this sense, they can become a vital support to smaller organisations, helping them to navigate their digital transformation and recommending which new technologies meet their business needs.

Complexity of new tech

When we look at how advanced new technology is today, we start to see how important the 'build vs buy' question is. AI, 5G, and the Internet of Things (IoT) are just a few that are set to develop massively over the years ahead.

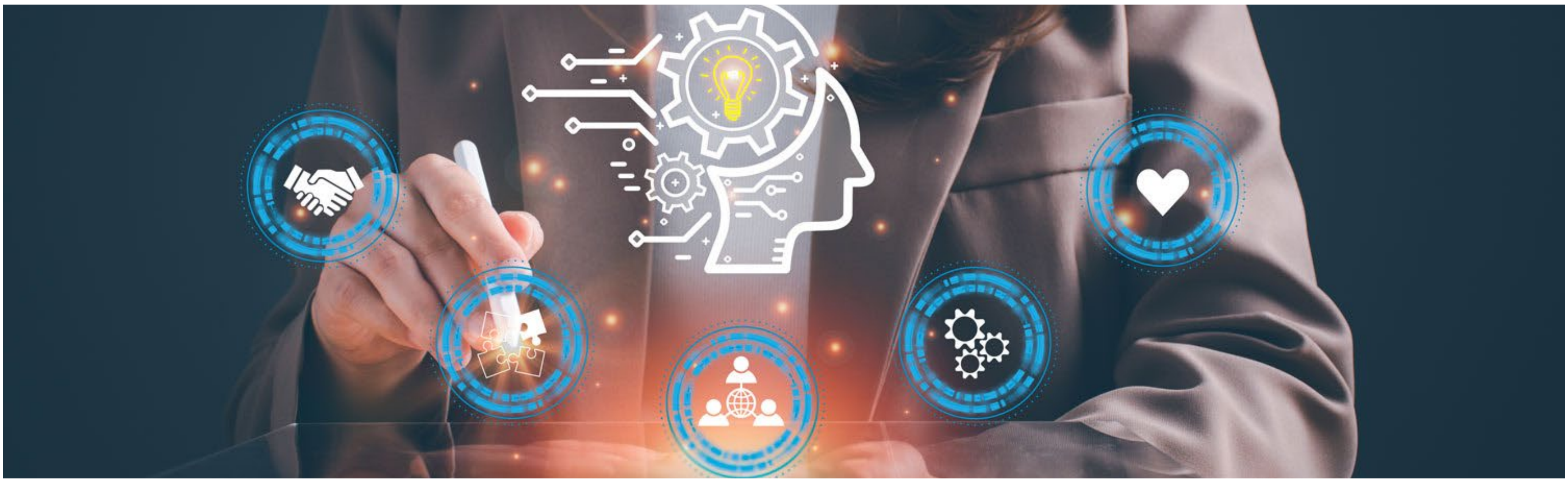
AI will bring with it the ability to mine complex data and process patterns to allow for the automation of business operations 5G networks and wireless leased lines (or radio connectivity) will deliver ultra-fast speeds for data transmission; and IoT will expand exponentially as more and more devices become digitally enabled and inter-connected.

Each of these technologies promise a goldmine of efficiencies and benefits to make business operations faster, deliver quality data, and automate routine aspects of workflows. However, any digital transformation project will require a heavy lift to get new systems up and fully integrated into existing IT infrastructure – not to mention the necessary training to get workers up to speed with the new technology.

Final words

For businesses looking to stay competitive and remain on the front-foot in today's digital landscape, they must be taking their first steps to embracing this new technology today, not tomorrow. When embarking on a digital transformation project, businesses must conduct their own assessments as to whether they have the resources to do it in-house. If not, and their IT teams face a road of fatigue ahead with tech breakthrough after tech breakthrough, seeking out the support of dedicated MSPs can help to create a more seamless digital transformation journey.

As AI, IoT and 5G continue to advance and work together in the years ahead, this convergence will unveil even more opportunities for innovation and efficiency. The businesses who are beginning to adopt these new technologies will be best prepared to thrive in the new digital age – but only if they get real when it comes to build vs. buy. ■



IT professionals skilling up for 2024

With the rapidly evolving IT space, the UK's enterprises are having a tough time sourcing the necessary skillsets to maintain operations efficiently and securely…

The last few years have seen monumental change throughout the IT world. Between the rise of remote/hybrid working required by the COVID-19 pandemic and the evolution of widespread use of machine learning (ML) and artificial intelligence (AI), the entire ecosystem has seen a fundamental shift – one requiring a whole new host of skills.

Both changes – arguably the biggest experienced with IT in a decade – have significantly increased the risk of cyber-attack. Keith Dube, director, solutions architect, product, Park Place Technologies, reports that "the single biggest change to in-demand skills in UK networking in 2024 is focus on security. The rise in cyber-attacks to access, modify or destroy sensitive data increases the need for professionals with experience in threat detection, network security and incident response."

Compounding the issue further, "the skills shortage in our sector spans across multiple disciplines and roles with competing demand both 'client side' and within the supply chain for the same people," says Jon Healy, COO at Keysource. "One of the key areas that this is negatively impacting is the ability for organisations to make informed decisions. Organisations are no longer confident in the quality of the information that is being provided - which in some cases is resulting in hesitancy in decision making and a greater level of governance being applied."

Accordingly, one question that we're seeing time and time again, is 'how will my business cope?'

Economically inactive

While the UK's unemployment rate has fallen to 3.8%, economic inactivity levels for 16–64-year-olds have risen by 100,000 in the last year alone. In a post-pandemic marketplace, fewer people are willing to take on undesirable/challenging work unnecessarily, while those closer to retirement age – many of them highly educated, well-paid and formerly in tech roles - have opted out in favour of leisure pursuits and time with loved ones following a lifetime of hard work.

I've seen firsthand that experienced, senior engineers and network operators are taking early retirement and are not being replaced due to a lack of qualified personnel.

Dube agrees: "with engineers retiring and a lack of incoming talent the current workforce may not be able to meet these demands. Cybersecurity in particular requires specialised knowledge and skills that may not have been a priority for network professionals in the past. There is a need for upskilling and reskilling of the existing workforce to bridge the skills gap."

"It is a challenging time for some organisations given the limited resource pool," concurs Healy. "One solution is to look at changing the way projects have been traditionally done with increased collaboration across the supply chain and learning from more mature sectors, particularly in relation to sustainability."

Given the scale of this challenge – one that is shared by most enterprises in the UK and abroad – solutions must be found, and fast.

"As an industry we have proven to be good at adapting and reinventing ourselves to cope with the fast-moving environment we operate in," asserts Healy. "But this approach would involve getting people to work together in a way they never have before and spending time to learn from those who have overcome similar challenges."

Soft vs tech skills

The employment environment in 2024 is a tricky place to be for enterprises – some 22% of workers are planning a move this year. With high rates of employee migration, in-house upskilling/retraining is being touted as one potential solution for gaining much-needed skills without having to endure the rigmarole of continual re-hiring.

Dube says that organisations must invest in continual up-skilling to keep pace with accelerating development: "in-house upskilling is an effective solution to address the rapidly evolving technological landscape, while retaining institutional knowledge and ensuring that the workforce is prepared to adapt to changes and meet the specific demands of the future."

However, Healy believes that while in-house upskilling may be one solution, "there isn't much time and this is a specialist industry, currently with little regulation, and so without the right people and the right advice now - there could be some very expensive mistakes being made."

Specifically within the data centre world, the Keysource 2023 state of the industry report finds that speed, substance, and sustainability are key considerations for success.

Reflecting on the survey, Healy reports that "nearly half of our respondents chose to sub-contract more projects or services than they had planned, echoing our experience that the industry is turning even more to supply chain partners or relationships to keep to programme timescales. According to the majority of our respondents, this approach had a positive impact including better quality and quicker delivery, with the inevitable trade off of a higher cost."

And it's not just technical skills threatening the UK's networking sector. According to the 'Essential Skills Tracker 2023,' a study of more than 2,000 workers showed that 51% had missed out on essential soft skills building opportunities and cost £22.2 billion annually.

"As technology becomes more integrated into various aspects of business soft skills, such as communication, teamwork, leadership, and emotional intelligence, complement technical skills and are necessary for success in the workplace," says Dube. "Soft and technical skills are both essential for individuals to thrive in a rapidly evolving technological environment."

Enter automation

The entry of AI into the networking arena has opened many possibilities for enterprises, from intelligently detecting increasingly sophisticated, and – critically – new forms of cyber-attack before the threat develops, to automating time-intensive tasks previously performed manually by human employees.

"We are starting to see AI, in some form, being used to take on time consuming administrative tasks," says Healy. "The hope is that this will free up time for senior executives to train the next generation of data centre professionals to support clients and help address the skills shortage. Moving forward, AI will play an even more significant role in predictive maintenance, anomaly detection, and network optimisation."

"Organisations remain focussed on improved operational efficiencies and customer experience through 'zero-touch automation' resulting in a significant impact on the workplace," adds Dube. "As AI and ML continue to advance, certain tasks and roles will be automated, leading to changes in job requirements and the need for new skills."

Indeed, Dube believes that job automation will include human intervention such as approvals before a task runs reducing routines from hours of monotonous tasks to a single-click freeing up human workers to focus on creative thinking; problem solving; and decision-making. "However, we are unlikely to see full automation - we are likely to see a sharing of skills, the machine assisting instead of replacing the human," concludes Dube. ■

John Healy

Keith Dube

IoT is an answer to the increase in damp and mould complaints, poor social housing conditions, and tenant health and safety concerns

Chris Jones, chief executive officer, Aico|HomeLINK

According to the Housing Ombudsman's Annual Complaints Review 2022–2023, the social housing sector has seen more than a four-fold increase in serious failures or delays by landlords over the last 12 months. The Ombudsman branded this a "sobering overview" of the situation across England after receiving over 5,000 complaints that were escalated for formal investigation; a 27% increase on the previous year and a record high.

The spike in complaints came as a result of poor property conditions (37%), health and safety complaints (52%) and bad handling of complaints (39%), all of which paint a picture of challenging social housing conditions.

Gaining a central view of all property conditions is essential to decrease tenant complaints and improve residents' health and safety. The simple step of implementing Internet of Things (IoT) sensors and connected home technology is emerging as an effective strategy for landlords (both public and private), to monitor the condition of properties. In implementing IoT smart home devices landlords bring a new level of efficiency to the management and monitoring of the health of their housing stock, while also improving the wellbeing of residents.

> "By installing environmental sensors in high-risk areas such as bathrooms, kitchens, bedrooms and living rooms, housing providers can measure factors contributing to damp and mould, such as temperature, humidity, and ventilation."

Property condition monitoring

There is an urgent need to understand and address the health risks of damp and mould in homes. Guidance issued by three UK Government departments aims to ensure every person in the country lives in a home that is safe, warm and dry. Recommendations for the report include the use of smart sensors to monitor the condition of properties.

Solutions which include a network of alarms and sensors offer social housing landlords access to a scalable and future-proof approach to their IoT strategy. A portal and connected devices provide the information those landlords value most, to optimise investment, identify and tackle fuel poverty, improve maintenance and deliver unrivalled service to all tenants.

Moreover, the UK government's endorsement of sensor technology as the best practice for damp and mould is echoed by other authorities. The Housing Ombudsman's follow-up report to its spotlight on damp and mould indicates a proactive shift in the social housing sector towards the adoption and integration of sensor systems, not just as a passive measure but as a proactive instrument for managing and resolving damp and mould challenges.

By installing environmental sensors in high-risk areas such as bathrooms, kitchens, bedrooms and living rooms, housing providers can measure factors contributing to damp and mould, such as temperature, humidity, and ventilation. These sensors also provide calculated insights into allergens and heat loss risk. These insights can be used by landlords to tackle issues such as disrepair and fuel poverty thereby enabling landlords to proactively address these issues before they escalate into larger complaints.

Preventative maintenance and other IoT benefits for landlords

Social housing providers will see a return on investment thanks to IoT technology identifying maintenance issues early and encouraging proactive measures for timely fixes. By analysing data to understand the health and safety of housing stock, landlords can identify properties most at risk of disrepair and step in when warning signs are detected. This is particularly relevant in addressing the challenges laid out by the Housing Ombudsman regarding delays and failures in managing housing conditions. Other benefits that IoT brings include improving maintenance and repair efforts, increasing efficiency and enhancing resident satisfaction, plus reducing operational costs and improving remote management.

Moreover, apps for residents are another innovative step in this direction. By providing residents with access to recommendations and advice, it empowers them to take an active role in the maintenance of their living conditions and home life safety. Equipping residents with the knowledge and advice they need can help in minimising issues such as fire risk, disrepair and fuel poverty; landlords will see improvements in the maintenance of their housing stock with less intervention. This can enhance the relationship between landlords and their tenants, and this proactive engagement helps to reduce the incidence and severity of damp and mould issues, in line with the Housing Ombudsman's emphasis on better tenant-landlord communication.

Protecting residents and housing stock without in-person checks

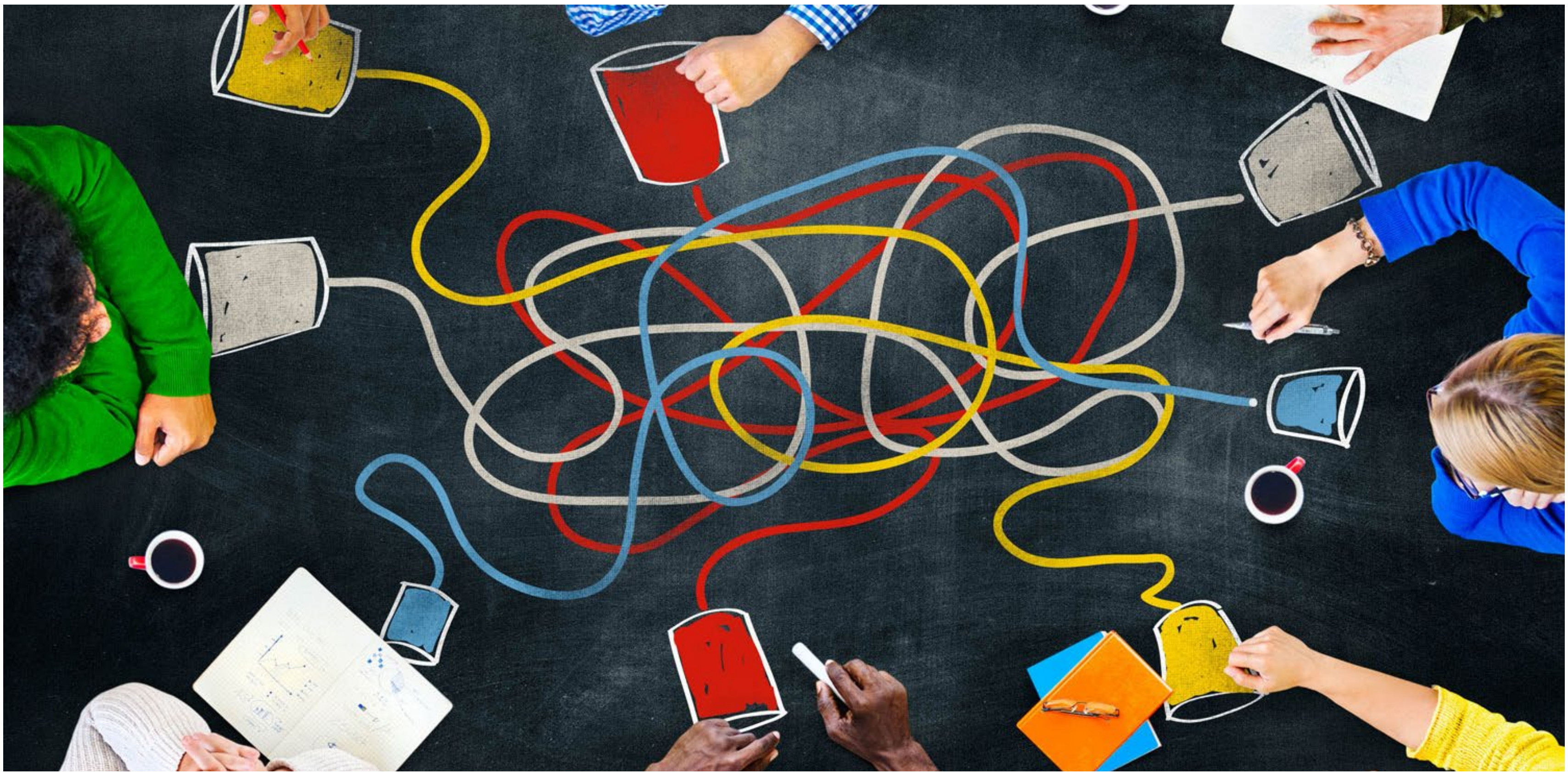
A connected home IoT-enabled portal facilitates remote management across an entire housing portfolio. Having direct centralised access to the relevant sensors' data, housing providers can understand where potential problems may occur and target the homes that need immediate attention, allocating resources where they are needed most to ensure residents' homes remain healthy. This proactive approach to asset management reduces the time and cost associated with reactive measures.

Remote management of a housing portfolio enables landlords to track the performance of their connected alarm system and indoor environmental conditions without performing in-person checks. All the information stored in one central location provides landlords with the full picture. This provides reassurance that residents are protected and that housing stock is fully compliant.

Having access to these in-depth reporting tools enables landlords to forecast alarm replacement and maintenance, helping to streamline maintenance, therefore, reducing call-out costs. When overcoming challenges related to accessing properties, language barriers, and communication gaps between landlords and residents, IoT technology always proves itself to be instrumental. It not only streamlines maintenance and reduces costs but also ensures complete compliance with housing regulations as they may change and any new legislation that is introduced.

Using IoT technology and connected home sensors can also help landlords monitor the occupancy of housing units to avoid overcrowding while regularly reviewing and sharing data in real-time for energy efficiency, temperature and humidity, ventilation, and smoke and indoor carbon levels.

There is a fundamental gap between some of the services landlords deliver and the expectations of their residents, so communication must always be a key factor. But, combined with open communication channels, integrating IoT solutions is a proactive way for housing providers and landlords to address damp and mould concerns, creating healthier and more comfortable living spaces for residents. ■



Connecting the classroom at Westwoodside school

Westwoodside Church of England Academy school is situated in the heart of the village of Westwoodside, Doncaster. Each member of staff works tirelessly to provide students with an exciting curriculum and learning environment, with ICT in every classroom to ensure children are prepared for the modern world.

Addressing the limitations

Having invested in front-of-class technology and mobile devices to help improve curriculum delivery, Westwoodside's wireless and network limitations needed addressing, and a planned for upgrade within the budgets available.

The school network infrastructure was a mixed estate, refreshed and replaced six years earlier. Like many schools, the pace of accelerated device procurement meant that the network was struggling with wireless coverage and capacity issues.

As a trusted Department for Education (DfE) framework provider, Primary Technology's infrastructure team were aware of the 'Connect the Classroom' programme – which was launched by the DfE with the aim of helping schools by providing grants to fund upgrades to enterprise wireless, switches and cat6 data cabling - and it was quickly identified that Westwoodside would be eligible for funding. As the schools managed IT support provider, Primary Technology discussed the eligibility criteria and helped the school complete the application process with the DfE.

Laying the groundwork

Primary Technology conducted a comprehensive technical survey and network audit that reviewed the existing data cabling, access points, switches, and network cabinets. This appraisal of the entire infrastructure was used to produce a future-proof solution suitable for the school for the next 10 years, one that was designed to meet the DfE's technology standards for switching and wireless.

Primary Technology supplied, installed, and configured enterprise-grade Meraki MS355 switches with a 10-year licence and support. The MS355 units are managed through an intuitive cloud-based interface, providing full 10G multi-gigabit (mGig) access switching for demanding enterprise and school environments. The cloud managed switches serve eight high performance Meraki MR46 wireless access points. This series of access points are designed for nextgeneration deployments in offices, schools, hospitals, and hotels, offering Multi-User MIMO technology to allow a larger capacity of connections at one time.

In addition to indoor coverage, an outdoor access point was installed with dual antennas to extend coverage beyond the school building and reach outdoor areas. A floor standing network cabinet was installed to house the new network hardware and this was connected with Cat6A cabling to maximise network performance.

Future-proofing across sites

One of the major benefits of Connect the Classroom is the ability for schools to improve wireless coverage across their sites.

Westwoodside has benefited by not only receiving fully funded enterprise-grade switching and wireless, but by having improved coverage and capacity in areas where WiFi was especially poor. The school now has the capacity to support their front-of-class technology and growing mobile device fleet, without any performance constraints.

The solution provides seamless access to a high speed, reliable wireless infrastructure with a peace of mind 10-year licence and support. The investment from the DfE to provide funded wireless will serve a positive purpose at Westwoodside, providing staff and students the best user experience and help them achieve their teaching and learning objectives.

"We had been planning to try and upgrade our wireless in the coming years, so it was fantastic to learn about the DfE funding that was available," said Carolyn Tuscher, business manager. "Primary Technology helped guide us through the whole process and completed the works to a very high standard. We are delighted with the end result. We now have great WiFi coverage, especially in areas where our old WiFi struggled due to the number of mobile devices we have in school." ■

Sheffield Hallam University secures networks

Sheffield Hallam University is one of the UK's largest and most diverse universities: a community of more than 35,000 students; 4,500 staff; and more than 295,000 alumni around the globe. Of those students, 53% are the first members of their family to attend university and 23% are from low-participation neighbourhoods.

The University standardised on Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) to safeguard its network some ten years previous. However, the education sector has become increasingly vulnerable to ransomware since then. Jisc's Cyber Impact Report 2022 reveals that UK institutions spend an average of £2 million on responding to ransomware attacks – and ransomware is now the sector's top cybersecurity risk, with more than 100 institutions falling victim since 2020.

"We have seen a 20-fold increase in ransomware since lockdown. We host highly sensitive student, administrative, and research data. We work collaboratively across the world. And people are operating 24/7, so cyber protection needs to be highly resilient, proactive, and continuous," said Dave Ainscow, head of cyber security at Sheffield Hallam University.

Scaling remote access

As the COVID-19 lockdown struck, the University's remote connectivity also needed attention.

"Almost overnight, we needed to scale remote access to 39,000 students and staff. Our Cisco VPN could do that but was expensive to operate and lacked the functionality to support a modern hybrid workplace," said Dave Ainscow, head of cyber security at Sheffield Hallam University.

Endpoint protection has also been a challenge: "the Sophos tool that protected our server estate required additional resources to manage exceptions. We also needed to extend EDR to support our new Azure estate," added Ainscow.

With these increasing challenges in scaling remote access, upgrading endpoint protection, and – perhaps most critically – protecting itself against ransomware attacks, it was time for the University to modernise its entire cybersecurity infrastructure.

The University's next-generation cybersecurity strategy would be required to: prevent cyberthreats across cloud, network, and endpoint devices; protect staff and students' personal information and IP; deliver flexible, policy-driven remote access experiences at scale; and accelerate the Zero Trust journey.

The University opted to extend its existing Palo Alto Networks network security solution into endpoint protection and remote working.

One unified portfolio comprising Palo Alto Networks ML-Powered NGFWs, Cortex XDR, and Panorama provides continuous 24/7 protection against both new and existing threats. Cortex XDR protects the University's 370 on-premises servers and Azure environment. It detects and responds across all data, regardless of origin or location. Complete visibility eliminates blind spots, while the management console offers end-to-end support for all Cortex XDR capabilities, including endpoint policy management, detection, investigation, and response. Remote working has been similarly transformed - GlobalProtect is the University's exclusive VPN solution, enabling secure remote working for up to 34,000 staff and students.

"The switch from Cisco during lockdown was a remarkable achievement. We had everyone live in less than two months," said Ainscow.

KHIPU Networks played a vital role in orchestrating this modernisation too: "KHIPU have been a long-term, trusted partner, providing higher education expertise, insight, and professionalism. Their engineers really understand our business too – they have become an extension of the University," added Ainscow.

In 2022, the University began using the KHIPU Networks Security Operations Centre (SOC) to provide 24/7/365 cyberthreat monitoring, detection, and response. The SOC uses the Palo Alto Networks Cortex XSOAR platform to accelerate security orchestration, automation, and response.

"Their SOC is staffed by cyber experts who are always available, their service integrates into our existing environment and doesn't just alert, it protects and prevents threats," said Dave Thornley, head of digital architecture at the University.

"We don't think there's any other solution on the market like Palo Alto Networks," opined Ainscow. "The integration, simplicity of interface, visibility, and reporting outpace anything offered by other vendors. By utilising our existing Palo Alto Networks NextGeneration Firewalls we are to extend their capabilities by using their portfolio alongside KHIPU Networks as a low-risk, fully interoperable single partner."

The benefits of this connected, agile cybersecurity portfolio include continuity of learning and research: despite the growing threat landscape – especially from ransomware – students and staff can connect, collaborate, and learn globally, confident that their data is protected and available.

Moreover, student and staff security has been enhanced further than ever before. The portfolio prevents cyberthreats across cloud, network, and endpoint devices while protecting personal information and IP. It also safeguards highly sensitive research and government data.

"Some people write risky PowerShell scripts. Cortex XDR identifies these among everything else so we can take action to close the threat," said Ainscow.

The new portfolio delivers modern, flexible, policy-driven remote access experiences at scale – across any user, any application, any device, and any network, fully supporting remote working and learning.

Efficiency has been increased too. Today, the University requires fewer resources to manage its IT estate, despite relentless growth in data, applications, and users. With the unified management of a single cybersecurity solution across servers and services, simple, integrated security is driven across cloud and SaaS workloads.

Palo Alto Networks and KHIPU Networks assess, protect, and manage the ever-increasing digital risks and threats posed to Sheffield Hallam University, ensuring staff, students, and partners are protected throughout their education. ■

Evolving critical national infrastructure

Duncan Swan, chief operating officer, British APCO

British APCO is a founding member of the Collaborative Coalition for International Public Safety (CC:IPS). The partnership is currently looking at where critical communication networks are designated as critical national infrastructure.

The world is marching ever quicker towards an all-digital infrastructure – and this brings with it challenges that break the norm. The solutions and underlying business processes delivering business continuity and disaster recovery no longer hold water, and different approaches must be considered. Simple challenges include the migration from copper landlines to voice over IP for all UK telephone connections, which was paused once it became apparent that during bad weather conditions, when power was lost, many customers had no way of making an emergency 999/112 call; and users of health alarms are unable to call for help. The onus on protecting the vulnerable has switched to ensure all utility providers take this responsibility. Next generation communications help drive improved processes and opens new communication channels – but when we take these steps, we need to ensure that we are not alienating those in society who are unable to embrace this level of change.

Here in the UK, the move some 20+ years ago from each emergency service organisation having its own self-provisioned analogue radio communications infrastructure to sharing a national digital infrastructure providing critical communications as a service was a huge step. A key element of the service was the business continuity elements, not all of which had been fully considered at initial deployment; fully duplicated switches that supported hot-standby mode; several hundred key sites that had generator back-up capable of lasting several days; and the ability to alternate route infrastructure interconnectivity in case of outage and/or failure. There's also off-network communications and the ability for nominated radio sites to act as a localised repeater in a major infrastructure outage, i.e. multiple layers of redundancy and fallback, and no need to consider this as part of – or relying upon – critical national infrastructure per se.

Fast forward and we are seeing a shift for the critical communication systems relied upon by our emergency services using commercial mobile network infrastructure to deliver next generation capability based upon 4G/5G – in particular radio sites, spectrum, and backhaul transmission networks which then feeds into a private, hardened, packet core network. This adds another obligation onto the network operators to ensure service availability – and move them ever closer to be classed as critical national infrastructure. So how do you justify the expense of protecting a significant subset of tens of thousands of radio sites and their corresponding transmission links?

In Australia they define critical national infrastructure as including 'those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.' In Canada they identify that 'disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.'

Then across the members of the EU, Directive 2022/2557 sets out how countries need to ensure the resilience of critical services, with 'critical infrastructure' defined as 'an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service.' In the same legislation, an essential service is 'a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment.' The importance some countries place on public safety communications can be seen in Germany and the Netherlands where 'communication with and between emergency services through the 112-emergency number and their emergency service mobile network falls under critical infrastructure.

Just a few days after the Optus network in Australia suffered an unplanned outage the Australian Minister for Home Affairs announced that 'telecommunications' will be recognised as 'critical infrastructure' – the Minister going on to say, "these rules, frankly, should have been in place years ago." This starts to recognise the level to which society has become ever more dependent upon communication networks. Here in the UK, it is well documented that during an outage to the 999-emergency communication system a total of more than 11,000 unique calls were unable to be connected through to the emergency operator for onward connection to the emergency services.

The whole fabric of society has digital communications interwoven with heightened expectations and huge societal dependency. As in Australia, we can expect to see telecommunications being categorised more widely as critical national infrastructure. And whilst critical communications will rarely be classed as critical national infrastructure, the networks and infrastructure upon which they are built will be, because of the adverse economic impact; the harm to public confidence in the establishment; and the potential for significant loss of life with any prolonged unavailability.

Australia has taken the lead; let's hope the UK is not slow to follow. ■

PRESENTED BY:
TCCA
TCCA
CRITICAL COMMUNICATIONS WORLD 2024
ENTER THE GLOBAL NETWORKING HUB
REGISTER YOUR INTEREST
14-16 MAY 2024
DUBAI WORLD TRADE CENTRE, DUBAI, UNITED ARAB EMIRATES
WWW.CRITICAL-COMMUNICATIONS-WORLD.COM
@CritCommsSeries
TCCA Critical Communications World
PLATINUM SPONSOR
MOTOROLA SOLUTIONS
GOLD SPONSORS
ERICSSON

UPS – let's make it modular

Stuart Dealing, sales, service and project execution leader, ABB Power Protection

When choosing a power protection scheme for a data centre, the first thing to consider is the total cost of ownership (TCO).

Operators typically want a 20-year lifetime for a UPS nowadays. So, investing in a more energy efficient model will result in significant overall cost and emissions savings, especially with energy prices surging. Similarly, specifying a UPS with better quality components, that only need replacing once rather than two or three times over the lifetime of the UPS, drastically reduces TCO.

Some data centres still rely on traditional monolithic UPS configurations – where all the components are built into individual blocks. So, the capacity cannot be adjusted without replacing the entire system or adding another UPS.

Alternatively, a modular UPS consists of multiple smaller, swappable, autonomous modules that work together within a single frame. For example, a 1MW modular UPS can be built from four parallel 250kW modules.

While the upfront cost of a monolithic UPS is often lower than a modular one of the same capacity, the TCO and availability benefits of going modular almost always outweigh a monolithic setup.

This is because modular UPS have more in-built redundancy. Operators can simply specify an additional module rather than an entire monolithic UPS block. For example, to achieve redundancy on a 1MW capacity data centre, you can save 30% costs by specifying a 1.5MW modular UPS frame to achieve N+2 redundancy compared with N+N from two 1MW monolithic blocks. This can also produce a lighter UPS system that can more easily be installed on the raised floors or building's roof, for example.

In addition, a modular setup reduces the need for additional power equipment, like cables and switchgear. In the above case, two parallel monolithic UPSs would have two input switches and two output switches, where a modular setup would only have one on the input and one on the output.

Furthermore, modular UPS systems are more energy efficient. For example, if load demand is low, modern modular setups can automatically switch modules to sleep or economy mode to reduce energy consumption.

Operators managing 30+MW data centres are deploying medium-voltage (MV) equipment. The most obvious advantage of an MV UPS is that it offers lower TCO for several reasons.

Since the MV structures are able to cater for hundreds of megawatts, alternative power protection schemes for the entire facility can be proposed with ease, leading to lower capital expenditure.

The lower currents at the MV level enable smaller cable sizes, in turn reducing installation costs and space, allowing for the UPS to be placed further away from the load and maximize the given land plot.

Switching to MV also lowers overall footprint compared to using multiple LV UPS. Not just because of the size of the UPS itself, but also because less electrical equipment is required in the energy centre. Not only is it easier to maintain fewer UPS, but it also frees up space for server racks, maximizing available revenue from the same footprint. Since an MV system can handle the UPS function of the whole data centre, rather than selected server racks, it can often sit nearer the grid connection rather than in the server room. This saves more space and protects the entire facility through resilient architectures, such as distributed redundant and similar.

They are also more energy efficient than LV UPS as they suffer lower electrical losses because they run at lower currents. Compared to a rotary UPS, an MV UPS can save up to 4.2GWh of energy. This is equivalent to 1,245 tonnes of CO2 emissions over a 15-year lifetime.

According to the Uptime Institute's Annual Outages Analysis 2023, 70% of events causing data centre downtime cost $100,000 or more, with 25% costing more than $1 million. With downtime costs this high, operators are looking for ways to ensure data continuity and reliability.

Remote monitoring supports this through a proactive approach to maintenance that means UPS issues can be addressed before they result in faults or downtime, heavily reducing TCO.

Moreover, remote monitoring avoids unnecessary emergency site visits from service professionals – reducing costs and the carbon emissions associated with their travel. In fact, it's possible to troubleshoot UPS alarms remotely without the need for a call-out, which is especially valuable for more inaccessible data centres.

Data centres often hold very sensitive data, in which case, operators can opt for a remote monitoring system with one-way communication coming from the UPS, with no signals or commands going back to the UPS – it's more of a 'read-only' connection that doesn't allow for remote access but provides alarms.

The most important priorities when specifying a UPS are efficiency, footprint, and weight - modular and MV solutions meet all these criteria. With these strategies, data centres will significantly reduce their overall costs, minimize the risk of outages, and gear themselves for future growth. ■

PRODUCTS

Kohler Uninterruptible Power (KUP) has announced the launch of a new model in its highly successful KOHLER MF series – the MF 2000DPA-CSB. The CSB designation refers to a pioneering, removeable, dual-feed Centralised Static Bypass featuring patented load balancing technology. This enables a 97.4% VFI energy efficiency and compact footprint of the KOHLER MF Series to be maintained, while built-in redundancy ensures the resilience of the decentralised parallel architecture (DPA) modules is also retained.

Offering flexible, scalable power of 1500–4500kw, the CSB variant uses hot-swappable 250kw modules like the rest of the MF Series, though it also adds a hot-swappable centralised bypass switch. This in itself uses unique parallel matrix technology to provide load balancing and redundancy.

The slide-in design of the modules and CSB greatly speeds installation and maintenance whilst also significantly reducing physical footprint. Compatible with a range of battery technologies including VRLA, lithium-ion and nickel-zinc, the MF Series also allows users to choose a battery system that matches their load, budget, and facility size.

Additionally, the KOHLER MF 2000DPA-CSB has optional electrical grid interaction functionality, supporting the adoption of renewable energy sources into the national power infrastructure.

The **Mitsubishi Electric 9900D UPS** was designed with data centres in mind.

It delivers high power density with 2/3 the footprint of competitive units; high-speed sampling and switching; higher operating temperatures at higher altitudes; expandable UPS via modular design; advanced IGBTs for increased reliability; new HMI for easier user interface; and Lithium Ion, VRLA, and pure lead compatible for greater flexibility.

The 9900D features a self-load test mode of operation, providing the ability to run burn-in tests on the UPS without needing an external load bank connected. Running a burn-in utilising the self-load test realises savings from removing the need to rent a load bank and cables, the set up and removal labour, and reducing utility power usage.

The robust technology is designed to deliver continuous power in the most demanding environments, with a sustained load carrying capacity of 99.9995% of actual operational history.

Moreover, its modular design enables supplemental modules to be added over time as warranted by increasing capacity needs, making hyperscale expansion faster, easier, and more economical.

EnerSys' Alpha FXM HP is the next generation of rugged UPS power modules for the most demanding environments where clean backup power is needed.

It offers a user-friendly interface for improved operational performance and integrity. FXM HP is designed to operate in extreme environments for reliability and maximum flexibility. While ensuring equipment remains protected from power disturbances and outages, FXM HP UPS provides centralized setup, control, and monitoring.

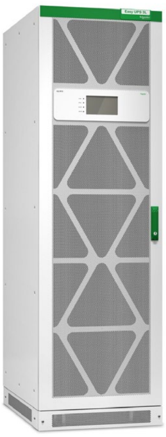
The FXM HP brings increased processor horsepower, advanced security, and configurability to the proven FXM outdoor family. An LCD touchscreen display provides access to multiple configurable tabs for quick system status, overview, and configuration without the need of a laptop. Moreover, FXM HP includes multiple communication ports to permit simultaneous local craft access as well as permanent LAN/WAN connectivity.

Environmental conditions and other equipment can be monitored via CAN port, while enhanced security using modern encryption technology ensures proper authentication and privacy for remote connection with the UPS.

The **Schneider Electric Easy UPS 3L** is an easy-to-configure, easy-to-use, and easy-to-service 250-600kVA (400V) 3-phase UPS that delivers high availability and predictability to medium and large commercial buildings and light industrial applications.

Its fault-tolerant design streamlines installation and service, while its compact footprint saves valuable real estate. With up to 96% efficiency, the Easy UPS 3L delivers predictability for utility costs.

The design is a fault-tolerant architecture. If a power block becomes inoperable, the load will continue to be supported by the remaining power blocks, provided that the load is below the capacity of the functional power blocks in the system. The enterprise can install up to 5 UPSs in parallel for capacity, and can increase availability by installing two isolated busses (UPSs) to receive power from two independent power sources. The UPSs are synchronized automatically, making installation and set-up easy and resilient.



According to **Centiel**, its CumulusPower UPS range offers the highest levels of availability and the lowest total cost of ownership (TCO), while being designed with flexibility for future growth in mind.

The CumulusPower portfolio features fault-tolerant, three-phase, true modular UPS-systems combining a unique Intelligent Module Technology (IMT), with a fault-tolerant parallel architecture, Distributed Active-Redundant Architecture (DARA).

The portfolio of frame sizes range from 20-600kW and comprise modules with power of 10, 20, 25, 50 and 60kW. Systems are parallelable up to 3.6MW. The range of UPS boast 99.4% efficiency in Eco-mode operation, as well as 'nine nines' 99.9999999% availability.

“Please meet...

Gordon Cullum, technology director, Axiologik

Who was your hero when you were growing up?

Sir Michael Palin. Not only do I love Python humour, but when I was 12 he did ‘Around the World in 80 Days.’ I wasn’t allowed to stay up late enough on a school night to watch it, so it was the highlight of my week when my mum recorded that from the telly, and I got to watch it the next day. Exploration, creativity, adventure, problem-solving. All things that have inspired me forever since.

What was your big career break?

I’m not sure I’ve ever really had ‘a break’ as such. There have been a couple of steep inclines in my progression. My first was way back at Syntegra. I was working in technical support and I was assigned a mentor, Rob Clayton. He recognised that I was more interested in design and development, but had a grounding in ‘what not to build’ coming from having to get out of bed at 1am regularly and fix problems caused by other people’s deliveries.

He got me seconded to a delivery team building the London Eye’s ecommerce website. He pushed me hard to learn new skills and integrate with that team, so much so that when the team bid for a rebuild of all of the London Eye’s systems (tills, reporting, access control, website) I was named as the solution architect. That was a big step in responsibility for me, and whilst it was hard work and a big ask, I worked with a great team and we all learned and grew so much in so short a time.

Rob is no longer with us, but I think of him often and am so grateful for having had such a great role model.

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

A fast jet pilot in the RAF. Partly because I wanted to travel the world, partly because I love complicated machines and partly because I love speed. Sadly, I was told by a recruiter for the officer training programme when I was 16 that I would never fly because of my eyesight.

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

I’m lucky in this question in that the person I admired while growing up is still alive, so I’ll say Sir Michael Palin. I think it would be a riot of tall tales, humour and learning about the world that he has explored. He comes across as such a genuine person, too, so I would like to think that he might enjoy talking with me about some of my, albeit less impressive, experiences.

What’s the best piece of advice you’ve been given?

Get a mentor – someone who can help you understand where you need to grow based on who you really are, what you want to be and why. Not just someone who’s interested in you from a professional excellence point-of-view, but someone who can see past your immediate ‘use’ and help you become the person you want to be.

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

Given I can’t fly fast jets for the RAF, motorsports! One way or another – either involved in a team, driving, leading, or being in some way linked to that excitement. I had the pleasure of visiting the Mclaren Technology Centre a few years ago and the way that that whole organisation comes together behind the mission and everyone is excited about the part they play was amazing.

The Rolling Stones or the Beatles?

The Beatles and it’s a simple reason - I grew up with the Beatles. When I was in a band we covered loads of Beatles songs. Their music evolved so much over the years but remained accessible. Almost anyone can sing their songs, pick up a guitar and play their songs, yet to have created such masterpieces in the first place totally belies that simplicity and accessibility.

What’s the greatest technological advancement in your lifetime?

In my view, the thing that’s had the most impact is the internet. Or, more specifically the World Wide Web. Whilst the internet is the technical enabler, the World Wide Web is the great leveller that has created a step change in the learning ability of the world.

I do recognise that there are, of course, still parts of the global community that don’t have the same levels of access to it. Often these communities are closer to home than we in the developed world think. Simplifying and extending access to the web is probably one of the most powerful things we can continue to do to drive our planet forward.

What would you do with £1 million?

I probably should do something like pay off the mortgage, and invest it for my boys’ future. In reality, I’m not much of a personal planner so I’d probably spend it on an assortment of holidays for me and my boys, cool gadgets and probably a Ferrari. ■ ”