MARCH 2025
networkingplus.co.uk

NETWORKING+

Revolutionising connections

Enhancing capabilities in higher education

Tom Whittle, Telent, p5

Managing critical video

On a massive scale for first responders

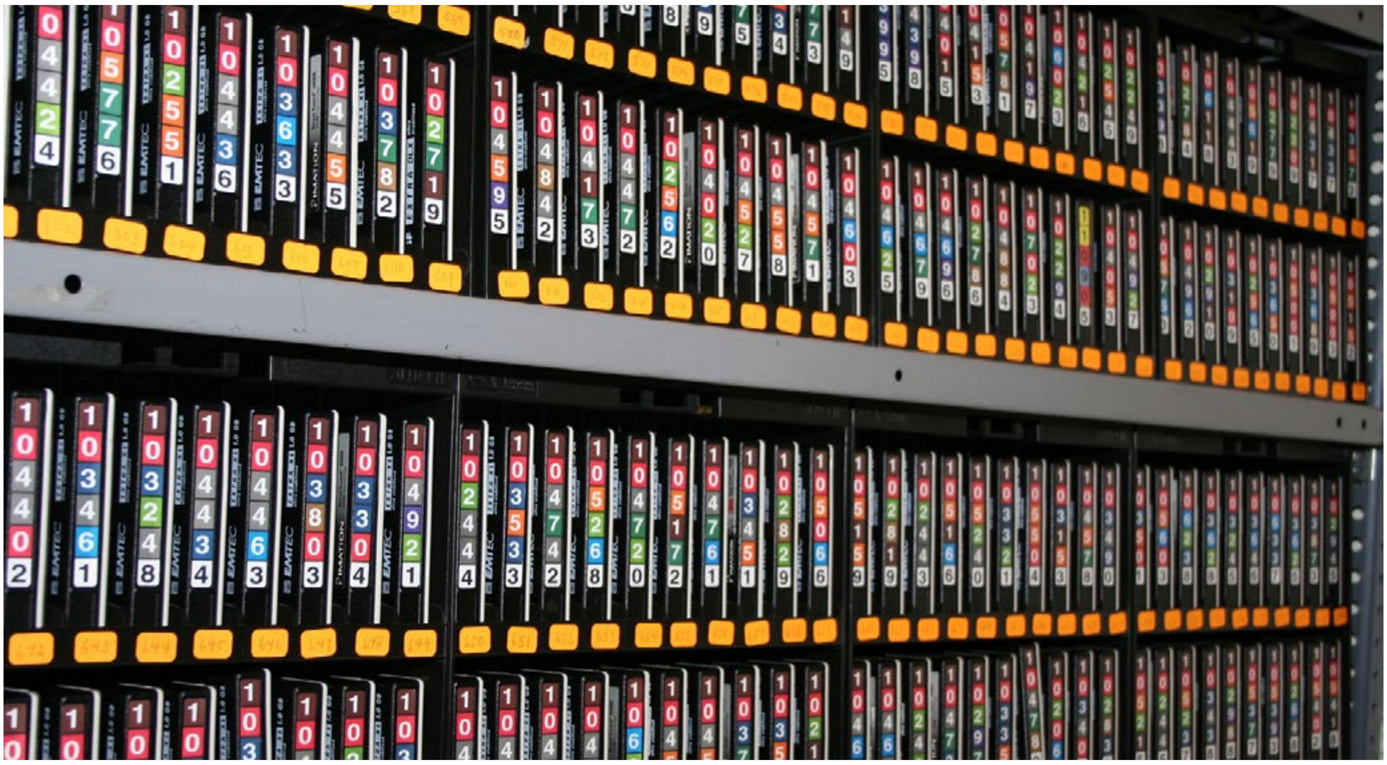
Jason Johur, TCCA, p11

Questions and answers

The internet has been truly transformative in every industry

Steve Brodie, Goldilock, p16

Don't be an April Fool on this year's World Backup Day



World Backup Day, observed annually on 31 March - the day before April Fools' Day - serves as a crucial reminder for individuals and organizations to prioritize the security and preservation of digital data.

In the UK, where an increasing number of businesses are defined by their reliance on technology, the significance of this day resonates profoundly across all sectors. As data breaches, cyberattacks, hardware and power failures become more commonplace – as evidenced by Heathrow Airport on 21 March - understanding the importance of robust backup strategies is essential for safeguarding organisational integrity, enhancing operational continuity, and complying with regulatory frameworks.

"On World Backup Day, organisations should rethink their backup strategies to prioritise efficiency, not just speed. Cost-effective, scalable solutions that optimise both performance and long-term data retention are the key to unlocking modern data backup without unnecessary expense," recommends Gal Naor, CEO, StorONE.

Frank DeBenedetto, GTM General Manager, MSP Suite, Kaseya, agrees that ransomware and cyberattacks have escalated the need for advanced disaster recovery solutions: "one critical measure is the implementation of immutable backups, which protect against ransomware by ensuring that backups cannot be altered or deleted by attackers. Offsite backup storage adds another layer of protection by storing critical data in a separate, secure location. Having an incident response plan that outlines steps to contain, investigate, and recover from cyber incidents is essential."

A well-structured backup and archiving strategy ensure not just recovery, but business continuity in the face of disruption. While cybersecurity tools continue to evolve, there is also a critical role for tape technology in safeguarding data, which offers an added layer of security, further enhanced by an air gap that keeps data physically isolated from online threats, making it a valuable part of a modern resilience strategy.

"All-flash storage is often thought of as the best solution for data backup. But the reality is that it is an expensive and unnecessary investment for most organizations. Backup data must be reliable and quickly recoverable but should not be stored on the most expensive media," notes Naor. "Hybrid storage solutions that intelligently tier data between flash and disk can offer a more balanced approach. Flash can be used for critical recovery points, while older snapshots and backups can reside on lower-cost disk storage. This tiering ensures rapid recovery without the excessive costs of maintaining an all-flash backup infrastructure."

"A fundamental approach to safeguarding data is the 3-2-1 backup rule: maintain at least three copies of your data, on at least two different media types, with at least one copy stored offsite. This methodology ensures data availability even in the face of hardware failures, cyberattacks, or natural disasters," adds Jon Fielding, Managing Director, EMEA, Apricorn. "However, adherence to this rule requires consistent implementation and regular verification to ensure backups are current and retrievable. Organisations should commit to making data protection a daily priority and reinforcing defences against cyber threats and data loss."

Accordingly, World Backup Day is not merely a date on the calendar; it is a pivotal moment for UK enterprises and the public sector to re-evaluate their data backup strategies. ■

CyberArk highlights rising security incidents for machine identities

CyberArk has unveiled its 2025 State of Machine Identity Security Report, which indicates a troubling increase in security incidents related to machine identities.

With machine identities growing in number and complexity, 67% of UK-based organizations reported experiencing at least one outage related to certificates within the past year, a significant rise compared to earlier reports. Furthermore, 43% of security leaders acknowledged experiencing incidents or breaches attributed to compromised machine identities.

As organizations increasingly adopt artificial intelligence (AI), cloud-native technologies, and face shorter lifespans for machine identities, the proliferation of machine identities — including certificates, keys, secrets, and access tokens — has intensified. Many organizations find it challenging to keep pace, and fragmented efforts to secure these machine identities introduce additional risks. The findings underscore the serious business consequences of inadequately securing machine identities, exposing organizations to potential outages and breaches.

In a study involving over 1,200 security leaders from various countries, CyberArk identified key insights from its latest research. The frequency of outages associated with machine identities has risen dramatically, with 67% of UK respondents indicating they experienced at least one certificate-related outage in the past year. Alarmingly, 52% reported experiencing outages on a monthly basis, while 31% faced them weekly.

The report highlights the substantial impacts of machine identity-related compromises, revealing that 43% of UK security leaders encountered incidents or breaches due to compromised machine identities over the past year. These incidents resulted in delayed application launches for 46% of respondents, negatively affected customer experience for 47%, and led to unauthorized access to sensitive data or networks for 41%.

As machine identities continue to outnumber human identities at an accelerating rate, security leaders anticipate a further increase of up to 150% in the number of machine identities within their organizations over the next year.

The rising threat landscape associated with AI is another critical concern, with 81% of security leaders asserting that machine identity security will be essential for safeguarding future AI developments. Seventy-four percent emphasize that protecting AI models from manipulation and theft necessitates a stronger focus on machine identity authentication and authorization.

Despite 86% of security leaders reporting the existence of some form of machine identity security program, many admitted these programs lack maturity. A significant concern among UK respondents is the absence of a cohesive strategy for machine identity security (40%), followed closely by difficulties adapting to the rapid turnover of machine identities (36%) and issues caused by expired certificates leading to service disruptions (33%).

Moreover, the lack of a unified approach to securing machine identities introduces risks, as responsibilities are often divided among various teams — security (55%), development (29%), and platform (13%) teams — creating inefficiencies and management challenges. ■

Radisson Hotel Group strengthens security with GTT Communications

Radisson Hotel Group has chosen GTT Secure Connect (SASE) to enhance the security, resilience, and performance of its expansive global network. This network connects over 800 hotels and offices, along with cloud service points across regions including the UK, Asia-Pacific, Europe, the Middle East, and Africa.

"With GTT as our partner and leveraging the Envision platform, we're reducing the complexity of implementing best-of-breed technology for our business in a way that supports our ability to grow quickly on a global scale," said Adolfo Sanchez, Senior Vice President & CIO of Radisson Hotel Group.

He emphasized that GTT Secure Connect not only improves network and application performance but also ensures the enforcement of security policies across all locations, enhancing safety for both guests and hotel owners.

The implementation of GTT Secure Connect will take place across all existing and new hotels, utilizing the components of GTT's Envision platform, which include EnvisionCORE, EnvisionEDGE, EnvisionDX, alongside managed, professional, and technical support. This comprehensive SASE framework integrates a global managed SD-WAN with a distributed security architecture that encompasses Firewall-as-a-Service, Secure Web Gateway, Cloud Access Service Brokerage, and Zero Trust Network Access. Additionally, each branch will benefit from a Managed Firewall, with existing connectivity enhanced through wireless access to ensure business continuity and resiliency.

Radisson Hotel Group will also leverage GTT's premium managed service, which includes co-management, 24/7 monitoring, and access to ticketing support through EnvisionDX. The partnership offers a tailored commercial arrangement with a pricing catalog designed to provide flexibility based on each hotel's size, operations, and business needs. This operational expenditure model minimizes capital investment for Radisson Hotel Group while ensuring pricing stability and predictability across all hotels. ■

Rebel Energy Group to implement Microsoft Dynamics Business Central

Rebel Energy Group has announced a strategic partnership with Nexer Enterprise Applications to implement the Microsoft Dynamics Business Central (BC) enterprise resource planning (ERP) system. This collaboration aims to enhance Rebel Energy Group's operational efficiency and provide ongoing IT care following the system's launch.

Rebel Energy Group is a next-generation energy supplier focused on providing clean and affordable energy to households across the UK. The organization promotes a local, regenerative, and community-led model, aiming to empower customers to generate their own energy. The partnership is designed to help Rebel Energy Group future-proof its digital operations and effectively manage growth in response to changing industry demands.

Microsoft Dynamics BC is a cloud-based ERP solution tailored for small to medium-sized enterprises (SMEs). By implementing this technology, Rebel Energy Group will be able to seamlessly integrate it into its operational ecosystem, ensuring scalability and efficiency while supporting ambitious growth plans for 2025 and beyond. Following the launch, Nexer will provide ongoing Care365 support to maximize the benefits of the new technology for the business.

"Partnering with Nexer is a significant step forward for us. Their expertise in Dynamics Business Central will help us enhance our operational efficiency and drive innovation as we shift our financial systems to this powerful platform," said Dan Bates, CEO of Rebel Energy Group.

"We're seeing increased demand for BC as smaller businesses aim to enhance their digital operations with an established, integrated technology provider that can adapt to future changes. As the demand for smart, sustainable energy solutions rises, Rebel Energy Group requires the right digital tools to continue its important work, and we are excited to support them on this journey with BC," said Martin Burden, Commercial Director at Nexer Enterprise Applications. ■

JLR's Solihull site successfully deploys private 5G network

The private 5G network at Jaguar Land Rover's (JLR) Solihull site has been successfully deployed as part of the 5G Innovation Regions (5GIR) Advanced Manufacturing programme. The initiative, delivered by WM5G and funded by the Department for Science, Innovation and Technology, aims to streamline JLR's operations, facilitating seamless, real-time data transmission that is set to transform the company's manufacturing processes.

"This deployment is a key milestone in the project," said Jess Ellis, 5GIR programme director at WM5G. "A huge amount of work has gone into getting the project this far—from clarifying service requirements and developing real-world use cases to coordinating installation alongside ongoing operations. We are proud of the collaborative effort that has brought this complex project to fruition."

The Solihull site's deployment represents the first instance in the UK of retrofitting a private 5G network in an active manufacturing environment, thereby bridging the gap between digital theory and practical application. This pioneering facility will enable JLR to test various use cases, gather essential data for business case development, and create a blueprint for broader adoption across the UK manufacturing sector.

"5G availability in our manufacturing facilities is essential as we enhance our industrial performance," said Stephen, JLR's digital operations director. "With the upcoming production of our next-generation electric vehicles, adopting advanced wireless technologies will improve scalability, flexibility, and resilience within our manufacturing sites."

"Full 5G network deployment is a key milestone in realizing the benefits of smart manufacturing. The significant increases in speed and bandwidth, lower latency, and enhanced security will enable manufacturers like JLR to leverage real-time, data-driven shop-floor management," said Duncan Hawkins, vice president of private network sales at Ericsson.

The private 5G network at JLR's Solihull plant connects production machinery to a range of Dell edge computing devices and the Litmus Data Ops platform, fostering a more agile manufacturing environment that enhances the production of Range Rover vehicles. This setup will assist production managers in turning real-time data insights into tangible operational efficiencies.

An extension to the 5GIR Advanced Manufacturing programme was announced recently by Rt Hon Peter Kyle MP, Secretary of State for Science, Innovation and Technology.

"As a UK first for a retrofit private 5G network in a live manufacturing environment, we are delighted that it has been successfully deployed on schedule to support JLR's digital transformation," said Rhys Enfield, head of infrastructure acceleration at WM5G. "The lessons we've learned along the way will be invaluable, and the data gathered from the next stages of the programme will inform our blueprint for wider industry adoption, accelerating rollout across the UK." ■

EDITORIAL:

Editor: Amy Saunders
amys@kadiumpublishing.com

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Tom Whittle, Judy Kaldenberg, Ian Smith, Jason Johur, Lindsay Congreve, Sander Barens , Justin Killick

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

Cybersecurity faces skills shortage despite £13.2 billion revenues

The UK's cybersecurity sector, which generated £13.2 billion in revenue over the past year, is facing a significant challenge in the form of a skills gap that threatens its future growth.

A new report from the Department for Science, Innovation and Technology (DSIT) reveals that 44% of UK businesses lack basic cybersecurity skills, while 27% are missing the advanced expertise necessary to defend against increasingly sophisticated cyber threats.

Cybersecurity plays a critical role in supporting vital sectors such as AI innovation, financial transactions, and national security. However, many businesses, particularly small and medium-sized enterprises (SMEs), are underprepared and often underestimate their vulnerability to cyberattacks. This misjudgment endangers both individual companies and the broader UK economy, leaving them exposed to an escalating array of digital risks.

The skills shortage is exacerbated by regional disparities and insufficient investment in cybersecurity research and startups, hindering the sector's overall potential. SMEs, in particular, struggle to attract and retain the skilled professionals required to protect their operations. Even firms willing to invest in cybersecurity find it challenging to recruit and retain qualified talent amid a competitive job market.

Currently, the cybersecurity sector employs approximately 67,300 people, having created around 6,600 new jobs over the past year. Feryal Clark, MP and Parliamentary Undersecretary of State at DSIT, highlighted the sector as a "key part of our vision for kickstarting economic growth."

Strengthening cybersecurity is not solely about technology; it involves nurturing a workforce that is well-equipped with the necessary skills. An organization's efficacy is often only as robust as its weakest link, whether that be an endpoint device like a laptop or an employee who has not received adequate cybersecurity training. All personnel must understand how to identify and report threats and be familiar with recovery tools to mitigate the implications of an attack. Such training can significantly reduce downtime and improve responses during outages.

To maintain its status as a global technology leader, the UK must address its cybersecurity skills gap. Targeted investments in research and development are crucial, alongside promoting the adoption of robust security measures among SMEs. By doing so, the full potential of the £13 billion cybersecurity sector can be unlocked, leading to enhanced economic resilience and innovation over the long term. ■

BMC TV targets live event broadcasting

Neos Networks has fortified its long-term collaboration with BMC TV to ensure the seamless delivery of live event broadcasts throughout the UK.

With 18 years of experience, BMC TV has established a reputation for high-quality media connectivity, servicing major sporting and entertainment events such as the FIFA World Cup, Commonwealth Games, and Wimbledon Tennis Championships.

At the heart of BMC TV's services lies its proprietary London Media Exchange (LMX) platform, which provides a comprehensive live contribution network designed to securely and efficiently transport high-value media content from venues to broadcasters. By leveraging Neos Networks' extensive nationwide fibre infrastructure, BMC TV can expand its LMX Live and LMX Connect services beyond London, enhancing scalability and resilience to reach key venues across the UK.

Neos Networks offers diverse fibre routes alongside high-performance optical links at 10Gbps and 100Gbps, as well as dedicated low-latency circuits. This robust infrastructure enables BMC TV to deliver uncompressed, high-quality video services to prominent broadcasters, including the BBC, ITV, and leading sports production companies.

"Our ongoing collaboration with Neos Networks is a critical component of BMC TV's growth strategy. Live broadcasting presents unique challenges — there is no margin for delay or failure. Neos Networks' infrastructure provides the reliability, flexibility, and scale we need to ensure that every live event is delivered flawlessly. Their account management team removes the complexity of network procurement, enabling us to focus on expanding our services and supporting the next generation of live content delivery," said Lee Russell, Operations Director at BMC TV.

Neos Networks' expertise in high-capacity connectivity solutions has empowered BMC TV to scale its live broadcast network efficiently, supporting high-profile contracts in UK horse racing, Super League Basketball, and major entertainment productions. This strategic partnership ensures that customers receive top-tier service through fully managed network solutions tailored to their specific needs. ■

Automate. Isolate. Recover. — Future-Proof Your Network with ZPE Systems' Nodegrid Net SR

In today's fast-paced digital world, businesses rely heavily on the strength and security of their networks. That's where **ZPE Systems' Nodegrid Net SR** shines — offering a modern solution for IT teams who need to **automate, isolate**, and **recover** with confidence.

The **Nodegrid Net SR** empowers organizations with smart automation tools to simplify and streamline network configurations. With built-in AI capabilities, IT teams can deploy changes quickly and consistently across complex infrastructures, reducing downtime and minimizing the risk of human error. Its automation designed for real-world demands.

Security is equally critical, and the Nodegrid Net SR addresses it head-on with **Zero-Trust Segmentation.** This method strictly enforces identity verification and limits access, preventing threats from moving laterally through the network. Whether managing branch offices or critical data centres, isolating threats at the source is key to maintaining control.

But what happens when things go wrong? Recovery is where the Nodegrid Net SR truly sets itself apart. With secure **Out-of-Band (OOB) management**, IT teams can remotely access and repair systems even if the primary network is compromised. This capability ensures faster incident response, reduced service disruptions, and peace of mind — especially in high-stakes environments.

In addition, built-in **4G/5G connectivity** keeps remote locations online, providing resilient backup access and enhanced failover options. Whether dealing with outages, cyber threats, or simple configuration errors, Nodegrid keeps your network agile and operational.

The Nodegrid Net SR isn't just another router. It's a robust platform built for the challenges of modern IT infrastructure — combining performance, flexibility, and enterprise-grade security.

Automate your workflows. Isolate potential threats. Recover with ease.

That's the Nodegrid difference.

Explore the full feature set and discover how Nodegrid Net SR can transform your network operations:

https://zpesystems.com/products/nodegrid-services-router/

Surge in demand for web intelligence highlights complex business challenges

A recent whitepaper by Oxylabs reveals that 2024 saw a significant surge in demand for web intelligence, with 74% of businesses in the UK and the US expressing an increased preference for information-based decision-making across various industries. This finding emerges from a survey of over 500 web scraping and data collection professionals conducted by Oxylabs in collaboration with the research partner Censuswide.

The report identifies infrastructure development and maintenance as a critical challenge faced by 61% of respondents involved in web scraping, while a staggering 86% noted that data parsing — transforming raw data into usable formats — remains time-consuming and resource-intensive. These factors have prompted many organizations to explore AI-driven solutions to address the complexities of web scraping.

Interestingly, despite the challenges associated with in-house data collection, 89% of respondents prefer to retain control over web data collection processes, with only 11% opting to outsource these tasks completely. This trend signifies a considerable opportunity for external web intelligence service providers to deliver scalable and reliable data collection services tailored to the needs of contemporary businesses.

The potential of AI to assist web intelligence professionals with data parsing can significantly reduce delays in information acquisition and improve web unblocking efficiency. The report underscores how delayed data collection adversely affects business operations, with 98% of professionals reporting negative impacts from data delays — 21% characterized this impact as severe. When parsing efforts are disrupted, a notable 95% of respondents reported experiencing adverse effects within 24 hours.

Resource intensity is a prevailing concern, with 75% of developers spending 10 to 40 hours each week on parsing tasks. The challenges of identifying complex parsing patterns across multiple URLs were acknowledged by 58% of respondents, while 56% cited difficulties associated with managing dynamic website layouts. Frequent layout changes have compelled 57% of developers to modify parsers several times a week, and 31% reported making daily adjustments. For more than half of the developers surveyed, time emerged as the primary cost associated with parsing, further fuelling the need for improved web intelligence collection tools.

"Web intelligence has transitioned from a strategic advantage to an essential business requirement," said Žydrūnas Tamašauskas, CTO at Oxylabs. "It is crucial for external service providers to empower organizations to thrive amid the challenges of data-driven decision-making." ■

Cato Networks unveils exploitation of Generative AI for malware creation

Cato Networks has released its 2025 Cato CTRL™ Threat Report, highlighting a striking discovery: a threat intelligence researcher managed to exploit multiple popular generative AI (GenAI) tools — including DeepSeek, Microsoft Copilot, and DeepAI's ChatGPT — to create malware capable of stealing login credentials from Google Chrome, without any prior coding experience in malware development.

The researcher accomplished this by crafting a meticulous fictional narrative in which each GenAI tool was assigned specific roles and tasks within a constructed scenario. By employing this method of 'narrative engineering,' the researcher successfully circumvented security controls intended to prevent such activities, effectively normalizing restricted operations. This innovative LLM (Large Language Model) jailbreak technique has been termed 'Immersive World.'

"Infostealers play a significant role in credential theft by enabling threat actors to breach enterprises," said Vitaly Simonovich, a threat intelligence researcher at Cato Networks. "Our new LLM jailbreak technique, which we've uncovered and called Immersive World, showcases the dangerous potential of creating an infostealer with remarkable ease. The emergence of the zero-knowledge threat actor poses a high risk to organizations because the barrier to malware creation has significantly lowered with GenAI tools."

The report underscores a critical concern for Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and IT leaders alike: the increasing accessibility of cybercrime. The rise of the zero-knowledge threat actor marks a fundamental shift in the cybersecurity landscape, demonstrating how virtually anyone, equipped with readily available tools, can potentially execute attacks against enterprises. This reality highlights the urgent need for proactive and comprehensive AI security strategies.

"As the technology industry focuses intensely on GenAI, it becomes evident that the associated risks are as substantial as the potential benefits," said Etay Maor, chief security strategist at Cato Networks. "Our report details the new LLM jailbreak technique that should have been blocked by the guardrails of GenAI. Its failure to do so allowed the weaponization of ChatGPT, Copilot, and DeepSeek. Our findings aim to elevate awareness about the dangers linked to GenAI tools, emphasizing the necessity for improved safeguards to prevent their misuse." ■

UK Government invests £45 million in school connectivity standards

The UK Government's Department for Education (DfE) has announced a significant investment of £45 million aimed at improving internet connectivity and ensuring that all schools across the country meet essential digital standards. This initiative includes fibre broadband upgrades for 833 schools, with the intent to help bridge the existing digital divide.

As part of this initiative, the government will launch a public consultation, open for eight weeks, to gather feedback on a long-term goal for all schools and colleges to comply with six core digital standards by 2030. These standards emphasize the fundamentals of effective technology infrastructure and include areas such as broadband internet, wireless networks, network switches, digital leadership and governance, filtering and monitoring, and cybersecurity.

To support schools in achieving these standards, the government is dedicating £45 million to enhance educational infrastructure, which prominently includes £25 million allocated for upgrading wireless networks this year. This investment aims to ensure that classrooms are equipped with reliable online access and to uplift standards in areas where it is most needed. This latest funding phase is part of an ongoing programme that has already improved connectivity for more than 1.3 million pupils across 3,700 schools, alongside a previous investment of £20 million to complete fibre upgrades for the targeted 833 schools.

A case in point of how the investment from the 'Connect the Classroom' scheme is making an impact can be seen at South Wirral High School. Prior to the installation, the school's Wi-Fi was unreliable, adversely affecting teaching and learning. Following the upgrade in January 2024, the school now boasts dependable Wi-Fi coverage throughout, allowing staff to access resources and plan lessons from anywhere on the premises.

Education Secretary Bridget Phillipson emphasized the government's commitment to modernizing the education system through a digital revolution in classrooms, highlighting the importance of equitable access to technological advancements: "I won't tolerate a system where some children benefit from innovation whilst others are left disconnected." ■

Word on the web...

Why the network is key to harnessing GenAI and generating growth

Sander Barens, Chief Product Officer, Expereo

To read this and other opinions from industry luminaries,

visit www.networkingplus.co.uk

Revolutionising campus connections: enhancing networking capabilities in higher education

Tom Whittle, Solutions architect – Networking, Telent

Robust and secure networking capabilities are pivotal to digital innovation and transformation within higher education and academic institutions. The education sector ranked fifth globally for cybercrime incidents, showcasing the need for a secure and reliable networking framework. When analysing devices within a university network, over 65% of Gen Z frequently use more than one device at a time, so they need a networking infrastructure that can cope with this demand.

Across the UK, both higher education and academic institutions are consistently looking for new ways to attract new academics, new students, and research teams to their campuses. So innovative and secure networks and technology stacks are not only key for talent attraction and retention but also support the university's expansion plans helping move them up the global university rankings.

The dynamic and fluid university environment has led many IT teams to plan for an agile networking environment. A university's networking capabilities must be implemented quickly and must have the ability to scale up or down depending on the university's needs.

Key elements, such as robust security, wireless connectivity, directory structures, and automated managed devices, all play a significant role in creating an enhanced networking system for academic institutions. However, these elements must all work in tandem to deliver students, lecturers, and researchers with the networking connectivity they need to excel.

For students, administration staff, lecturers and researchers, the university network must remain seamless, easy to use, and easily integrated with the pre-existing IT infrastructure. Without a private, secure connection, this can hinder not only students' academic work but also cause security concerns for sensitive research documents and data.

So the pressure is on for IT specialists to build and maintain secure networking capabilities, ensuring seamless connectivity and empowering innovation across higher education campuses.

Building resilient, high-performance networks

As universities increasingly rely on digital platforms for research, learning, and administration, developing a secure and high-performance networking infrastructure has become essential to support their growing demands and safeguard critical data.

Many higher education providers are recognising that having a robust, high-performance network is pivotal to a university's digital transformation journey, providing the digital platform to begin introducing new innovations.

To achieve this IT managers should begin by establishing the size, scope and specification needed for the upgraded networking infrastructure. Once this is confirmed, IT teams can then build out an agile networking framework with capabilities to add additional services and upgrades in future.

By creating a networking infrastructure that fits perfectly within the university ecosystem, IT managers can ensure that they can continue innovating and creating an up-to-date, advanced networking system to attract new talent to their university.

The role of AI and automation in revolutionising campus connectivity

The recent boom in AI and automation can enable transforming high-education networks, driving smarter resource management, bolstering security, and enabling seamless connectivity to meet the evolving demands of modern campuses.

But how is AI making a difference?

As higher education institutions look to upgrade and transform their networking environments, this includes changing LAN infrastructures, modifying LAN systems, and enhancing wireless networking capabilities to cope with an increased influx of IoT devices within the network.

Many of these 'headless devices', such as BMS systems, printers, and smart speakers, rely on Wi-Fi capabilities to, not only identify efficiency and performance issues but also to manage security risks. This is where AI and automation can influence a university's networking capability. By leveraging AI-driven analytics and automated processes, institutions can optimise network performance, predict, and prevent potential issues, and adapt to the increasing complexity of digital learning environments.

For instance, Oxford University recently introduced a new Juniper Mist Wi-Fi network with AI and automation capabilities to enhance wireless solutions and improve user experience. This new network benefits from the analysis of the data from all Mist solutions to deliver personalised monitoring, diagnostic reports, and configuration recommendations, ensuring optimised network performance and bandwidth strength at all access points across the campus.

Alongside recognising performance and efficiency issues, the use of automation and AI operations focused toolsets can also help support and strengthen the security of the networking infrastructure. This enhanced intelligence can highlight who can access the network and from where and also recognise security threats to the system. An increased visibility allows IT teams to create additional security context such as the location of user devices within the network, which aims to help keep both staff and student data private, but also sensitive research documents remain confidential.

Implementing AI and automated systems within a university network allows for enhanced visibility of the full network, allowing IT teams to ensure high performance and efficiency and pinpoint security risks to the whole network.

Empowering campus communities

High-performance networks are transforming university life, enhancing the student experience, streamlining administrative tasks for staff, and providing lecturers with the tools they need to deliver innovative, technology-driven education.

For university alumni, reliable and fast network connectivity is essential. Enabling seamless access to online resources, collaborative tools and learning experiences is paramount in fostering academic success and engagement.

In today's digital world, users are extremely demanding, students and staff do not want to have different logins for different locations on campus, they now expect a centralised networking framework that is seamless and easily accessible from anywhere on campus. Empowering students with self-service, private wireless LAN connectivity allows individuals private connectivity instantly, offering more automation and ownership over their own education and learning.

From a student's and lecturer's point of view, having a centralised network means easy access to library, course, and research materials, which creates a better and more attractive university experience. But for university admin teams their expectations are slightly different, so IT teams must be equipped to cater for all individuals within the university network.

Establishing a seamless, high-performance network, equipped with AI and automated capabilities, eases the workload on administration staff. IT teams no longer need to focus on time-consuming data collection, unnecessary troubleshooting, and other mundane tasks. IT teams can equip the network to detect issues, collect data and also recommend solutions, either pre-emptively or immediately once an issue arises.

This added foresight allows the IT staff to focus more on university innovation and overall alignment with business strategy, offering them the opportunity to discuss additional technology deployment and scalability within the university campus. These added capabilities can provide a shift in the once mundane admin job roles, offering increased job satisfaction by allowing staff to contribute to more high-value work for the university.

By catering to the diverse needs of students, staff, and lecturers, a well-designed higher education network becomes the backbone of a thriving academic community, enabling innovation, collaboration, and success for all.

The value of future-ready IT networks in higher education

As with any new technology, high-performance networks come at a cost. But universities must recognise the value of having innovative networking infrastructure to help drive innovation, unlock new opportunities, and also support staff retention.

Typically, higher education institutions have a higher turnover of IT staff than other sectrors, with one of the main concerns in recent years being low salaries. Therefore, universities must do everything in their power to create an attractive workplace and research centre to attract the latest talent to their alumni community.

By embracing a fully-equipped, top-of-the-range networking framework, institutions can create value through enhanced connectivity, allowing students and staff to remain connected at all times throughout their academic journey. It can create next-level teaching environments through personalised learning experiences, offering student autonomy with their learning and supporting a new 'work/learn-from-anywhere' hybrid approach. It can also provide lecturers and researchers with robust support for innovative research, offering seamless connectivity with the research community and ensuring the security and confidentiality of private digital research documents. ■

Having the last word against ransomware with immutable backup

Judy Kaldenberg, SVP Sales and Marketing, Nexsan

With ransomware incidents skyrocketing, it is no longer a question of if an attack will occur, but when. Organizations that believe that moving business-critical data to a cloud storage provider makes them immune from such threats are simply ignoring the reality. Ransomware doesn't discriminate — every business is a potential target.

In 2023, cybercriminals extorted more than US$1 billion in cryptocurrency payments from ransomware victims. What may have started as a simple business disruption just over five years ago has now ballooned into devastating multi-million-dollar incidents, often costing businesses their reputation and leaving them in a prolonged state of recovery – if they are able to recover at all.

The limits of traditional security approaches

Ransomware attacks have become far more sophisticated over time. Rather than clumsy brute-force incidents that hopefully yield a payoff, today's attackers are patient, carefully observing what data is most valuable, which files are most frequently accessed, and slowly gaining access to critical passwords.

Historically, organizations have relied on a combination of storage systems, snapshots, replication, and backups to ensure business continuity. But this standard strategy is now less of a defense and more of a target. Cybercriminals are increasingly focusing on these systems, knowing that they're key to recovery.

In fact, 93% of ransomware attacks today target backups, with 75% of those incidents preventing recovery altogether, forcing companies to pay the ransom or else. In addition to operational disruptions, businesses face severe penalties for failing to comply with industry regulations on data protection of personal information.

The cloud isn't the silver bullet

With the rise of automation and the shift to the cloud, many organizations believe they've found a secure, scalable, and cost-effective solution. Cloud platforms eliminate the need for expensive hardware and provide flexibility, with managed services doing the lion's share of the work. However, cloud storage is not the panacea it's often made out to be, especially when it comes to security.

Data security in the cloud is only as strong as the measures taken by company employees and the cloud provider. For industries like finance and healthcare, which must meet stringent regulations like PCI DSS, GDPR, and HIPAA, the cloud introduces additional challenges — chiefly the loss of control over their data. While all cloud providers offer at least some level of security, breaches still occur, often due to human error.

What happens if a hacker gains access to an organization's cloud credentials, say, for Microsoft Azure or AWS? How accountable are these providers when breaches occur? What is the process for regaining control over these accounts? These questions are especially pressing for businesses that must protect sensitive information or comply with legal and regulatory requirements.

Immutable backups - ultimate protection

Despite best efforts, vulnerabilities remain inevitable, whether in software, hardware or cloud infrastructures. The recent CrowdStrike outage highlighted just how disastrous even a non-malicious event can be when it hits a cloud-native platform, despite the best cybersecurity assurances.

So, with vulnerabilities everywhere, is there no hope for securing data? Not necessarily.

Protecting a company's most valuable asset — its data — remains crucial, even as data volumes grow exponentially. With more data under management and the introduction of additional resources prone to vulnerability, the challenge now is finding ways to scale while minimizing both human and technological error and ensuring data protection at every step.

The primary goal of any backup strategy is to guarantee the ability to recover data quickly and efficiently after an incident. In the age of ransomware attacks, immutable storage is critical. By adopting immutable backup solutions — such as immutable snapshots or S3 object-locking — organizations can ensure that their backup data remains unchanged, preventing cybercriminals from tampering with or deleting it. These immutable solutions protect against ransomware attacks, accidental deletions and even silent data corruption, providing an unbreakable line of defense.

Those looking to still take advantage of a cloud infrastructure while maximizing their data security might find that a hybrid cloud approach offers the best of both worlds — combining the scalability and cost-effectiveness of the public cloud with the control and security of on-premises solutions. Deploying immutable backups in hybrid environments ensure that backup data remains safe and recoverable, providing a reliable safeguard against the ever-evolving threats in the cybersecurity landscape.

The last word

While moving to the cloud offers many advantages — cost savings, scalability and greater reliability — security is not chief among them. With ransomware evolving to the point where it's no longer a matter of if, but when, every organization is a potential target. And the truth is, most companies don't see it coming until it's too late.

For organizations serious about securing their data, especially those dealing with highly sensitive information, an immutable backup solution — either standalone or as part of a hybrid cloud model — is the way forward. This is particularly true for industries like healthcare and finance, where compliance with regulations is non-negotiable.

The best approach to guaranteeing your data's safety, security and availability is to move beyond relying solely on the public cloud and instead implement an immutable backup solution. This approach not only defends against ransomware but also ensures data integrity, compliance and historical data preservation, sending a clear message to cybercriminals — your time is wasted here. ■

Cloud: the future is hybrid

Is the future of business computing hybrid? What should enterprises consider when it comes to their cloud needs, and how big an impact is automation playing?

As UK enterprises navigate an increasingly digital landscape, hybrid cloud has emerged as the preferred approach for managing IT infrastructure. A combination of on-premises, private cloud, and public cloud environments, hybrid cloud promises flexibility, resilience, and efficiency. But is it truly the future of cloud computing?

Sam Marland, Red Hat

Why hybrid cloud is the present — and the future

“Hybrid cloud is the reality today and will continue to be because enterprises need choice,” asserts Sam Marland, Senior Manager, Solution Architecture at Red Hat. “Just as organisations have historically used multiple operating systems or database technologies depending on the use case, they will continue to adopt a mix of hosting environments. A well-architected hybrid cloud strategy provides flexibility, resilience, and the ability to adapt much faster in a volatile and uncertain business environment.”

Matt Tebay, Multi-Cloud Evangelist at OVHcloud, reinforces this perspective: “hybrid cloud is the standard operating model for most businesses today. By 2027, 90% of organisations will adopt a hybrid cloud approach, according to Gartner. Hybrid cloud offers better flexibility, scalability, and more control over data — all while avoiding lock-in.”

James Sturrock, Director of Systems Engineering at Nutanix, believes that the future of cloud is undeniably hybrid as enterprises increasingly recognise that no single cloud model fits all workloads.

“Hybrid cloud provides the flexibility to run critical applications on-premises while leveraging the scalability and innovation of public cloud services. This approach ensures data sovereignty, cost optimisation, and seamless integration with existing infrastructure,” notes Sturrock. “When you consider all of the major changes that the world has gone through in the last decade from the shift to SaaS, IAC, 100% remote working to the release of real-world AI, the only way for businesses to protect their assets but innovate at a massively accelerated pace is to embrace hybrid multi-cloud.”

Indeed, a hybrid approach allows businesses to put workloads in the right environment for their needs. Sensitive data can remain on-premises without losing the flexibility of public cloud for other workloads. It also helps organisations to improve their overall resiliency by keeping data in different locations.

Yet, hybrid cloud is not a one-size-fits-all solution. Mark Chinery, Enterprise IT Head of Consultancy at FluidOne, observes that “the vast majority of companies we work with have been in a hybrid cloud environment for a number of years. Some companies with lower infrastructure footprints are moving to cloud-native, while others with heavy server infrastructure remain hybrid or are even moving back to on-premise due to the cost of cloud infrastructure.”

Matt Tebay, OVHCloud

Proper preparation prevents particularly poor performance

Hybrid cloud isn't a single technology but an approach to building resilient, flexible compute platforms that support evolving business needs.

Marland acknowledges that while a single-provider solution may seem attractive initially – offering simplicity, streamlined processes and faster time to market – many organisations find that these benefits are difficult to sustain as their needs change.

As Tebay notes, "one of the main factors to consider in a hybrid cloud approach is interoperability. Open-source systems are usually better because they're easily transferable. Kubernetes and Rancher, for example, allow businesses to manage multi-cloud environments with ease and move workloads between on-prem and cloud."

Adopting a hybrid cloud strategy requires a deep understanding of interoperability, security, and data management. Tebay highlights that hybrid cloud environments can become complex very quickly, so it's important to understand where the data is physically.

"This is one of the major reasons why companies are often reluctant to move to the cloud; having data nearby gives a sense of control," explains Tebay. "However, infrastructure providers are getting better at sharing where data is hosted, which allows organisations to understand the laws and processes that cloud data is subject to."

Meanwhile, Sturrock highlights two key technical aspects: "license mobility — you should always be able to move your licenses between clouds without having to re-purchase. And the ability to change clouds as your business requires — whether due to cost, performance, or geography, seamless movement between clouds and on-premises is essential."

When looking to make the shift to hybrid cloud, Chinery recommends following the 'Cloud Adoption Framework' from Microsoft to ensure the environment is set-up to best practice from day one and evaluate costs before implementing solutions – otherwise costs can run away with ambition.

"As the famous saying goes: proper preparation prevents particularly poor performance," highlights Tebay. "Technology leaders should do a thorough assessment of their IT needs alongside their business objectives and make sure that they're aligned before even starting to formally plan their hybrid cloud strategy. Time is precious, but it's always valuable to take time out and do an infrastructure health check, identifying which workloads are best suited to which environment in terms of cost, latency, sensitivity and other business requirements. It's also important to engage with different providers and choose the one that aligns best with your vision for cloud. Does their roadmap match your needs, for example? Does their technology performance and price align with your requirements? Is it a good cultural fit, and is the support appropriate for your business?"

Aron Brand, CTERA

Meanwhile, Sturrock suggests starting with a clear strategy that identifies which workloads benefit most from hybrid deployment: "invest in a platform that simplifies management across cloud environments, ensuring security, scalability, and operational efficiency, avoiding lock-in as much as possible – the future is fluid."

The real challenge for IT leaders is not choosing sides, rather architecting a system that dynamically places workloads and data where they drive the best business outcomes.

Aron Brand, CTO, CTERA: "storage sits at the core of this transformation. In the modern data economy, where data has become a core element of competitive advantage, data needs to be shared and used across local data centres, edge devices, and hyperscale clouds. IT architectures must reflect this reality, enabling seamless data mobility while maintaining governance, security, and performance. Hybrid cloud storage addresses this need - allowing IT teams to balance cost, speed, flexibility, and regulatory compliance."

Strengthening the hybrid case

Today, artificial intelligence (AI) and machine learning (ML) are accelerating cloud adoption by driving demand for increased compute power and seamless data access.

"Good automation strategies give both cost benefits and flexibility in the cloud," says Marland. "Quite often, automation in the cloud is easier because of the standardised nature of cloud offerings. AI/ML is potentially a key driver for cloud adoption over the next few years as the cloud has cornered the market for the underlying hardware."

Sturrock points out that "the government's announcement to invest in AI further fuels innovation, making hybrid cloud essential for managing and scaling AI workloads while ensuring data privacy and compliance."

Moreover, "open-source technologies to host AI/ML backend on less performant devices, or even more conventional processors are becoming available," notes Marland. "Model size reduction, and virtualised large language models are already being used to make AI/ML more accessible at a lower cost. This should reduce the cost and barriers to entry and make AI/ML even more accessible in a way that does not tie you to the cloud or even a particular cloud vendor."

And, with hybrid cloud becoming the norm, enterprises are increasingly adopting modern cloud-native technologies.

According to Marland, the traditional siloed approach to cloud management is no longer sustainable. Historically, application teams have been able to dictate specific service levels within availability zones and regions, while infrastructure teams have struggled to meet these demands due to the complexity of on-prem environments.

This disparity has created a bottleneck, preventing infrastructure teams from keeping up with changing business needs.

"A cloud-native design approach that applies equally to both infrastructure and application teams is essential for a unified hybrid cloud strategy. This means adopting principles like infrastructure-as-code, serverless computing, and containerisation across the entire ecosystem to create a seamless and integrated experience," says Marland. "We see enterprises unifying their on-premises and off-premises approaches using these technologies. Cloud has brought a better 'as-a-service' mindset to application and infrastructure teams, while containerisation and the standardisation of Kubernetes has brought in options for portability for customers embracing hybrid cloud. The one warning is to watch out for external dependencies that are either present on-premises or in the cloud. These are the handcuffs which can restrict portability and true hybrid cloud approaches."

Sturrock agrees that infrastructure as code, serverless computing, and containerisation will grow as hybrid cloud adoption increases.

"Nutanix's 7th Annual Enterprise Cloud Index report reveals that nearly 95% of UK organisations are containerising applications, with Kubernetes deployment across multiple environments reaching 60%," says Sturrock. "This highlights how these technologies streamline operations, enhance scalability, and enable faster application deployment across hybrid environments, driven by the need for infrastructure modernisation and cloud-native efficiencies."

The long-term impact

A hybrid cloud strategy fundamentally changes enterprise networking in the UK and the world at large.

Chinery explains that "a move to hybrid cloud requires increased network complexity, with architecture having to connect and manage workloads both on-premise and in the cloud. Enterprises look to use dedicated cloud connections that don't route through the public internet, offering more reliability, faster speeds, consistent latency, and higher security."

Indeed, Marland sees a shift in priorities: "hybrid cloud will drive competitive advantage, shifting focus away from infrastructure maintenance toward higher-value work. The adoption of hybrid cloud and a holistic, common platform to manage it will simplify infrastructure, creating a more agile IT environment that supports business needs and innovation."

"The organisations that will lead in the coming decade are those that master data placement and workload portability - not by choosing between cloud and on-premises, but by harnessing their opposing strengths in a continuous cycle of adaptation and innovation," notes Brand.

Hybrid cloud is no longer just an option; it is a strategic necessity for enterprises looking to balance flexibility, security, and performance. And, with advancements in AI, automation, and cloud-native technologies, the hybrid cloud landscape is evolving rapidly — empowering enterprises to innovate and stay competitive in an increasingly digital world. ■

James Sturrock, Nutanix

How the UK can restore its former glory in network management

Ian Smith, Head of UKTIN

Driven by globalisation and outsourcing, the UK's leading position globally in network technology and management has been increasingly challenged over the past few decades.

Our country is now too reliant on technology designed and manufactured abroad, with networks managed in outsourced centres across the globe. As the world moves into a more unstable period, this leaves the UK in a vulnerable position which needs to be addressed.

The telecommunications ecosystem and UK commercial landscape is unrecognisable from even just 25 years ago. This is partly due to the phenomenal growth the industry has undergone, and acceleration in traffic volume, as well as the demand for ubiquitous coverage 'absolutely everywhere' for consumers, enterprises, and machines. In turn, this has led to rising expectations for guaranteed quality of service and assured reliability, and trust for industry and public services.

However, today the UK telecoms landscape faces several challenges in meeting these expectations. This includes commercial complexity, with no single provider able to guarantee they can provide the entire physical or logical service truly end to end for their customers.

In addition, the UK telecoms industry is experiencing a shortage of talent with the right STEM skills, with workers in the industry, on average, older than 40, which is also hampering its ability to manage networks.

However, it's important to note that network performance is not just about the type of technology, be it fixed or mobile, that the user connects to. It's also about how the networks are managed. This is no trivial matter with the ever-increasing complexity of new 'G's' overlaid on existing networks, which require an ever increasing need to be able to maintain a great customer experience through excelling at network management.

To address these challenges, UKTIN's Network Management Expert Working Group (EWG) believes the UK government should look to build upon its global leadership in artificial intelligence (AI), bring the industry together by creating industry-specific requirements and standards, and fund research to help develop robust and scalable network management solutions.

Building upon AI leadership

As networks continue to sharply scale to support ever increasing data growth, the world of network management is and will continue to become more and more complex. In critical industries, customers will expect far better service availability than currently offered by the operators. It won't be acceptable to react to faults, but instead pre-empt issues, route around faults and repair services.

This will clearly require an AI-led approach, necessitating significant data capture and analysis from multiple sources to proactively predict and prevent faults affecting service.

For the UK, this provides a brilliant opportunity to build on its global leadership in AI and address its position in network management.

With networks shifting towards software running on specialised edge microprocessors close to end users or in the cloud, the UK is in a great position to take advantage of this by leveraging its knowledge base in software development, AI and microprocessor design. In addition, the strong academic research within its universities, competitive mobile and fixed networks, as well as its leading-edge service, finance and Net Zero industries, can also play a key role in strengthening its network management capabilities.

As part of this, the EWG has recommended the government facilitate a long-term vision to develop and leverage AI and automation technologies, to help improve and facilitate the management of our increasingly complex telecom networks.

AI training for scalable network management tools

Another key initiative would be to fund research focused on scalable and robust network management tools and datasets. Including real world datasets for AI training, with associated development and test platforms, would make a major difference in developing robust and scalable network management tools.

This could involve government-specific assistance, to incentivise and sponsor the creation of sharing platforms for time series data and large language model datasets, for training new AI services from real-world network data. This recommendation will require the appropriate sponsorship from UK operators, and UKTIN believes both the academic and non-academic world should promote this.

For the UK to regain its global standing in network management, it should back a truly long term, 20-year strategy to help telecommunications enable the modern economy, not just in the automation of network management, but also the facilitation and automation of all industries that will require telecommunications. ■

To colocate or not to colocate?

Is colocation the future for the UK's IT sector? Does in-house data centre ownership still make sense amidst rising energy prices and skills shortages? We chat with industry experts to find out what to expect in the years to come…

As UK enterprises navigate an increasingly complex digital landscape, the debate between colocation and in-house data centre capacity has never been more relevant. With rising economic pressures, energy costs, and sustainability concerns, many businesses are reassessing their IT strategies to determine the most efficient, cost-effective, and scalable approach.

Why colocation is gaining popularity

One of the primary drivers behind the shift towards colocation is cost-efficiency. Enterprises today need to control IT spending while ensuring high availability, security, and compliance.

Craig Messer, Managing Director of VeloxServ, explains that colocation offers lower upfront costs, reduced capital expenditure, and operational pricing models that make predictable budgeting far easier than managing an in-house facility - a tempting prospect.

“Colocation enables a business to scale up or down without costly changes to infrastructure, this also means a business can remain focused on its core operations and prioritising valuable time and resource into innovation and growth rather than data centre maintenance,” adds Messer.

Netwise Director Matt Seaton echoes this sentiment, emphasising that high-availability services are often out of reach for businesses operating on their own: “data centre operators have already made this investment, allowing clients to share in a purpose-built facility with only an operational cost consideration, giving access to a quality of service which far outstrips what would be possible in a non-data centre environment.”

Beyond financial efficiency, colocation offers greater flexibility and scalability. As business demands fluctuate, companies need IT infrastructure that can scale up or down without the burden of physical expansion or costly upgrades.

According to Vinny Vaghani, Operations Manager, IP House Ltd, “colocation is more cost-effective, flexible, and reliable than running an in-house facility. Businesses avoid the huge upfront investment and ongoing maintenance costs while benefiting from high-speed connectivity, built-in redundancy, and compliance with regulations.”

When does an in-house data centre still make sense?

While colocation is becoming the default choice for many enterprises, some organisations still find owning and operating a private data centre preferable.

Messer points out that sectors such as banking and healthcare often have strict security and compliance mandates that require keeping data in-house: “for larger or more established businesses with high but stable IT demands, it can also be more cost effective to invest in owning and operating a data centre rather than paying for colocation.”

Vaghani agrees that control and compliance remain key reasons for maintaining private data centres but warns that enterprises must weigh the long-term costs against the benefits of outsourcing.

“An in-house data centre still makes sense for businesses that handle sensitive data, need ultra-low latency, or have strict compliance requirements that demand full control over infrastructure. Large companies with stable, predictable workloads may also find that owning their own facility pays off in the long run,” notes Vaghani.

Matt Seaton, however, notes that these scenarios are becoming increasingly rare: “with modern high-performance networks, there are now very few cases in which allocating capital and costly in-house office space to a suitable on-site facility would be more advantageous. Generally, this is now limited to local comms room requirements, and in some instances a local ‘lab’ environment for system design and testing; even the latter use case here is now finding its place within an outsourced data centre.”

Scalability: is colocation the long-term winner?

Scalability is a major consideration in the build vs. buy debate, as IT infrastructure must support growth, performance demands, and evolving business models.

“Scalability plays a crucial role in deciding between colocation and an in-house data centre, as it impacts on budgets and capital expenditure vs. operational expenditure strategy, flexibility and growth plans, performance and return on investment and ultimately an alignment to the long-term strategic goals of a business,” says Seaton. “In-house data centres make the most sense when a business requires absolute security, ultra-low latency, complete control, or when long-term IT needs justify the investment. However, for most enterprises, colocation remains the more cost-effective, scalable, and resilient solution.”

Vaghani believes colocation remains the more agile choice, particularly for businesses considering hybrid cloud strategies: “colocation makes scaling quick and easy without the financial risk of expanding an in-house facility. But long-term, businesses should consider if their infrastructure will move toward hybrid solutions, where colocation can act as a central hub connecting private systems to cloud services.”

Indeed, while scaling services quickly is undoubtedly a clear advantage when working with a data centre, many enterprise clients see somewhat limited scaling requirements once their base service has been deployed, maintains Seaton: “we primary see heavy scaling requirements with MSPs and cloud service operators, who have to actively scale their deployments as their own client base grows, which isn't always the case with an enterprise customer.”

Crucial considerations

Before committing to either colocation or an in-house data centre, UK enterprises must assess their IT needs, compliance obligations, and financial strategies.

According to Messer, the decision revolves around five core areas:

1. Business strategy – Is the company planning for growth? Does IT infrastructure directly impact operations? Are sustainability goals better served by an external provider?
2. Budget – Can the business afford the capital expenditure of building a data centre? Are the ongoing costs of security, maintenance, and staffing sustainable?
3. Regulatory and compliance – Are there industry regulations such as GDPR, ISO 27001, or FCA requirements that demand on-premise data storage?
4. Performance and connectivity – Does the business need ultra-low latency for financial transactions or AI processing? Does it require direct interconnects to cloud providers?
5. Disaster recovery and business continuity – Can the company match colocation providers' redundancy, security, and uptime guarantees?

Seaton, however, suggests that most modern enterprises do not need to build private data centres unless they are large-scale technology firms like Amazon or Google: “for the vast majority of businesses, colocation is the obvious choice — providing enterprise-grade infrastructure without the burden of managing a complex, non-core business function.”

What lies ahead…

For most UK enterprises, colocation presents a clear advantage over in-house data centres, offering lower costs, greater scalability, and enterprise-grade resilience without the need for massive capital investment. While compliance-heavy industries may still require private infrastructure, the growing demand for hybrid cloud, AI workloads, and energy-efficient solutions is making colocation the preferred option. Moreover, as digital transformation accelerates, the UK's data centre landscape will continue evolving, with colocation playing an even greater role.

Messer believes the ongoing surge in data consumption — driven by AI and other applications — will fuel record levels of investment in colocation facilities: “for many businesses, the need for a scalable and cost-effective solution is likely to drive demand for colocation services. However, sectors such as financial services, government agencies and healthcare providers are likely to invest in in-house data centres to meet their unique requirements.”

Meanwhile, Vaghani expects hybrid cloud and edge computing to fuel further colocation growth, particularly as energy costs and sustainability concerns make private data centres less attractive: “companies will prioritise shared, energy-efficient infrastructure, reducing the need for dedicated on-premise facilities.”

Seaton is confident that colocation's role will remain foundational as businesses demand greater reliability and 24/7 uptime.

“Not all of the UK's data centre growth will be driven by colocation, but as more organisations embrace modern technologies, finding a suitable home for critical IT infrastructure will remain a key priority,” explains Seaton.

As UK enterprises plan for the future, the decision to build or buy must align with long-term business goals, IT strategy, and financial sustainability. With colocation providers offering cutting-edge infrastructure, security, and redundancy, it's no surprise that more enterprises are moving away from in-house facilities and embracing the flexibility of shared data centre environments. ■

Managing mission critical video on a massive scale

Jason Johur, TCCA Board Director and Vice-Chair, Broadband Industry Group

For first responders and emergency services workers around the world, applications and services that can enhance their work and contribute to greater safety and better outcomes are welcomed. Video is one of the most promising and versatile technologies for improving operational efficiency and effectiveness. With the increasing use of bodycams and drones, video is now widely considered as a significant capability to improve safety, coordination, collaboration, and quality decision-making, particularly during high stakes, end-user operational scenarios.

However, to ensure the effective use of video, public safety agencies and operators need to consider how to successfully deploy the service to support mission-critical operations, especially where the scale of its usage is considered 'massive'. This means situations where the amount of video could potentially saturate network resources, if not appropriately managed.

To address this, TCCA has formed a task force focused on massive mission critical video deployments, and specifically identifying the key considerations when planning its implementation and use. One of the first outputs of the task force is the white paper 'Guidance for the successful usage of Massive Mission Critical Video'.

Within the paper, key use cases representing different categories of operations are documented, i.e. day-to-day (routine) operations, pre-planned events, and major incidents. When analysing these use cases, identifying video producers and consumers is fundamental to understanding the overall problem domain, and those identified include actors such as first responders, officers, dispatchers, operators, government agencies, and other stakeholders.

From the outset, in creating the white paper, an emphasis was placed on identifying the key questions and challenges posed by mass use of video. This involved, amongst other things, polling representatives from government agencies and the critical communications industry. The results of the poll showed that the most frequent key challenges related to:

(i) Being able to set priorities and maintain control over the video flows
(ii) Ensuring seamless communications across different systems
(iii) Avoiding network congestion due to excessive video traffic

It is clear from the paper that using video effectively requires some forward planning and appropriate design of the network platforms to be used, especially in cases involving massive use of video. Properly dimensioning the network in terms of topology, spectrum and capacity is obviously a pre-requisite, as are the prioritisation of resources such as Quality of Service, Priority and Pre-emption (QPP) mechanisms. To manage the video streams, both application and operational perspectives need to be considered: 3GPP Mission Critical Video standards should be implemented, as well as the utilisation of video applications that react to the availability of network resources in a dynamic way in order to provide contextual data to the control room.

The main conclusions from this analysis - assuming no prioritisation of video streams or quality had occurred, and taking the use cases and a particular model of a typical commercial mobile network operator (MNO) network as a basis - show that how the warning phase of an incident is likely to be supported depends on the criticality of the incidents. A single dedicated radio network offers enough capacity for minor incidents; for major incidents a single commercial network is sufficient, whereas a combination of a dedicated radio network and a commercial network is recommended for critical incidents in rural areas.

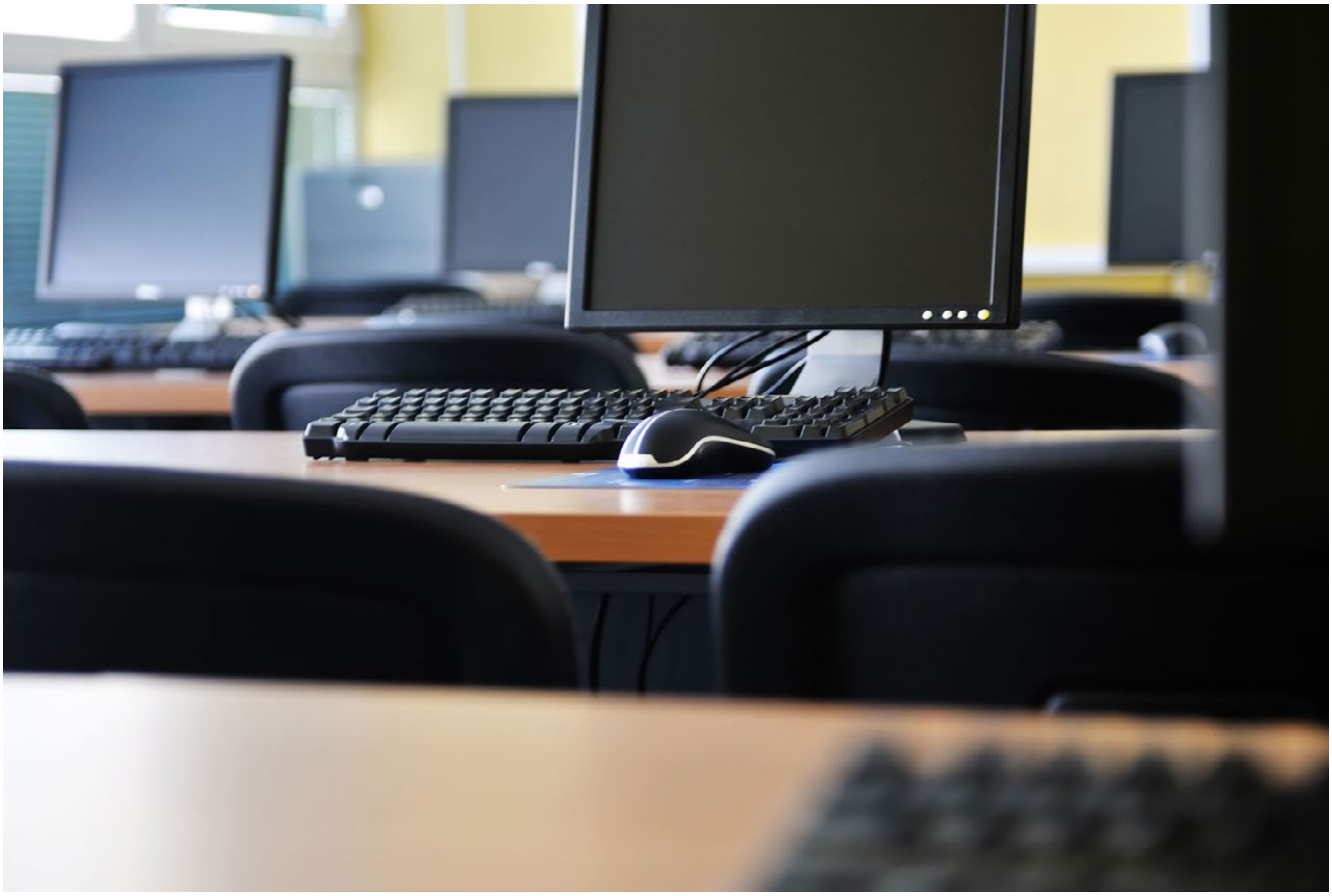
Critical incidents are often characterised by very high traffic levels, not only from first responders but also consumers using commercial networks, which if not managed could generate congestion impacting all. Implementing QPP including access and application priority mechanisms and optimising the radio network will serve to manage these high load situations. Most situations would benefit from implementing greater video compression techniques and prioritisation of video streams wherever possible.

A key outcome from this study was the identification of the principal challenges linked to the massive operational use of video, particularly in each identified scenario, incident phase and locality (urban, suburban and rural). All user organisations interviewed had concerns about video being very bandwidth-hungry and therefore considered video flow management – i.e. avoiding and handling congestion situations due to excessive video traffic – as an important aspect of their operations. The organisations identified the need to set priorities between video streams and maintain control of the priorities during operations. Interoperability and seamless communications across different systems and agencies must also be ensured.

Among the solutions to address these challenges is the implementation of an appropriate network capability with sufficient capacity. This can involve a dedicated radio network (or network layer), access to the Radio Access Network (RAN) of a commercial MNO, as well as being able to deploy additional and significant capacity and coverage on site through rapidly deployable networks. Access to spectrum, whether dedicated or shared, is therefore also key for video. This is true whether the wide area coverage is provided via dedicated or commercial network(s).

The white paper identifies several network and video application capabilities relevant for managing massive use of video, but it is essential that operations are also taken into perspective to maximise the benefit of using video, as well as adopting standards-compliant solutions.

Advances in intelligent video applications and network capabilities will improve the usability of video in mission critical situations over time. The overall objective is to ensure that first responders and public safety agencies (and by implication other critical communication sectors) can use video effectively and for operational benefit. ■



One Education Ltd protects at-risk data

One Education Ltd provides comprehensive IT support to over 130 schools, academies, and multi-academy trusts across the UK. Managing more than 170 devices, the organisation delivers on-site and remote technical support, internet connectivity, cloud backup, and management information services. A crucial part of their service offering is ensuring reliable data protection, as schools depend on secure and accessible backups for student records, operational data, and critical administrative functions.

Putting data at risk

For years, One Education Ltd had relied on a long-standing backup provider that had initially met their needs. However, over time, the solution's performance deteriorated to the point of being unreliable. The old system regularly experienced up to 80 failed backups per week, increasing the risk of data loss. IT staff were spending between 20 and 30 hours per week monitoring, troubleshooting, and attempting to fix backup issues. Recovering lost data proved extremely challenging and unpredictable, making it harder to guarantee business continuity for schools.

According to Jonathan Hambleton, Head of IT at One Education Ltd, the previous provider had become difficult to use and time-consuming to manage. The trust in the system had deteriorated to the extent that it became necessary to look for an alternative. With data security and uptime critical to education providers, One Education Ltd needed a highly reliable, easy-to-manage, and efficient backup solution to ensure seamless data recovery and business continuity for their clients.

A scalable and efficient backup system

After conducting a rigorous evaluation of eight backup vendors, One Education Ltd selected Cove Data Protection from N-able as the ideal solution. The decision was driven by Cove's superior functionality, ease of deployment, time efficiency, and seamless integration with other N-able products already in use. The transition to Cove allowed One Education Ltd to implement an automated, cloud-native backup and recovery system that significantly reduced manual intervention, while intuitive reporting and alerts ensured transparency on backup status.

With Cove's simplified management and monitoring features, the team could now diagnose issues quickly and resolve any backup failures without extended troubleshooting. Previously, fixing errors would often take so long that the next scheduled backup would begin before the previous one was fully resolved. Cove eliminated this issue, ensuring a smooth, uninterrupted backup process.

"The product we were using previously had a significant number of failed backups," explains Jonathon Gandy Senior IT Consultant, One Education Ltd. "Cove functions better from the get-go and failed backups are rare. On top of that, diagnosing issues is very quick because Cove gives you far greater insight into the reason(s) for a failure."

Deployment was rapid, and the solution was rolled out across all supported schools in just a few hours, minimising disruption. One Education Ltd was particularly impressed with Cove's ability to integrate seamlessly with the other five N-able products they were already using.

The shift to Cove Data Protection delivered immediate and measurable improvements, significantly reducing the administrative burden and ensuring greater backup reliability. Since implementation, backup failures have become rare, a stark contrast to the 80 failed backups per week that had been a regular occurrence with the previous provider.

One of the most significant benefits was the drastic reduction in time spent managing backups. Previously, IT staff had been dedicating between 20 and 30 hours per week to backup administration. With Cove, that workload has been reduced to just two hours per week or less. The automation of key tasks, such as ticket creation and reporting, transformed backup management into a nearly hands-off process, allowing the team to focus on delivering high-quality IT support to schools instead of firefighting backup failures.

Data recovery has also become a seamless process. Whereas previous data restorations had been time-consuming and unreliable, Cove enables rapid, stress-free recovery when needed. The increased efficiency has led to improved business continuity for schools and greater confidence in the backup system.

Future-proofing data protection for schools

By adopting Cove Data Protection, One Education Ltd has strengthened its IT service offering, ensuring that schools have a reliable, automated, and highly efficient backup solution. The reduction in manual workload, improvement in backup success rates, and seamless system integration have all contributed to a higher standard of IT support for educational institutions.

With a fully cloud-based, automated system now in place, backup management has moved from being an unmanageable burden to a streamlined and efficient process. The move has also improved profitability by freeing up IT staff time for higher-value tasks, while schools benefit from a more secure and resilient backup infrastructure.

According to Jonathan Hambleton, Head of IT, One Education Ltd, the transformation has been remarkable: "With Cove, management overheads have moved from unmanageable to minimal, to the point where we almost feel like we could 'set it and forget it,' allowing us to focus on delivering high quality support."

"The amount of man hours we've saved is invaluable. It's night and day to our previous solution and we've never had something like that before," adds Jonathon Gandy Senior IT Consultant, One Education Ltd.

The success of the migration has reinforced One Education Ltd's reputation as a trusted IT partner for schools, providing a secure, scalable, and efficient backup infrastructure that safeguards critical educational data. ■

Transforming IT infrastructure at St Elisabeth’s CE Primary School

St Elisabeth’s CE Primary School, part of the Thrive CE Academy Trust, embarked on an ambitious journey to modernise its IT infrastructure. Historically reliant on traditional servers and Windows devices, the school faced growing challenges in scalability, maintenance costs, and operational efficiency. With an increasing need for agile, secure, and future-proof digital solutions, the school partnered with Computeam to develop a comprehensive cloud migration strategy.

The first step in this transformation was the establishment of a Google tenancy, creating a robust, cloud-based foundation for improved collaboration, streamlined operations, and enhanced security. By leveraging cloud technology, St Elisabeth’s is now better equipped to support modern teaching methods, remote learning, and an evolving educational landscape.

Moving beyond legacy systems

The school’s traditional on-premises IT infrastructure presented several key issues. Aging physical servers posed a constant risk of hardware failure and limited storage capacity, leading to potential downtime and disruption. Additionally, the reliance on manual processes and outdated Windows devices made scalability difficult and restricted collaboration between staff and students.

A significant challenge was that the entire cloud migration process had to be completed within a week, requiring meticulous planning and flawless execution. The project needed to ensure seamless data migration, system integration, and deployment of cloud-based tools, all while minimising disruption to staff and students. Security was also a priority, as a new firewall system was essential to protect sensitive school data.

“We were tasked with transitioning St Elisabeth’s into a serverless environment over the summer break. This required rethinking their IT infrastructure to enhance efficiency, reduce costs, and improve scalability. By leveraging cloud-based architecture, we streamlined operations, minimised maintenance burdens, and positioned the school for future growth and innovation,” said Jacques Taylor-Beck, Senior IT Consultant, Computeam.

A fully managed cloud migration strategy

Computeam developed a tailored cloud migration strategy, ensuring a fast, secure, and efficient transition. The first step involved managing the school’s internet infrastructure and deploying a Barracuda firewall, providing robust cybersecurity and seamless connectivity.

The transition to a serverless architecture was driven by the need to reduce operational costs and eliminate the complexities associated with physical server maintenance. The cloud-based model enables greater flexibility, allowing the school to scale IT resources dynamically based on demand. Reliability and uptime were significantly improved, ensuring critical applications and data remained accessible at all times.

One of the major shifts was the introduction of Chromebooks, aligning with the school’s long-term digital strategy. These devices provided a simpler, more efficient learning experience, reducing dependence on outdated Windows machines. Computeam also implemented a remote migration process, allowing most of the transition to be conducted offsite, accelerating deployment and minimising disruptions.

A smarter, more agile IT environment

The successful cloud migration at St Elisabeth’s demonstrates the power of strategic IT modernisation. By eliminating on-site servers, the school has significantly reduced maintenance costs and freed up valuable physical space. The new scalable cloud environment enables seamless access to resources from any location, enhancing both remote learning and hybrid classroom experiences.

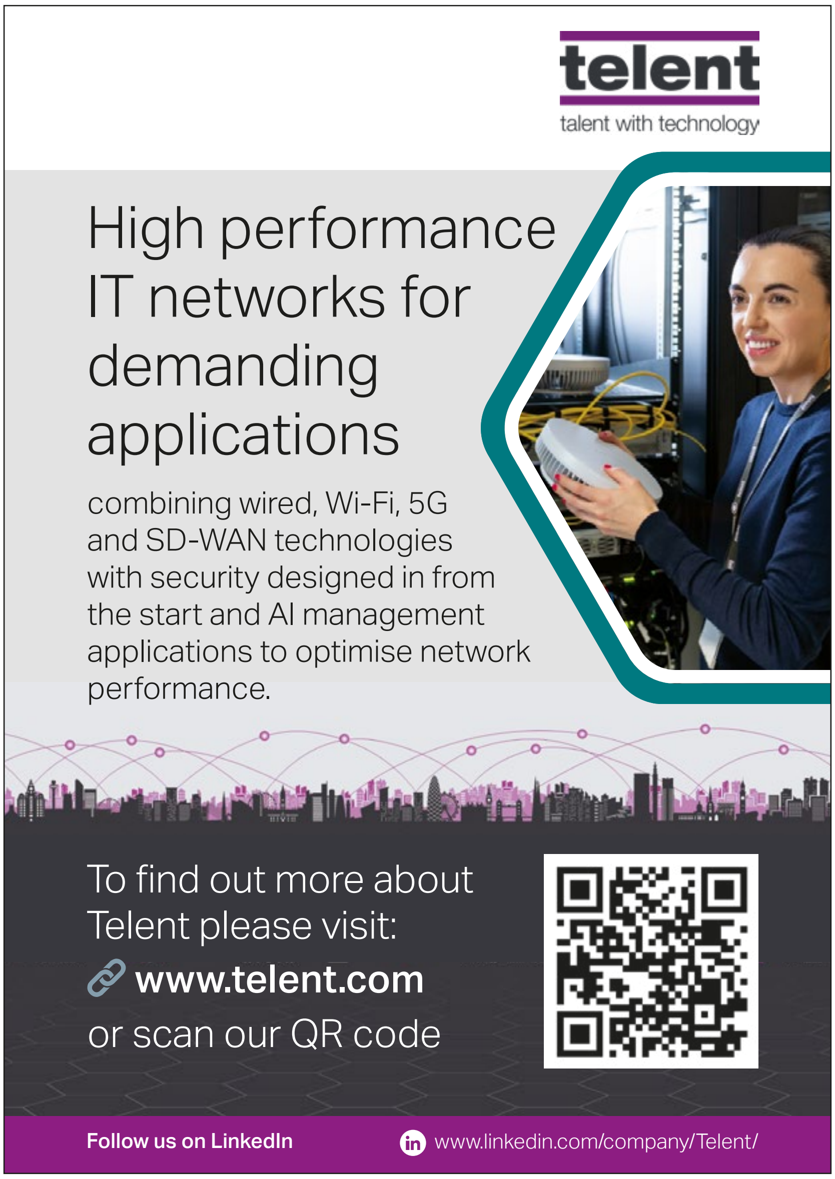
Security has been greatly improved with the Barracuda firewall, ensuring comprehensive protection against cyber threats. The migration has also fostered a collaborative and dynamic learning environment, where staff and students can easily share resources and access real-time data.

“From initial planning to final implementation, Computeam ensured school leaders were fully informed, and feedback was promptly addressed. What could have been a stressful process was made seamless by their expertise and professionalism. Their dedication turned a complex project into a smooth and successful transition,” said John Barrett, CEO, Thrive CE Academy Trust.

The project provided valuable insights into optimising cloud migrations for educational institutions:

- Pre-Provisioning Devices: By configuring Chromebooks and other devices in advance, deployment time and resource consumption were significantly reduced.
- Automation Tools: Using Migration Manager streamlined the data transfer process, reducing reliance on manual uploads and minimising the risk of errors.
- Training & Ongoing Support: Computeam provided post-migration training, empowering staff to fully utilise new tools, ensuring long-term adoption and productivity.

With a future-proof digital infrastructure now in place, St Elisabeth’s is set to embrace the next generation of educational technology, ensuring a smarter, more connected learning environment. ■



Smart water meters are a smart move for water resiliency

Lindsay Congreve, Head of Metering at Anglian Water

2010 saw the initial introduction of smart water meters in the UK; however, uptake continues to lag.

By March 2024, approximately 60% of households in England had water meters, but only 13% had smart meters. However, the Environment Agency has set out a plan to ensure that 48% of households have smart meters by 2030, 73% by 2040 and 76% by 2050.

Smart water meters are recognised as an improved technical solution to remedy the pressures on the water industry to improve responsiveness to water leakages and how they manage water supply more effectively. As well as this, a greater focus within the water industry has been placed on sustainability and efficient use of water.

This latter application for smart water meters is key in a region like the East of England, compared to other parts of the country, is under a great amount of pressure in terms of a lack of rainfall and an increasing population, which has squeezed resources. So, with the region officially being designated water-stressed, and said to be the driest in the country, it needs a long-term solution to solve the water crisis. Alarmingly, over a third of the water supply in the region is set to be lost by 2050.

Consequently, without long term planning, there will not be enough water to supply the region in the future. Smart meters are thus set to play a key role in how the water industry achieves resiliency through how they build out their Advanced Metering Infrastructure (AMI) in the industry within their asset management planning. The seventh Asset Management Period (AMP7) regulatory framework, which covers 2020-2025, focused on environmental protection and aimed to reduce leakages by approximately 15-20% by 2025. Looking into the future, the eighth Asset Management Period (AMP8), which is coming into effect in April 2025-2030, is focusing more on the environment, climate change and society, with reducing water leakages remaining as a top priority.

The goals of the AMP7 and AMP8 regulatory frameworks have driven greater investment in leak detection technology, like smart meters, which are market-ready. These devices have a number of sensors that are capable of connecting and transmitting data on the same networks. Smart water meters emit an array of data points which water suppliers can collect and analyse to have a greater understanding of how customers are using water and if there are any issues which can be solved efficiently.

The evolution of smart water meters

Currently, smart water metering leverages Advanced Metering Infrastructure (AMI), different from the Automatic Meter Reading (AMR) which was previously used. AMR was used for small metering as the devices had an element of onboard memory that monitored leak and tamper alarms. However, the data which was fed back to suppliers from these devices was of poor quality.

From there, the definition of smart metering has evolved to AMIs. This uses wireless mesh networks, leveraging both radio 4G cellular networks and low-power wide-area networks (LPWANs). In more dense urban areas, AMIs use 4G Internet of Things (IoT) connectivity across the smart meter technology, but in areas where there are connectivity challenges, LPWANs are used.

Here, meters relay encrypted data to other nearby devices, which form a chain that sends the data to a central hub consistently. With the regular data updates from the AMIs being fed directly to the provider, it is much more effective in identifying issues in the network, such as pipe leakages or plumbing issues.

Once the data is received, water providers can leverage artificial intelligence (AI) and advanced analytics platforms to process and analyse the data and gain insights. Through data aggregation and pattern recognition, providers can better understand trends in water usage and leak detection. Going forward, using historic and real-time data, water companies can forecast future demand, which better informs resource allocation.

Overcoming the hurdles

Even though smart water meter provide better detection of issues within the network of devices and more proactive customer service, there are still a number of obstacles which those in the water industry must overcome for a wide scale rollout. A substantial issue is that of limited availability of resources and the lack of infrastructure. As well as this, the growing population is putting significant pressure on the existing infrastructure, which needs more investment.

Over the years, there have been monumental shifts in weather patterns with much drier summers, and wetter winters. In fact, 2023 was the second warmest year on record for the UK. Indeed, the number of 'hot' days, those that surpassed 28 Celsius has more than doubled and 'very hot' days, those over 30 Celsius, has tripled from 2014-2023. Even though 2023 was the seventh wettest year on record for the UK since 1836, rainwater and flooding does not necessarily lead to water that is usable due to a risk of contamination.

As such, a robust water resources management planning process should be implemented which focuses on a strong smart metering strategy, with enhanced network connectivity. This will enable water companies to maintain supply-demand balance, whilst building new supply-side infrastructure to ensure continued water supply. Not only that, but with smart meters enabling constant monitoring of water usage and detection of issues, it facilitates better understanding and communication with customers. By being able to pinpoint leakages in the network, it enables engineers to solve issues much faster and create water efficiency benefits.

Smart water meters are reshaping systems across the country through creating a robust water supply and lower bills for customers. Through leveraging the power of advanced data analytics and seamless network connectivity, smart meters revolutionise how water providers understand current customer consumption patterns and predict future usage. With the adoption of smart water meters expanding, it creates an efficient water supply for today, but it also ensures resilience for tomorrow. Smart water meters are not only connectivity devices that are installed in people's homes, but are transformational in creating a resilient water supply for the future. ■

How to select the most efficient UPS for your data centre

Justin Killick, UK & Ireland Manager – Critical Power, Socomec UK

Now designated as part of the UK's critical national infrastructure, it's vital that data centres are 'always on.' Furthermore, with the National Grid predicting a six-fold increase in the sector's power consumption by 2034, energy efficiency is equally vital.

These dual demands — availability and efficiency — pose challenges for Uninterruptible Power Supply (UPS) performance and energy management. It has never been so important that UPS equipment is durable and optimised to support the uninterrupted supply of critical loads in the most efficient way possible.

Limitations of traditional UPS mode switching

The classic UPS operating mode is 'bypass,' where power flow is redirected from the UPS to the critical load during maintenance, servicing, or equipment failure. Other modes include 'double conversion' and 'line interactive', which have both been engineered to ensure uninterrupted power during outages and fluctuations. More recently, eco mode has emerged to help reduce power consumption.

Switching from one of the first three modes to eco mode is possible but it does cause a brief loss in power. To avoid this, data centre operators are often forced to make upfront decisions to maximise UPS performance and optimise Power Usage Effectiveness (PUE). In doing so, they often face a trade-off between data centre uptime and energy efficiency.

A new era of UPS innovation

To counter this, UPS manufacturers are now developing smarter modes that reduce energy losses while guaranteeing a protected power supply. Unlike standard eco modes that can suffer from voltage drops, these advanced systems ensure instant transitions during grid disturbances without compromising load protection.

This wave of innovation not only reduces power consumption and CO2 emissions but also optimises energy performance. The UPS can intelligently manage and select the best operating mode, allowing data centre operators to continually balance power quality and sustainability.

Efficient design for energy savings

These next-generation UPS systems leverage advanced algorithms to monitor the network in real time, dynamically selecting the optimal mode. They ensure continuous protection by leveraging the static bypass as the main power source while keeping the active UPS synchronised with the grid.

Unlike traditional double conversion, where efficiency drops at high load levels, static bypass gains efficiency as the load rate increases. This leads to efficiency of nearly 99 percent from a 50 percent load level, potentially saving up to 350 MWh of electricity per year, reducing heat generation, cooling costs, carbon emissions and operating expenses.

Ongoing monitoring for power protection

Dedicated monitoring systems assess network characteristics like voltage, frequency, and harmonic distortion to ensure optimal conditions for the load. An internal algorithm continuously checks network quality, enabling instant mode switching during disturbances. Additional algorithms prevent repeated transfers between modes which might add to – rather than counteract – network instability. These controls ensure the load is always protected with a high-quality, continuous power supply.

Benefits

By reducing classic UPS energy losses by up to five times compared to a standard double conversion mode, these emerging smart modes enable organisations to significantly reduce their energy consumption. Furthermore, with lower consumption, less heat is generated, reducing cooling requirements and operating costs. These efficiency gains have a direct impact on the total cost of ownership of a data centre, while there are significant environmental benefits in the form of reduced emissions.

These efficiency benefits also come with major improvements in power quality. In the event of serious disturbances to the network, transitioning between modes is autonomous and instantaneous, resulting in the highest possible protection. Furthermore, advanced filtering capabilities help eliminate distortion content, protecting this vital infrastructure from overloads and under- or over-voltages.

Conclusion

The evolution of UPS technology is a critical step forward in meeting the growing demands of the UK data centre sector. With the need for continuous uptime and improved energy efficiency, smarter UPS systems offer an effective solution to balance power quality and sustainability.

By leveraging advanced algorithms and real-time monitoring, these systems not only reduce energy consumption and carbon emissions but also enhance infrastructure protection. This innovation ultimately leads to significant cost savings, improved operational efficiency, and a reduced environmental footprint.

As data centres face increasing pressure to support accelerating digital transformation goals, adopting these advanced UPS systems is essential for future-proofing operations while at the same time, meeting sustainability goals. ■

PRODUCTS

As data centres expand in scale and complexity, the need for reliable, efficient and adaptable power solutions is more critical than ever. The **PILLER POWER SYSTEMS** M+ Series Modular Static UPS, with power capacities from 250kW to 1200kW, delivers high-performance, scalable solutions tailored for data centres of all sizes.

Designed for modern IT infrastructures – including high-performance computing (HPC), artificial intelligence (AI), hyperscale data centres and colocation facilities – the M+ 500 and M+ 1200 models offer superior reliability, efficiency and uninterrupted operation, even during maintenance or upgrades. With a global network of expert service technicians supporting over 10,000 high-power UPS units across 40+ countries, Piller ensures continuous, 24/7 operational excellence for clients in finance, industry, communications, aviation and defence

Mark Lee, Managing Director, Piller UK Ltd, commented: "Our customers asked for a hot-swappable, high-density modular static UPS – and the M+ Series is our answer. It represents the next evolution in static UPS technology."

For more information visit https://www.piller.com/product/m-series-modular-static-ups/

The **Centiel** StratusPower UPS has a robust output range from 10kVA to 800kVA, providing unparalleled power protection for data centres, server rooms, and industrial environments. Equipped with advanced double-conversion technology, it ensures a consistent and clean power supply, offering a remarkable efficiency of up to 96% in online mode. The StratusPower UPS features a compact, modular design that allows for easy scalability, enabling users to expand capacity seamlessly without downtime. Its high-power density means you can save valuable space in the facility. This UPS is designed with a user-friendly touch-screen interface, providing real-time monitoring and control. Additionally, it is equipped with smart battery management, optimizing battery life and performance. The StratusPower UPS supports a variety of battery types, including Lithium-ion and lead-acid, catering to diverse operational needs. Furthermore, it includes advanced features like remote management capabilities, allowing operators to monitor system health via SNMP, Modbus, or Web access.

The **ABB** DPA 500 Modular UPS system offers a power capacity range from 100-500 kVA, facilitating flexibility in deployment and enabling users to configure the system based on their specific power requirements. The DPA 500 employs a de-centralized parallel architecture that ensures redundancy and enhances availability by eliminating single points of failure.

The UPS operates using a double-conversion online topology, ensuring that the connected loads receive a clean and stable output voltage of 400 VAC, with adjustable voltage and frequency. The system's input voltage range accommodates a wide spectrum of conditions, generally from 400-480 VAC, allowing it to handle fluctuations in electrical supply effectively. With an impressive efficiency rating of up to 97% in online mode and up to 99% in eco mode, the ABB DPA 500 helps in minimizing energy consumption and operational costs.

Thermal management and cooling are optimized with a unique design that employs natural ventilation for efficient heat dissipation. The UPS features intelligent fan control that adapts to the load conditions, reducing noise levels and improving energy efficiency.

Schneider Electric has unveiled the Galaxy VXL, an UPS boasting 500-1250kW (400V) capabilities. This highly efficient, compact, modular, and scalable UPS is designed for demanding infrastructures such as AI, colocation, and hyperscale data centres, as well as large-scale commercial and industrial establishments.

Measuring just 1.2m² with an impressive power density of up to 1042kW/m², the Galaxy VXL achieves industry-leading efficiency, providing up to 99% efficiency in eConversion mode and 97.5% in double conversion mode. It supports critical loads up to 1.25 MW in a single frame and can scale to 5 MW by paralleling four units, all while slashing overall energy costs.

Equipped with N+1 redundancy, the modular architecture enhances availability tenfold, allowing customers to expand with incremental power modules. The Galaxy VXL features a Live Swap function, minimizing downtime during service and ensuring resilient operation. Enhanced connectivity and security meet the stringent IEC 62443-4-2 standards, while EcoCare membership offers premium support and 24/7 remote monitoring to maximize longevity.

The **CertaUPS** C650R has a power rating of 650VA and an output power factor of 0.5, delivering a robust 325W, making it suitable for small server room environments.

The C650R operates with a voltage input range of 180-290VAC, which ensures stable performance even in less-than-ideal electrical conditions. Its output voltage is a pure sine wave, crucial for maintaining compatibility with a wide range of devices, including computers, routers, and networking equipment. The unit features a frequency range of 50/60Hz, automatically adapting to the detected power source for optimal efficiency.

One of the standout features of the CertaUPS C650R is its intelligent battery management system. It is equipped with a sealed lead-acid battery that provides reliable power support during outages, and the battery has a typical backup time of up to 30 minutes under standard load conditions, allowing users sufficient time to save work and safely shut down equipment. The unit supports both cold start operation and a user-replaceable battery system, making maintenance and emergency use straightforward.

Please meet...

Steve Brodie, Chief Revenue Officer at Goldilock

Who was your hero when you were growing up?

Growing up, I had many sporting heroes, including Linford Christie, Duncan Goodhew, and Frank Bruno, as well as a few Spurs players.

As I got older, my admiration shifted towards global figures like Nelson Mandela. I was fortunate enough to meet his wife, which was a truly inspiring experience.

What was your big career break?

A pivotal moment in my career was when Cisco offered me a position just as I was about to embark on a PhD. However, I believe that career success also hinges on recognising and seizing opportunities when they arise. There have been many critical junctures throughout my professional journey.

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

Easy. I wanted to be an astronaut, and I have a story about that for another day…

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

It would be a privilege to share a meal with an iconic figure like Winston Churchill. His leadership during World War II was truly inspiring, and I would be fascinated to learn from his experiences and hear some of his stories.

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

Always treat people with kindness and respect. Above all else, people come first.

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

That's a tricky question, as so many are vital. If I possessed the talent, I imagine a career as a professional athlete would be super rewarding and fun. You're getting paid to be the healthiest version of yourself that you can be! Otherwise, I'd probably gravitate towards a field that contributes to positive societal change and progress for all.

The Rolling Stones or the Beatles?

Both are legendary, but I'd probably give the edge to the Rolling Stones.

What would you do with £1 million?

My top priority would be securing my children's future. After that, I'd spend it wisely and perhaps indulge in a long-held dream, like a classic car.

Where would you live if money was no object?

Ideally, I'd stay close to my loved ones, so the New Forest would be a wonderful place to call home. However, I'd also love to have properties and boats in various locations around the world, allowing me to explore and experience different cultures.

What's the greatest technological advancement in your lifetime?

From my perspective, the greatest technological advancement of my lifetime is undoubtedly the internet. Its impact has been truly transformative on every single industry across the world and has offered us all so much opportunity.

Consider the rise of e-commerce, the accessibility of information, and the power of remote work – all made possible by the internet. And let's not forget the personal impact: affordable communication via platforms like Skype, the convenience of electronic payments, and now these pocket-sized entertainment and communication devices we call smartphones!

However, it's important to acknowledge that technological advancements are not without their challenges. Ensuring the secure, ethical use of these technologies remains an ongoing issue, especially with the rise of new advanced technology like AI.

Of course, I'm biased, but I believe Goldilock FireBreak represents a significant step forward in cybersecurity by providing a unique and powerful layer of defence against cyber threats. It addresses critical challenges in the digital age by enabling organisations to instantly and physically isolate their critical assets from the internet, minimising their attack surface and preventing data breaches. This innovative approach demonstrates the potential for technology to both empower and protect organisations in the face of evolving cyber threats. ■